9-2016

Internet Access and Freedom: Constructing and Reacting to Transnational Norms about Internet Diffusion and Use

Heather L. Katz
The Graduate Center, City University of New York

INTERNET ACCESS AND FREEDOM: CONSTRUCTING AND REACTING TO TRANSNATIONAL NORMS ABOUT INTERNET DIFFUSION AND USE

by HEATHER L. KATZ

A dissertation submitted to the Graduate Faculty in Political Science in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York

2016

Internet Access and Freedom: Constructing and Reacting to Transnational Norms about Internet Diffusion and Use

by

Heather L. Katz

This manuscript has been read and accepted for the Graduate Faculty in Political Science in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

_____	_____
Date	Professor George Andreopoulos Chair of Examining Committee
_____	_____
Date	Professor Alyson Cole Executive Officer

Supervisory Committee

Professor George Andreopoulos

Professor Stephen Brier

Professor Matthew Gold

THE CITY UNIVERSITY OF NEW YORK

Abstract

Internet Access and Freedom: Constructing and Reacting to Transnational Norms about Internet Diffusion and Use

by

Heather L. Katz

Advisor: George Andreopoulos

This dissertation explores how demands for Internet access have taken shape in the international system and to what degree a right to access or the Freedom to Connect (F2C) can be said to exist. It also studies how states have responded to demands related to access and Internet penetration. A review of the literature reveals that most work concentrates on violations of users' rights on the Web and bypasses questions about whether and how users can access this vital piece of technology. Utilizing discourse analysis, the study shows that the F2C is being framed by a diverse range of actors using traditional international platforms and through transnational means that include the medium itself. Nine case studies are conducted to gauge states' reactions to demands for increased Internet penetration and meaningful access. It demonstrates that a state's political culture and its preexisting relationship with human rights are the greatest predictors of what steps governments take in relationship to a right to access. Liberal states are quick to view access as either a right in itself or as enabler of other rights like expression and political participation, while illiberal states claim their sovereignty extends into cyberspace as a necessary exception to human rights. This dissertation investigates how access is related to larger issues of Internet freedom like monitoring and censorship. It also addresses how international relations theory can apply to questions about states' relationships to information and communications technologies. Finally, it will help us understand how human rights are understood on the Web and how normative discourse and development are carried out on the Internet.

Acknowledgements

This study is the result of many people's patient and thorough assistance. I would like to thank the members of this dissertation committee, George Andreopoulos, Stephen Brier, and Matthew Gold; particularly, I appreciate George Andreopoulos's reading of numerous drafts and his assistance in shaping the theoretical implications of this work. I am forever indebted to my family for their thoughtful input and unwavering support.

Table of Contents

List of Tables

List of Figures

List of Acronyms

Acronym	Term	Definition of concept or associated nation-state
APJII	Association of Indonesian Internet Service Providers	Indonesia
ARPANET	Advanced Research Projects Agency Network	United States
BPO	Business process outsourcing	A type of outsourcing involving routinized office functions or customer relations
BTS	Base transceiver station	Infrastructure connecting mobile Internet users to network provider
CeC	Community eCenter	Philippines
CEDAW	Convention on the Elimination of Discrimination Against Women	Human rights instrument
CENIAI	Center for Automated Exchange of Information	Cuba
CERD	Convention on the Elimination of All Forms of Racial Discrimination	Human rights instrument
CGI.br	Internet Steering Committee	Brazil
CMEA	Council for Mutual Economic Assistance	Economic organization lead by Soviet Union among communist states during the Cold War
CNNIC	China Internet Network Information Center	China
F2C	The Freedom to Connect	Internet freedom norm
FCC	Federal Communications Commission	United States
FOM	The Public Opinion Foundation	Russia
GON	Government-owned networks	Typically broadband networks fully or partially operated by the public sector
ICANN	Internet Corporation Assigned Names and Numbers	Organization responsible for Internet domain names
ICCPR	International Covenant on Civil and Political Rights	Human rights instrument
ICESCR	International Covenant on Economic, Social, and Cultural Rights	Human rights instrument
ICT	Information and communications technology	
IFT	Federal Institute of Communication	Mexico
IGF	Internet Governance Forum	Outcome of the WSIS process that is a platform for Internet governance policy considerations; non-binding recommendations
INEGI	Instituto Nacional de Estadística y Geografía (National Institution of Statistics and Geography)	Mexico
IR	International relations	
ISP	Internet Service Provider	Organizations that sell Internet service to consumers or businesses
ITB	Institut Teknologi Bandung	Indonesia
ITU	International Telecommunications Union	United Nations specialized agency
IX	Internet exchange	Point of exchange of Internet traffic between providers of content and access
LoIs	List of Issues	HRC questions to periodic reports of states parties to ICCPR

MDGs	Millennium Development Goals	United Nations 2000 development agenda
MENA	Middle East and North Africa region	
MNC	Multi-national corporation	
MODITUH	Los microdatos del Módulo sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (Availability and Use of Information Technologies in the Household)	Mexico
MVNO	Mobile virtual network operator	A wireless ISP that buys bandwidth wholesale and resells it to customers
NIEO	New International Economic Order	United Nations set of proposals
NSA	National Security Agency	United States
NTC	National Telecommunications Commission	The Philippines
PLDT	Philippine Long Distance Telephone Company	The Philippines
PNBL	Programa Nacional de Banda Larga (National Broadband Plan)	Brazil
POP	Point of presence	Physical location used by ISPs to house equipment that supplies Internet service
PRISM	Planning Tool for Resource Integration, Synchronization, and Management	United States, shorthand term for NSA surveillance program
REI	Red de Innovación Aprendizaje (Learning Innovation Networks)	Mexico
RNP	National Research Network	Brazil
SDGs	Sustainable Development Goals	United Nations 2015 development agenda
SES	Socioeconomic status	
TCP/IP	Transmission control protocol/Internet protocol	Set of technical rules between two communications systems on how data will be transferred
TVWS	Television White Spaces	Unused television frequencies that can transmit Internet service
UNHRC	UN Human Rights Council	United Nations body
USAID	United States Agency for International Development	United States
WEF	World Economic Forum	
WSIS	World Summit on Information Society	UN conferences on bridging the digital divide in Geneva (2003) and Tunisia (2005)

Chapter 1: Theoretical Framework and Literature

Access to the Internet is fundamental to economic, social, and cultural life in the 21st century. For many in the developed world fast, reliable service does not only mean the banalities of posting to social media or deleting spam emails, but also means access to the job market, research materials, healthcare information, government services, and in some cases the chance to directly participate in the democratic process. For those in developing states, membership in the Information Society could mean leapfrogging over the development hurdles that typified economies of the past. Despite its importance Internet penetration within states and across the globe is uneven and inequality of access threatens to deepen in the years to come.

Internet penetration grows each year; by the end of 2015, 3.2 billion people around the world used the Internet, representing 43.4 percent of the world's population. These figures have quickly grown since 2000 when only 6.5 percent of the world used the Internet (ITU 2015a). Nonetheless, there is a significant "digital divide" between the Global North and South, urban and rural populations, the rich and impoverished, and more. This dissertation seeks to understand how demands for access have taken shape and to what degree a right to access or the Freedom to Connect (F2C) relates to other Internet freedom norms that have been disseminated in the course of the Internet's worldwide development. The norms that exist in regard to the spread of the Internet are developed by transnational norm entrepreneurs working on typical international platforms like the UN and through virtual networks among professionals working across states. This study seeks to address the normative development processes of the F2C and other Internet freedom norms and which theoretical frameworks can be the most useful for scholarship on international relations (IR) and the Internet.

Power on the Internet is a topic often considered by IR and comparative politics scholars in the last two decades. States have proven themselves to be important actors in this area that initially invited cosmopolitan assessments about the diffusion of power embodied by the likes of the "Declaration of the Independence of Cyberspace (1996)." Despite John Perry Barlow's contention that states "have no sovereignty where we gather," they have asserted themselves in all areas of technological propagation and use. Studies have largely concentrated on censorship, surveillance, and cyber-attacks at the

expense of access. How have states reacted to demands for increased access and greater freedom on the web?

Finally, this study will also address the relationship among access, Internet freedom, and human rights. Freedom on the web can merely be viewed as the extension of the protection that many states guarantee offline: expression, assembly, privacy, education, work. But access demands that states take a proactive role in the provision of what was once considered a value-added service. Is it accurate or useful to see technology as a right? How have states responded to such demands?

In seeking to answer these questions, this study will test two hypotheses. First, the F2C is an emerging norm in the international system that is being advanced by those who work to bring it about, norm entrepreneurs, on traditional and non-traditional platforms. Even the Internet's founders question the idea that the Internet is a right that obliges a state not to interfere with its provision or directly provide the service. It is necessary to discover who the norm's proponents are and how they frame the problem of access. Further, has this norm had any effect on states' behavior? The second hypothesis argues that states will react to demands regarding increasing Internet penetration and access according to their political identity and I will use the Freedom House's *Freedom on the Net* rankings as a gauge to predict whether the states examined would have a proactive or reactive response a right to access.

This chapter contains a discussion of how theories of IR consider the relationship between normative development and power. The study of the development of new duties, rights, or ideas is most closely associated with constructivism, but is in fact integral to realism, liberalism, and the British school. Each of these theoretical frameworks' considerations on norms, cooperation, and the role of non-state actors will be considered in turn and a synthesis of their insights will be made for the purpose of evaluating the F2C. IR scholars have long-discussed the transformative capacity of information and communication technologies (ICTs), and the literature's merits will be considered. The power of the state should not be underestimated, but few scholars have given serious consideration to the issue of access itself.

Chapter 2 will discuss the research methodology for this study and lay out in more detail the data collection plans for the hypotheses. Framing methodology will observe how different entrepreneurs have modeled access as a right and what access means. Further, it will justify the selection of nine cases and

how they have reacted to the F2C, which frames they have adopted, which they ignore, and which they have explicitly rejected.

Chapter 3 contains the data collected for the first hypothesis, discussing who the norm entrepreneurs are and how they conceptualize a right to access. Chapters 4 through 6 contain the data observed for cases selected to test the second hypothesis, including background information, the history of Internet adoption, penetration statistics, state actions that have been designed to improve or restrict access, and other relevant efforts relating to the F2C within these states.

Finally, Chapter 7 will compare the efforts of each of the selected cases. Freedom House's categorization of cases is a good predictor for the types of efforts states have taken to increase Internet penetration and meaningful use. Free and Partly Free states partner with others—non-government organizations (NGOs), multi-national corporations (MNCs), local Internet service providers (ISPs)—in order to increase Internet access and its meaningful use. In Not Free cases, power remains centered around the state, limiting the diffusion of the Internet and opening windows of opportunity for interference in access, going so far as to switch it off. There are even stronger points of comparison between states in the same region that face similar limitations of geography, regime type, and political culture.

The F2C is a norm that is being developed by norm entrepreneurs on highly visible international platforms and through the diffuse networks one finds on the Web itself. Not all entrepreneurs frame the F2C in the same manner just as states will not interpret their duties to access or Internet freedom in the same way. Normative development surrounding the web is a multifaceted, indirect process in which states and non-state actors (NSAs) interact to shape the frames of the F2C. Not Free states are not absent from this process, but are competing with an international society based on a cohesive set of liberal rights in which the content of Internet freedom norms are understood.

Building a Theoretical Approach to the F2C

Considering the frameworks to IR theory used for this study—realism, liberalism, constructivism, and the British School—it is necessary to show how each of these approaches will contribute to understanding the F2C. At first glance this seems to be an overwhelming task, as doing so would mean this study is a theory-building enterprise that seeks to create new frameworks. On the contrary, constructing guideposts using each approach's theoretical assumptions will bring some order to the

chaos that is empirical IR research. By simply choosing one or two of these approaches as the backbone of this dissertation, much of its internal validity would be undermined. The goal of this research is for others to be able to understand and study the way in which norms in IR and the Internet are created and what effect they have, not creating a simple theoretical construct.

Such a task is complicated given that each approach has fundamental differences that are difficult to set aside. Evans and Wilson (1992) undertake a related problem in their article, "Regime Theory and the English School of International Relations: A Comparison." The similarities –cooperation, norms, international law—become problematic because of the differences in underlying assumptions and methodologies. These problems are multiplied in consideration of the F2C. The following related areas will be explored in the above paradigms: the role and power of norms, state-interest and cooperation, international governance, and the role of NSAs. In considering the F2C and Internet freedom at large, these areas will come into focus in ways dependent on the case and time-period examined.

Norms' power and role in shaping behavior. The interest in norms seems to lie predominantly in constructivists' court, having spent much of the 1990s discussing how norms are created, adopted (or not), and integrated into international institutions and structures. But norms are not the sole property of this approach, and others have discussed the roles and limitations of norms within their own frameworks.

Realists view norms, along with international governance and organizations, as epiphenomenal[1], connected to the fleeting whims of states that find them advantageous for short periods under particular circumstances. The role of morality is generally ignored. Yet this one-dimensional view of IR contains flaws inherent to the paradigm's assumptions. Barkin outlines the problem succinctly:

> …Waltz has come full circle to meet the Wilsonian idealists who provided the foil for both Carr and Morgenthau. Waltz's theory of the structure of power, without scope for morality, becomes static in the same way that theories of the structure of morality without power do. Neither pure realism nor pure idealism can account for political change, only the interplay of the two, subject to the assumption that morality is contextual rather than universal (337).

To this extent, realism becomes relevant to the study of norms when this critique is taken into account. Both Barkin and Carr, some four decades prior, come to a similar conclusion. Morality (for Carr) and

[1] Oddly, it is the critics of realism that use this term rather than realists themselves. See Ruggie (1998), Krasner (1999), Brooks and Wohlforth (2005).

norms (for Barkin) are molded by powerful states. In different ways, both contend that any discussion of norms in the absence of the consideration of power would be incomplete.

For realists, the rise and relevance of norms are largely dependent on whom the advocates are and the types of opposition they face. Norms exist for liberal and illiberal states, and for the weak and the powerful, but realists recognize how power predicates the likelihood of adoption and implementation. The relevance of the F2C could represent the epiphenomenal desires of liberal states, in keeping with two related elementary beliefs that liberal states share: the importance of political and civil rights and unencumbered economic enterprise.

Within the liberal paradigm, regime theory posits how norms and laws become widely accepted. Keohane repeatedly states among his publications that regimes are not a product of harmonious coordination of interests that promise mutual benefits to all parties, but are instead a result of a conflict-ridden bargaining process that attempts to maximize benefits and minimize losses for all parties. Norms like the F2C are subject to the same wrangling; states' interests are a powerful factor in defining the boundaries of any Internet freedom regime. Realists' concerns about power will make themselves evident when analyzing the bargaining process of the F2C and how powerful states and MNCs shape discourse.

An expansive understanding of the power of regimes indicates that they do not just depend on states for their content, but state behavior can also be affected by NSAs in significant ways not anticipated by ardent neo-realists. By its very nature, the Internet is a medium that must be analyzed in ways beyond formal state policy-making procedures. It will be necessary to study the feedback loops among states, individuals, and other interested parties, ICT companies, transnational civil society, and IGOs.

While in its early stages of development, an Internet freedom regime is predicated upon older Western human rights regimes and movements concerning civil and political rights, especially the freedoms of expression and the press. Rules and decision-making procedures already exist within formal institutions like the UN's human rights bodies and NGOs like the US's Freedom House. A violation of one norm does not indicate the weakening of an entire regime; instead these norms and rules work together to reinforce broader agendas.

The British school begins with the *a priori* and opposing assumption that international society is a given, and seeks to explain its purpose and how it is maintained. Compared to its American theoretical counterparts, the importance of norms is greatly increased even if not expressed using the same terms. Evans and Wilson (1991) state that "Though states do make power calculations, and from time to time act solely out of concern for power, in the main they are concerned with a variety of matters, not least their obligation, their standing, their honour and the propriety of their actions (339)." Given Finnemore and Sikkink's (1998) definition of norms—"standards of appropriate behavior for actors with a given identity (891)"—the concern of the British school about propriety and standing is entirely applicable. The divide in the school between pluralists and solidarists—in particular, how much society actually exists in the international system—is attention-worthy. Solidarists contend that there are common interests to all states beyond Bull's early contentions about things like security and the protection of property. The challenge lies in determining which states are included in a society that would support the F2C:

> Those campaigning in the name of solidarism need to be aware that they are advocating a particular type of solidarist international society, and not solidarism *per se*. They also need to add to their concerns about what values are shared and of equal concern with those variables that affect the stability of solidarist international societies: how and why are values shared, by whom, how strongly and with what degree of opposition (Buzan 2004 158).

Would Internet freedom norms simply be the reflection of a society that is based on liberal understanding of rights? By extension, would analysis be limited to members of that society, and that the violation of a norm from a state outside the West would not only be unsurprising, but expected? Despite these challenges, Andrew Hurrell (2007) claims the agreement on human-centered (rather than state-centered) norms is necessary in a globalized world (14), and this is only possible when powerful states can coordinate a response to global crises (295). Succinctly, the problem from the British School perspective would be how to determine the F2C and Internet freedom are important enough to generate general interest in their support throughout a cohesive, albeit liberal, international society.

John Boli and George Thomas in *Constructing World Culture* (1999) argue that there are distinct globalized cultures that in turn shape the actors and institutions that comprise the international system. Such an argument is similar to the concept of an international society. They continue that "…to an ever increasing degree, all sorts of actors learn to define themselves and their interests from the global cultural and organizational structures in which they are embedded (3)." Unfortunately, this convergence in

interests means that societies are more likely to come to conflict, rather than cooperation, over similar interests. Martha Finnemore contributes a chapter to the text about the Red Cross; she argues that a global culture supported humanitarian interests over the one that supported instead the unmitigated power of sovereign states. "Subsequent normative battles for human rights in the twentieth century have invoked similar principles of individual worth and universal humanity to protect people from state violence of all kinds (165)." In short, globalization means that control of Internet and the norms that surround it will be the interest of many powerful states that take on distinct global cultures: the West versus authoritarian states.

John Ruggie emphasizes the element of human consciousness and its role in international life. According to Ruggie, constructivism does not entirely dismiss the importance of material interests and their constraints on the system, but ideational concerns also drive decision-making. The most important contributive idea of constructivism is constitutive rules. Regulative rules stem from a need found in practice (driving on the right side of the road), whereas constitutive rules shape the game itself. Dominant theories of IR do not seek to explain why these rules become accepted at different points in time, and why they sometimes change (Ruggie 1998).

Constructivism does not dismiss the role of material interests on state behavior, but as a methodology in IR, it emphasizes the impact of norms, identity, and culture on behavior in the international system. For constructivists, at their fullest expression norms have a "taken for granted quality… [and are] no longer a matter of broad debate (895)." While variations exist, most authors agree that a norm's basic elements include: a) a sense of oughtness, appropriateness, or acceptability of certain behavior, and b) that it is accepted across a range of actors in a given system[2].

One of the successful ways in which norms can be internationally adopted is their adaptability. "Our contention is that norms diffuse precisely because — rather than despite the fact that — they may encompass different meanings, fit in with a variety of contexts, and be subject to framing by diverse actors (Krook and True 105)." This is akin to the adoption of universal human rights into new cultures by

[2] See Fukuda-Parr (2011) 123; Kleibrink (2011) 71; Krook and True (2010) 103-104; Legro (1997) 33; Nevers (2007) 55

framing them to be relevant to local contexts and political problems as Merry describes in *Human Rights and Gender Violence* (2006).

Sandholtz and Stiles's *International Norms and Cycles of Change* (2009) critique the dominant theories of norms because their proponents see them as linear rather than dynamic. The stages of the norm life-cycle neglect the dialectic of normative behavior resulting from how states interpret them (7). When a state's behavior seems to run in contrast with an established norm, the state must justify their actions by either convincing the group that the actions in fact comply with the rules, must attempt to establish exceptions, or argue for a new norm entirely. "As arguments modify norms, the cycle has completed one turn. The modified rules establish the context for subsequent choices of action and the precedents available in subsequent disputes (18)." While dialecticism of norms does not invalidate the study of an emerging norm like the F2C, it does highlight the need to appreciate the context of existing norms, the history of related technological developments, and regime type. Such concerns and gaps in understanding can be filled in by the alternative paradigms in IR that specialize in the interplay of history, identity, and the role of complementary norms.

Taken together, the adoption of norms is neither a harmonious nor a linear process, in which a problem is identified and a solution advocated by norm entrepreneurs, proposals presented on international platforms, and changes made throughout the state system through regimes and law. Rather, it is a conflictual process that is undertaken with self-interested actors, especially states, looming in the background. Norms are continually contested and shaped, first, by powerful actors who may attempt to change their interpretation to suit contemporaneous needs. This will mean that the belief in liberalism will necessarily frame their legitimacy and determine their spread. Second, states challenge them on the basis of the argument that they are the product of hegemonic interpretations of a common good that are really only common to but a few. Powerful states outside the liberal society will see them as alien products of the West, at best inapplicable to them or even detrimental to their people and interests. What is unique about Internet freedom norms will be the independent efforts of NSAs below the state and in international arenas. Demand for access or other manifestations of Internet freedom could bypass some of the processes outlined above, including the need for traditional powerful actors to advocate for new norms.

State-interest and cooperation. This area of theoretical inquiry at first appears to be dichotomous owing to realist and liberal interpretations. For the most ardent of realists, state-interest is the one-dimensional desire for the accumulation of power. Offensive and defensive realists disagree on how much power is necessary, but underlying both is the assumption that power is the means by which states attain their primary goal of security. Cooperation, if it occurs at all, is fleeting and depends solely on a rational calculation of benefits to be gained by a state associating itself with any organization, treaty, regime, etc. For liberals, the state's interest is defined more broadly than that of simple security, and that cooperation can occur given the right conditions and can change a state's preferences over time. Regime theory is one of the manifestations of this difference of each paradigm's underlying assumptions.

For the British school, state interest is not the starting point for analysis of the international system; rather they begin with a premise that an international society exists to fulfill states' needs. These needs, at minimum for pluralists, include stability and the limitation of conflict on one end of the spectrum, and at maximum according to the solidarists may include a cosmopolitan vision of world based on ideals of human rights. The British school does not question when and under what particular circumstance cooperation occurs—a phenomenon that is seen as relatively new by liberals (Evans and Wilson 342)—but tries to discover how cooperation and order can help states avoid the perils international relations. This focus especially concerns how to avoid war and conflict. In order to achieve this, states must care about their identity and the way that they are perceived by others within that society.

Strictly speaking, constructivism is not a paradigm but instead is a methodology that could exhibit "liberal," "realist," or any political or ideological bent; thus, it does not have a necessary set of assumptions about state interest and cooperation. Nevertheless, those who are constructivists generally are interested in when and how cooperation occurs. They study how interests and identity are created in the first place, and like the British school's view of society, see these as social constructions rather than phenomenal realities. Those who use this methodology often study the circumstances in which norms are introduced, adopted, and implemented—laws of war (Finnemore and Sikkink, Legro and Nevers), women's suffrage (Finnemore and Sikkink), humanitarianism (Keck and Sikkink), and development (Fukada-Parr). These studies seek to understand when and how norms will be adopted and implemented. The intersection of liberal and constructivist methods is at its strongest when one

considers that the study of regimes centers on the strength and adoptions of norms, and how those regimes are representative of emerging societies of like-minded international actors. These concerns are dominantly liberal in character. This does not preclude constructivists from studying why norms of sovereignty and preemption might in fact be adopted under a realist framework, but the former type far outnumbers the latter.

For the purposes of evaluating the F2C, a norm that in part conforms to liberal ideology of negative freedom, this study will assume that in most circumstances, states will care about the mutual benefits of cooperation more than relative gains. It will also assume that a normative consensus on the topic of the liberal international society is or will emerge in the near future. International society as envisioned by the British school is not universal, so the tenets of realism will become most apparent when states outside this society are challenged to conform to the standards set by the F2C and the Internet freedom regime. Regime theory will be able to structure the context in which the F2C is discussed, while constructivism will provide the tools to analyze how the norm develops.

International governance. For realists, the power of international law and the norms that exist within the system to explain state behavior face serious weaknesses. Rules, in whatever form, are both power-driven and epiphenomenal. The laws and norms embodied in organizations like the United Nations, for instance, have no bearing on foreign policy decisions made by powerful states today since they are reflection of an era that has long since passed. The desire to avoid another great power war is no longer at issue. When faced with new threats (or at least perceived threats) like terrorism, international organizations are not fit to deal with it and must be abandoned.

Yet for all the other approaches discussed, the power of norms, laws, and other forms of interdependence are cornerstones of their study. Liberals see norms as the building blocks of more complex regimes, which may or may not include formalized international organization that coordinate action among states and NSAs to accommodate state-interests, which go beyond the high-politics of security concerns. Nor does the abandonment of law or long-standing norms in one context or by one state mean that the system is in danger of collapse, but it is seen rather as a process of governance that changes according to need.

For the British school, their *a priori* assumption of the existence of international society rests on order. For pluralists like Bull, this order is embodied by things like international law and diplomatic relations. For solidarists this order goes beyond these codified rules and into the social constructions of norms and rules that are similar to the ideas expressed in regime theory. One of the weaknesses of this approach is the lack of recognition of precisely to whose order they are referring. As previously discussed, Evans and Wilson remark there is little recognition within the school of the imperialistic or hegemonic vein that runs through assumptions about international society. Those that follow the rules of law, however defined, are considered members of the society, and those that fail to do so are not (with perhaps some implication of barbarism).

Foot, Gaddis, and Hurrell (2003) address the problem of the extent of international society by reframing the issue of "order" and "justice" as articulated by the two branches of thought in the British school. Pluralists traditionally seen international society based around a rudimentary concept of order in an otherwise Hobbesian world, but they point out that even this view is in fact a moral supposition:

> More generally we should remember Weber's telling critique of reducing all politics to 'power politics', a move which reveals 'a most wretched and superficial lack of concern for the *meaning* of human action, a blasé attitude that knows nothing of the tragedy in which all action, but quite particularly political action, is in truth enmeshed (30).'

Sometimes order and justice conflict, and states choose actions that belie the pluralists' conception of order. The authors argue that the world today is no longer one that can "retreat" to pluralism because the problems that international relations face today are transnational in nature and not state-centric: ethnic conflict, environmental degradation, disease, etc. They recognize that while transnational civil society has increased exponentially, justice is a culturally contextual phenomenon. Regime theory supplements this problem by concentrating on particular problems—regimes will form around issues common to interested parties.

Underlying constructivism's focus on norms is an implicit assumption that some sort of cooperation, coordination, or society already exists, and that the question that constructivism asks is to what degree, in what ways, and which norms affect this system. The importance of identity is yet another of constructivism's foci that may impact the analysis of norms' effect on state behavior. Referring back to the concept of international society, identity will come into focus about who is or could be considered members of that society, and who effectively is out. This is especially true of regional organizations, but

the membership to an Internet freedom regime may hinge on whether the state identifies with the liberal tradition in general.

For the purposes of this study, there will be an assumption that norms and rules have lasting effects on state behavior and identity, and that despite the anarchical system, order does exist within the myriad of organizations, regimes, rules, and norms. The effects of norms will be the least powerful in states that do not already abide by or belong to organizations that are related to Internet freedom, or are not members of liberal international society. This will be apparent in the case of states that view the norm as an infringement to sovereignty or threat to national security, as has been the case with infamous Internet censors like China and Iran.

Non-state actors. Realists view NSAs with a fair amount of skepticism, seeing them as having limited relevance to a state's fundamental interests. While they acknowledge that international organizations, terrorist networks, and individuals are actors in the international system, they do not matter when it comes to state-led decisions about national security. Liberalism's concentration on cooperation brings NSAs back into analytical frame, and particularly it is international organizations that facilitate coordination so states may pursue their interests together to reach outcomes that will benefit all involved. Regime theory facilitates the investigation of the interception of organization and norms, but sacrifices some of its internal validity by not addressing the other NSAs that are involved in creating order. Sandholtz and Stiles address this very fact, drawing a parallel between regimes and legislatures, that studying only regimes would be akin to studying only the legislature in a given state in order to find out why a particular policy is adopted. Transnational networks and domestic politics, topics much-explored by constructivists, help to fill in some of the holes of regime theory.

The British school is primarily interested in a society of states with the interests of order and law. In fact, as Evans and Wilson report, Bull's early writings were leery of international organizations and their power to interfere with the process of order amongst society, disrupting the process of balance-of-power politics. Other scholars in the tradition have seen these organizations as strengthening order. However, the problem lies with the implication that the only organizations that matter are the ones created by international society, and that society is composed of powerful states that can control international ideology in a hegemonic fashion.

When studying norms, constructivists pay close attention to the actions of NSAs. In their role as norm entrepreneurs, individuals help to create new agendas and bring them to the international arena. Success or failure of new norms depends on the ability of these entrepreneurs to persuade a "critical mass" of states to adopt norms as their own. Additionally, these entrepreneurs will operate on both the domestic and international levels, attempting to convince local politicians and using international platforms to advance their agenda. Some of entrepreneur's work is explicitly geared to increasing Internet freedom, for numerous motivations like human rights, increasing marketplaces, or foreign policies, while others will pursue increases in Internet penetration

It is my contention that the norm of the F2C is being developed from both above and below the state level. Norm entrepreneurs generate pressure in a top-down manner, compelling states from international platforms of IGOs or NGOs. The very nature of the Internet suggests that this process does not have to be the sole avenue of a norm's early life, and individuals acting transnationally can bring the agenda to the attention of the political world beyond traditional channels. In time, states may be called to be responsive to agendas they only had partly helped to create. Sandholtz and Stiles' recognition of the feedback loop process of norm evolution might even be strengthened by studying the F2C and norms like it. Particularly, states will no longer only have to be accountable to each other and the agreements they make about norms, but they will also have to be accountable to the transnational actors on the very platform on which they are attempting to regulate.

One of the strengths of this dissertation could prove to be to provide a way to tie NSAs into traditional British school and realist analyses, examining how organizations and individuals can have an impact on norm formation and state behavior. While constructivists have been best at considering the impact of domestic and transnational actors in their analysis, the inability of constructivism to explain who matters and why can be supplemented by these other approaches.

***

The theoretical frameworks reveal a basic dichotomy among these approaches concerning the actors that are deemed important and the type of interests those actors have. On one side, emphases on the state and power lie squarely in realism's court, but are also relevant for British school pluralists as well. In practice, constructivism lies at the opposite end of the spectrum, emphasizing the importance of

identity, ideas, and all types of actors in the international system. Those of the solidarist school and liberalism lie somewhere in between; they still recognize the importance of dominant states while identifying the power of international institutions and society.

No single approach would be sufficient to describe the process of a norm life-cycle or loop. Traditional modes of power interplay with new sources, creating a dynamic that no one framework fully captures due to the limits of paradigmatic thinking. Paradigms are useful tools to simplify a complex system, especially global politics, enabling scholars to focus on key variables that will aid in the prediction of political behavior. Nevertheless, such tools are limiting when attempting to apply general assessments to particular problems. The path to the F2C will use the insights discussed here, and by extension, may provide a model for those researching norms related to Internet freedom.

Human Rights and Internet freedom

The norm of the F2C faces two related challenges. First, it must grapple with the history and the natural inclination for illiberal governments to control ideas. Western governments have and continue to struggle with balancing security and freedom, a fact that can only further justify violations of the norm by a state that does not have this history. Second, states can claim the norm itself, and its forebearers, are simply the product of a hegemonic culture that is inapplicable to their political structure. These challenges can nevertheless be overcome, due in part to solidarists' insights regarding the scope of international society. Since illiberal states are already participating in global society, demands to loosen controls on access will mirror the trajectory of other freedoms. To make the argument that liberal norms are inapplicable to non-Western states is implicitly arguing that culture is static, a fact that few social accept.

An example of the difficulties in translating these rights lies in the experience about the relationship between the state and journalists that highlight the divide between solidarists and critics from the Global South. The New Information World Order (NIWO) was an effort by UNESCO in the late 1970s and early 1980s that challenged the perceived domination of Western media coverage of the Third World. Before the growing power of the Non-Aligned Movement (NAM) and the NIWO, recounts Theberge (1981), UNESCO represented an attempt by the UN to promote education, culture, and scientific achievement. By the early 1980s, however, UNESCO had become overrun by critics of the West. The

NIWO claimed that representations of the Third World were biased, negative, and monopolized by Western and thus imperial perspectives. Further, "The role of media in the West as watchdogs and critics of the government and other institutions are widely perceived as a luxury poor nations cannot afford (715)." The NIWO's mission was to support a state-centered effort to develop media outlets in the Third World that could be alternatives to Western voices.

Criticism of the universal approach of Western advocates regarding the media continues today. Freedman and Shafer (2010) criticize the recent "Model Curricula for Journalism Education" adopted in 2007 for being too universal in scope, ignoring the problems of non-Western academia and the "…scarcity of profitable media organizations to attract successful graduates and reward them with jobs that allow them to practice their new skills (136)." The model, adopted with the United States once again a member of UNESCO, rejects the findings of MacBride Commission Report of 1978, which in part formed the basis for the now defunct NIWO, which took the differences of the Western and non-Western states into account.

The controversy surrounding both the NIWO and the Model Curriculum for Journalism Education stems from the broader struggle with universalism and international society. Advocates of the Global South's perspectives are using cultural relativist arguments, that the hegemony of the Western culture and its vision of political rights are simply incompatible with the realities of their states and societies. Moreover, the pretense of universalism masks the domination of Western visions of world. Western advocates who were against the NIWO and later the Model Curriculum argue that Global South's criticisms stem from a desire to continue authoritarian practices. Arguably, there are two "blocs" regarding the formation of the Internet freedom regime and the F2C, with Russia, China, and other authoritarian states claiming that the state needs to control the Internet in the same of security, while advocates for freedom do so either for the sake of the expression and/or unhindered capitalism. For advocates of the F2C, the point of the media—professional or social—should be as a check on state power as expressed in the UNDHR (Article 19).

Cyber-Utopianism: Disentangling Scholarly Approaches to the Internet's Impact on IR

There seem to be no scholarly voices discussing the development of the norm of the F2C at the time of this writing, but the issue of the Internet's impact on politics and IR has an extensive body of

literature that grows daily. The topics they cover range from issues of state power, censorship, the role of MNCs, privacy, and authoritarian states' backlash against citizen-critics.

The origin of the Internet as it is understood today has some bearing on what follows. Analysis of its history is mixed and centers around two major topics. The Internet's development can be traced to US military demands during the Cold War. Both Rosenzweig (1998) and Blum (2011) describe the context in which the need for keeping mainframes connected in a time when nuclear war seemed imminent led to the development of new communications technologies. Centralization of the control of nuclear weapons was seen as dangerous because in the event of war because there was no guarantee of the continued survival of a particular location or persons. The Advanced Research Projects Agency Network (ARPANET) and related technology were developed, in partnership with the UCLA and MIT, to decentralize control of these weapons. These early days of the Internet were highly controlled and exclusionary. The origin of the Internet as a tool for the US military and its initial limited access to academic elites is often forgotten today by critics who claim it has always been an open, free technology.

Keohane and Nye's "Power and Interdependence in the Information Age" (1998) is a relatively early study of the role of the Internet and IR, and complements their work on regimes that began decades prior. They lament how commentators, like Henry Perritt (1998)[3], had already been overly optimistic about the role that the Internet could play for IR, particularly because they did not sufficiently consider "...the continuity of beliefs, the persistence of institutions, or the strategic options available to statesmen (82)." The state and other traditional actors in IR would survive the introduction of new technology, and at that time, three-quarters of the world's population had no access to a telephone, let alone the Internet. Nonetheless, the authors recognized that interaction between states and NSAs would be altered by the new technology:

> Earlier transnational flows were heavily controlled by large bureaucracies like multinational corporations or the Catholic Church. Such organizations remain important, but the dramatic cheapening of information transmission has opened the field to loosely structured networks organizations or *even individuals* (83). [emphasis added]

While they predicted that the Internet will not profoundly change the dynamics of IR as a whole, new power struggles would result among "…actors who cannot control one another by force (90-91)." Closed

[3] He makes the notable claim that "The Internet is Changing International Law," because it makes information related to international law and the work of NGOs more accessible.

states would struggle to balance the demands of a sophisticated market economy with maintaining control of the information to which their population has access (93).

Hanson (2008) takes up the discussion of authoritarian attempts at their control information and censorship with the case that epitomizes such problems: China and its Great "Firewall." He labels the problem as the "dictator's dilemma" because of China's attempt to control all types of content it labels as illegal, from pornography, superstitious beliefs, to any information that it deems a "danger" to state security (185). It has/had received support for these efforts from MNCs like Microsoft, Sun, Cisco, and Google (at the time) that comply with the state's demands in order to do business there (186). However, despite the Great Firewall and the compliance of MNCs, China's diaspora and informal Internet usage undermines the state's attempts to stop information flows. Ultimately, the author claims that the presence of the Internet in China enables its citizenry to be more democratic, and may in fact to help foment a revolution. Such a conclusion seems like wishful thinking, but is representative of some of the cyber-utopianism and technological determinism that persists in the literature even with evidence to the contrary.

Katherine Tsai (2010) examines the case of Google in China and how non-state actors are entering the field of creating international law. The article is an important source of data for China's rhetoric regarding its own acceptance as Internet freedom. For example, in 2010 *Xinhua,* a government-run newspaper claimed that "China's Internet is open." Additionally, the story of Google's exit from China shows some impact of Internet freedom ideals, at least on Google. Tsai argues that Google was disregarding its bottom-line in its advocacy for Internet freedom in China:

> While Google could have remained silent regarding the cyber attacks like other victimized companies, it instead vocally campaigned against Internet censorship. Google executives called for the U.S. government to prioritize Internet freedom in U.S. foreign policy, arguing that Internet censorship creates human rights violations and barriers to trade (408).

For Google's efforts to be successful, Tsai recalls the advice of Arving Ganesan of Human Rights Watch about the simultaneous coordination of efforts between states and non-state actors like Google, using diplomacy, trade policy, and "meaningful pressure," to encourage further lifting of restrictions of Internet use. Tsai misses the fact that as a "quasi-state", like any state, Google pursues its self-interest (profit), and the lengths it would be willing to take in the name of human rights would be directly limited by this

pursuit. Nevertheless, the very fact that China remains adamant that the criticism it receives for censorship is part of Western imperialism is a tactic that cultural relativists have been used for decades and mirrors the NIWO.

Theorizing about the persistent power of the state, Evgeny Morozov (2011) coined the term "cyber-utopianism," and his book, *The Net Delusion* seems to be framed to establish him as the leading scholar of Internet pessimism. He claims that the high hopes for the "end of history" and the adoption of democracy worldwide has been dashed by the persistence of authoritarian states and the resistance to democratic change in some former Soviet states. Cyber-utopians see the Internet as an emancipatory tool but fail to take account of both domestic and international power structures.

> Failing to anticipate how authoritarian governments would respond to the Internet, cyber-utopians did not predict how useful it would prove for propaganda purposes, how masterfully dictators would learn to use it for surveillance, and how sophisticated modern systems of Internet censorship would become (xiv).

In their drive for new markets and profit ICT MNCs are stuck in the position of helping authoritarian states maintain systems of censorship. If democracy promoters want democracy to flourish, they need to adopt "a more realist posture," and not be reliant on new technology to do the work for them. Morozov's commentary highlights how technology is simply a tool that can be used for "good" or "bad" things. Yet, his analysis, like most instrumental analyses, concentrates too much on calculating the resilience of exogenously given power structures in the face of those who see the Internet as a tool for democracy. By doing so, he ignores the more subtle changes with regard to norms and rights about the Internet. The struggle between authoritarian states and their citizenry over the use of the Internet makes it a contested space in which new ideas will emerge.

Moving from analyses of actors, three articles examined describe the nature of the complex relationship between domestic and international law, especially the role of jurisdiction. These articles range from 1996 to 2005 and demonstrate both the growing understanding of the nature of the Internet in general by scholars in addition to the highly dynamic nature of the technologies themselves. Knoll (1996) and Fogo-Schensul (1997) both cite the "Declaration of the Independence of Cyberspace (1996)," by John Perry Barlow of the Electronic Frontier Foundation. The document asserts that the Internet transcends traditional geographic boundaries and therefore the regulation of sovereign states and further requires new forms of international law. Knoll and Fogo-Schensul tackle the complications surrounding

the Internet's transnational nature versus domestic and international law. Fogo-Schensul compares the approaches of the US, Canada, and Germany to Holocaust denial that has been promoted on the Internet. The author blames the US for too heavily conceding to domestic free speech protections, even to the determinant to other states' domestic policies.

> Despite the Net's phenomenal growth, we cannot continue to leave human rights behind in a cyber-cloud of electrons. To the contrary, given the medium's unique potential, it is more important than ever to establish in international law the principle that cyber-racists are subject to the same restrictions under human rights instruments as their less technologically advanced cohorts (274).

Knoll uses a survey approach, discussing how in the face of these hardships, some early Internet companies like CompuServe (now defunct) and Deutsche Telekom censored content on their own servers in the face of demands from particular states.

The ICT professionals' frame of Internet freedom reveals itself in the story of the creation of Internet governance. Mueller (2002) describes the 1998 adoption of International Corporation for Assigned Names and Numbers (ICANN) following a conference in Reston, Virginia. "The Internet was different, however. It seemed to call forth an entirely new spirit for collective action. It had created a perplexing set of issues that eluded resolution by any one government or organization. There was no suitable legal or organizational framework in place (4)." ICANN was adopted under the auspices of stakeholders—the people and corporations interested in the registration of potentially lucrative domain names. "Indeed, the original creators of ICANN always attempted to distance themselves from the term 'governance.' They preferred to say 'technical management (7). '" The sentiment surrounding ICANN mirrors how some historians have discussed the creation of the Internet itself, as belonging in the realm of technological "wizards" who operate beyond normal political channels (Rosenzweig). This type of thinking may in part result in the cyber optimism/utopianism dynamic discussed by Morozov and did not anticipate the wrangling over Internet governance today. Robert Damanski's research into Internet governance presents that each view, anarchism and the assertion of sovereignty, are in fact poles on reality's spectrum. Like the dichotomy between cyber utopianism and cyber pessimism, both governance and rights are shaped by the pull among states, NGOs, human rights advocates, ICT professionals, and the public.

Yochai Benkler's *The Wealth of Networks* (2006) takes a holistic approach to analyzing the impact of the Internet on politics, economics, and society. Benkler argues that the Internet has the capacity to increase the quality of democracy in developed states and enable it to consolidate in developing ones. The shift from manufacturing to a networked information economy means that change has occurred in not only how markets operate, but how information is accessed.

> This new freedom holds great practical promise: as a dimension of individual freedom; as a platform for better democratic participation; as a medium to foster a more critical and self-reflective culture; and, in an increasingly information-dependent global economy, as a mechanism to achieve improvements in human development everywhere (2).

Benkler is careful not to be too optimistic, repeating that his analysis is one of potential rather than inevitability. Social networks based on ICT platforms can be more democratizing than commercial mass media, but he says that it is not a cure-all. Instead, policy-makers decide the degree of democratization that is possible, and readers have reasons to be concerned that there are several obstacles to overcome, especially the tendency of law to respond to "old, long after the new has come" (borrowing a phrase from Mill). It is more likely, for example, for policy to respond to the proprietary concerns of Hollywood and ICT companies as it has done for decades than to give up its concern over copyright and assist in the strengthening of peer-produced, crowdsourced marketplace.

Rosenau and Singh (2002) discuss identity and interest formation on the Internet and their argument can be viewed as a reply to those like Morozov: "If we merely focus on actor capabilities and take their identities and interests as given, as most instrumental and structural power versions do, the transformation being brought about by information networks is missed (12-13)." The authors argue that ICTs create new spaces of interaction in IR beyond physical territory. Essentially a post-modern argument, they claim that traditional top-down approaches to understanding power and governance are not practical in world that is "in a state of flux (18)," in which power is contested on multiple levels by actors who can be official representatives, informal actors stemming from NGOs, MNCs, or even individual advocates. They recognize the multifaceted nature of power, which blurs the lines between domestic, international, and transnational spheres of action. Such informal bases mean that the progenitors of new norms in IR can come from anywhere and dominant theories about norms are lacking an appreciation for these changes.

A study on the ties between socioeconomic status and the digital divide in the developing world present an important thesis of what to expect the impact of Internet diffusion to be on societies with preexisting economic inequality. Sujarwoto and Gindo Tampubolon's 2013 study on the digital divide in Indonesia presents two theories about how Internet access proliferates and ask which best explains it diffusion in developing states. The "normalization" thesis argues the Internet will inevitably become widespread and readily available to all due to improvements that make hardware cheaper and easier to use for digital immigrants. Yet, such a viewpoint misses the socioeconomic and cultural contexts in which the Internet is disseminated. Conversely, the "diffusion" thesis argues that long-standing social inequities are the best predictors of Internet diffusion and use. In the case of Indonesia, geo-spatial inequalities that already exist will be mirrored in the percentage of citizens who can benefit from Internet access, and through a feedback loop continue to deepen socioeconomic divides. Thus, digital access could be another divide among ethnic groups and classes in a given society (4). Although social stratification is not inevitable depending as it does, among other things, on state intervention to provide infrastructure and on an equitable social distribution of wealth and resources, it is likely to occur in its absence.

***

Two additional sets of literature illuminate the development of the F2C. Social movement theory, largely the home of sociologists and those who study political activism, explains how entrepreneurs relate to one another in their work to increase Internet diffusion and promote freedom on the web. Second, a look into public-private partnerships (PPPs) will discuss why certain entrepreneurs promote their use in ICT development and some of their pitfalls.

Social Movements and the Internet

Social movement theory have developed along similar lines to IR theory. The dichotomy between structure and agency is found in the assumptions of social movement methodologies. Either rational actors are placed at the center of analysis while assuming the existence of a relatively stable system or the social systems in place are the primary focus that in turn shape actors' expectations and goals (Buechler). Resource mobilization theory mirrors realism's assumptions of the rational pursuit of self-interested, political goals, and authors point out that the theory fails to address why certain movements are successful and some are not (Meyer). Breaking the dichotomy, political opportunity theory places the

study of social movements within the political context of their societies that shape the possibilities of recruiting and goals.

Alongside political opportunity theory, Park (2003) and Vicari (2014) both discuss hyperlink network analysis, a social movement theory that can apply to the study of such movements on the Internet. "A social network is a set of nodes (people, organizations or other social entities) connected by a set of relationships, such as friendship, affiliation or information exchange (Park 50)." Hyperlinks are viewed as virtual social nodes, and thus a virtual network can be studied in much the same manner, seeing websites as the unit of measurement that is understood to be representative of individuals, states, NGOs, and other types of actors. Hyperlinked network analysis represent individuals and or groups that have more formalized presence on the Internet rather than informal nature of relationships found on social media pages. While the ITU and Internet Society both have Facebook pages and tweet on a regular basis, I claim that the connections represented in the hyperlinked images that are found on the likes of WSIS's official homepage are representative of formal working relationships.

Particularly, "new ICTs have provided early twenty-first century social movement coalitions with new resources for mobilization, political opportunities and platforms for framing purposes, facilitating transnational mobilization, diffused strategies and polycentric protest events (Vicari 95)." Vicari studies the hyperlinked social networks that grew around the World Social Forum, and discovered that while the Internet enabled connections among many actors, international nodes appeared to be more intertwined than regional or domestic chapters of the WSF. Highly visible nodes made the forum identifiable and supplied "master frames" that could be replicated or interpreted among other chapters. Transnational civic engagement would be translated to local levels (downward scale shift) and domestic experiences would also help to shape the frames from below (upward scale shift). Interaction among nodes was more common among geographic bases, especially in the WSF's early presence on the web. She concludes that "Its online developing process shows that the WSF's emergence bolstered interaction at local and national levels and enhanced transnational exchanges on a more symbolic dimension (106)."

Turner (2013) and Schradie (2014) touch on the plethora of social movements that have appeared in recent years and have asked what role social media have played in enabling the Arab Spring and Occupy movements. The question swirling around these movements is their longevity given their

amorphous organizational structure. Turner and Schradie both point out that these movements have grown up around a marked dissatisfaction with predominant power structures, specifically "a rejection of parliamentary and representative politics, deemed as excessively corrupt and influenced by corporations (Turner 378)." Schradie credits the rise of a "Silicon Valley Ideology" embodied by the supremacy of the individual along with the importance of the free markets.

> The assumption is that we are all untethered individual Internet *users* instead of organizational *members* of political movements. In this framework, we make our own decisions about when and where to get involved politically, and we connect through digital networks, not through a top-down organizational bureaucracy.

Turner notes that presidential nominees who were commonly viewed to be anti-establishment, e.g. Ron Paul or Howard Dean, were early success stories of the ability to use the Internet as an alternative media and organizational platform.

> This evidence indicates that the Web lends itself to more radical and oppositional forms of campaigning, sometimes progressive, and often unconventional and extra-institutional. The most salient accounts in this matter emphasize the Internet's contribution to the fostering of new models of direct democracy by creating an environment where rapid institutional adaptation and experimentation are common. From my perspective, this hybridization can be considered a contributory factor to this new egalitarian radicalism (Turner 380).

Yet Schradie points out that such analyses, while important, are methodologically unsound due to a bias in case selection. By picking the most visible and widespread movements, the everyday and more mundane types of social movements, like those focused on Internet freedom and access in particular, are left out. Additionally, her research reveals that digital activism often requires the "'passé' forms of traditional grassroots organization" in order to get people to show up to causes offline. It might be that Silicon Valley Ideology and traditional social movements work together in the 21st century, mirrored in the hyperlinked social network theory, in which strong attachments, both online and offline, are present according to issue areas based on geography.

Public-Private Partnerships

Touted by the ITU and various cases in this study as an effective way to overcome the infrastructural challenges to Internet penetration, public-private partnerships (PPPs) are a relatively common if misunderstood public policy tool. PPPs vary according to the types of projects being pursued and according to political climate.

The World Bank's PPP's Knowledge Lab defines all PPPs as: "A long-term contract between a private party and a government entity, for providing a public asset or service, in which the private party bears significant risk and management responsibility, and remuneration is linked to performance (17-18)." They are undertaken with the understanding that a certain service is necessary to economic and social development of a given community but the free market is unable to develop them on its own due little prospect of short-term profitability. The financial risk is therefore is shared between the public and private sectors while the reward is shared among the participants (Hodge and Greve 2007). PPPs are commonly used in sectors like water and electricity infrastructure, roads and transportation, and healthcare. They are used in multiple stages of projects: design, building or rehabilitation, finance, maintenance, or even the operation of a given project over the long-term. PPPs can improve infrastructure development by increasing sources of funding, improving planning through private sector analysis, incorporating private sector experience for more efficient delivery of goods, and long-term investment and planning (Knowledge Lab 31). The World Bank discusses their pitfalls, including the most poignant for the F2C that as political administrations change, projects can change or die away.

PPPs can be the subject of politicization as well as a "language game." For example, the frame of "privatization" or "contracting out" is unpopular with some constituents, likely due to the idea that certain public services should not be subject to market demands. Instead, "alternate delivery systems" or PPPs are ways to frame joint projects in ways that do not raise the ire of some voters. "The Blair government in Britain is famous for putting an emphasis on public-private cooperation and on PPPs especially (Hodge and Greve 548)," as in the case with National Health Service hospitals. The preference for public stewardship in Britain is opposite from the necessary frames in the United States, where there is a general disdain for public intrusion into the previously private markets; broadband rollout is something envisioned to be a task for Verizon or AT&T, not the FCC. Additionally, the US has commonly relied on the municipal bond market to fund public expenditures, so it has little experience with PPPs compared to other states. A recent case in Virginia that used a PPP to expand a highway (both under budget and on schedule) highlighted that its success was due in part to having a dedicated PPP office. Even better according to Holeywell is to have an independent company like Partnerships BC run a

PPP, which acts like a “consulting firm,” that assesses cost, risk, and providing realistic timetables and budgets.

The WB’s Knowledge Lab also points out the usefulness of PPPs to address markets that face monopoly or quasi-monopolistic conditions. Instead of relying on government regulators—which are sometimes inadequate to overcome the abuse of market power—PPPs offer a direct alternative to service providers that may be costly or inefficient. In many cases in this study—Mexico, the Philippines, China, Russia, and Cuba—telecom and ISP markets are dominated by one player, typically a state-run, or formerly state-run institution that has market shares exceeding 50%, often reaching levels near 70%. Mexico has begun to combat the dominance of América Móvil through PPPs and other public policy measures, but other governments struggle, or appear to be content with, the dominance of one player.

Two studies published in 2013 examine the roles of PPPs in broadband delivery, exploring successful and unsuccessful examples first in the US and second internationally. Fortunato et al. look at the problem in the US, focusing on the digital divide between urban and rural communities. While access is approaching universality, a significant gap remains between customers who can enjoy state-of-the-art, or even standard broadband speeds[4] versus those that can only get subpar service. They surmise the problem:

> For instance, in 2000 the National Exchange Carriers Association estimated that it would cost $10.9 billion to upgrade the 3.3 million rural telephone lines that would not already be capable of carrying broadband by 2002. With such a high initial investment, private Internet providers are not able to recover their costs in a reasonable time frame. In short, there is little financial incentive for private companies to extend high speed Internet to remote locations. (163)

Additionally, there is an aversion to local entrepreneurship, with customers usually more comfortable with well-known providers. They study how municipal and PPPs broadband projects compared in effectiveness and customer perceptions in three rural communities in Maine, Pennsylvania, and Wisconsin. The results provided both qualitative and quantitative data showing that the projects were successful in multiple areas beyond the basic provision of broadband. This included increased community revenue streams, better public service with more consistent service while saving $6,000-$8,000 per month, educational outreach programs, and increased customer satisfaction. Nearly 70

[4] The FCC defines these as 25 megabits per second (Mbps) downstream and 3 Mbps upstream as of January 2015.

percent of survey respondents supported public or PPPs as ISPs. Their suggestions, in addition to overcoming the legal and educational barriers, included framing PPPs as limited ventures with the goal of going private. This last suggestion overcomes of the political bias that Americans show in the provision of certain infrastructure as will be discussed in its respective chapter.

Roetter looks at best practices of broadband projects globally, making the observation that the best projects include complementary actions among central government, municipalities, and the private sector, noting that governments can choose among policies that will effectively encourage or discourage further broadband rollout. While there is no one best practice, they claim the most successful projects involve "sustained commitments over a period that is much longer than the typical life of an individual government administration (622)." Common themes that governments can undertake in broadband policy include: making policy that encourages a competitive marketplace, pursuing mobile broadband, and investment in "commercially unattractive areas" through both the marketplace and PPPs. They note that while mobile broadband is a popular tool, it has its physical limits; when the number of users increase, speed and quality deteriorate. He also notes that governments can frame broadband in a way that sees it as a tool for the betterment of the economy and political services, and allow a "bottom-up" projects to "aggregate the supply of the services needed to support the capital-intensive build-out of broadband infrastructure (630-631)."

PPPs in this study take on numerous shapes, including explicit projects to increase broadband rollout in underserved areas to arrangements with ISPs and other private sector corporations to provide service to underserved communities through public facilities. Each project, as the authors suggest, will be representative of the political climate and goals of the government in the case.

***

In reviewing the discussions on the relationship between ICTs and IR, a basic dichotomy emerges. On the one hand, quixotic enthusiasm of the transformative capacity of the Internet has invited much critique. Realist analyses have revealed the persistent role of the state and its desire to reign in any independent sources of power and to exploit technology to its own ends. On the other, liberal analyses have shown the multitude of actors that have a hand in shaping policy, and that while state

power persists, it does not do so in a vacuum. Analysis of the normative development surrounding Internet rights and freedom is absent, and the role of the international society is left to be discovered.

Some insights from sociology can illuminate the development of the Internet within states and how demands are shaped on the Web. The digital divide is in large part predicted by existing inequalities, and threatens to perpetuate them without intervention from outside the market. PPPs are one of the ways in which the private and public sectors can achieve gains, but their success is not guaranteed. Social movement theory, like IR theory, has the ability to take into account both structure and agency, and has revealed that there are different types of relationships to be analyzed on the Web.

Chapter 2: Research Methodology

Klotz and Lynch's (2007) work informs the research methodology for this dissertation. Throughout their text, they emphasize that despite our best intentions to be impartial social science researchers, we are inevitably influenced by our values and beliefs. This study requires a general acceptance that the system of human rights, regimes, and norms are universally applicable regardless of regime type or culture. This position has powerful opponents and consequences for how the F2C is interpreted by states.

The study uses is a non-experimental, qualitative research design. As there are two hypotheses to be tested, two different methods will be used. First, discourse analysis will be used on a variety of actors to examine who the proponents for the F2C are and what impact they have in their fields. Second, a comparative case study will examine how the norm of the F2C has developed in each of the states examined, using process-tracing to track the development of the norm's impact on state policy.

Klotz and Lynch recommend that practitioners familiarize themselves with the various manifestations of discourse analysis, which looks at texts to demonstrate the existence or dominance of a particular understanding or "frame" of a norm or belief. In particular, a framing methodology is used when researchers want to explore something like norms and how "…actors construct meanings [which] broadens our understanding of both goals and means to include attempts to alter language in policy debates (51-52)." What frames exist regarding the rights surrounding the Internet, including the F2C, and are any becoming dominant and embodied in the *status quo*? Sources for analysis include states' archives, IGOs, and NGOs, press reports and outcome documents from international conventions.

Additionally for the F2C, discourse analysis includes blogs, Internet forum posts, and other forms of digital expression. These sources reveal countless frames of the concept of connectivity, access, and/or the F2C, and how each advocate frames the general problem in relevant local contexts. ICT professionals often express their opinions in optimistic language that reveals their view of the Internet as an open forum for the exchange of all kinds of ideas. Western states couch Internet freedom within broader ideas of civil and political rights, seeing the Internet as an extension of the struggle for freedoms of the press, speech, and assembly. ICT MNCs are motivated by markets and the drive for profit, but their advocacy tends to adopt frames that are appropriate to particular problems or contexts.

Authoritarian states balance the need to control their population in the name of security or protection with the need to be connected in a globalized economy. Each of these frames' particulars is dependent on political contexts and short-term events or crises.

Other theories and approaches discussed complement the framing methodology. While some scholars within the British school argue that studies might benefit from empirical approaches, Bull outlines in 1966 why the classical approach to IR, relying on perception and intuition and utilizing philosophy, history, and law are superior to limiting empirical approaches. He anticipates Klotz and Lynch's emphasis on the recognition that studies are often premised on the researchers' biases, a fact that Bull implicitly embraces and that I disclose above. The effect of international society on the question of Internet freedom in general and the F2C will be a reflection of the acceptance of these values and how they will benefit the community's core interests. Regime theory will be especially pertinent when analyzing the effect the norm has on the cases selected. How the norm of Internet access has been accepted in the cases is correlated to the wider acceptance of Internet freedom regime; particularly, characteristics like regime type, political economy, and their experience with liberal norms will be important.

Robert Yin (1984) discusses comparative case studies in terms of "holistic" or "embedded" methods of dealing with independent variables. A holistic approach discusses the independent variable as one phenomenon, while an embedded approach evaluates the "sub-units," of the larger phenomenon. By using an embedded approach, this case study will be more focused and will make comparing each case easier for the reader. Instead of tackling the problem of Internet access as a whole, I will investigate some of the key components found within the larger framework, including statics, policy, financial incentives, relations to NGOs, and more.

Process-tracing will be instrumental to proving that the norm of the F2C has an impact on selected cases. This involves looking at the development of state policy regarding the control of the Internet from its introduction over the course of its existence. David Collier in "Understanding Process Tracing" (2011) lays out that technique's benefits, which includes identifying new phenomena, evaluating causal claims, addressing problems "such as reciprocal causation, spuriousness, and selection bias (824)," and its ability to bolster the validity of small-N designs in the absence of other quantitative analysis. As this dissertation uses just nine cases, this technique would necessitate the description of the

"snapshots" of state Internet polices regarding infrastructure and citizen access and comparing them over time. Subsequent analysis would allow for the F2C to be placed within existing or new theoretical frameworks.

Cases

The cases selected for study of the first hypothesis include states, traditional norm entrepreneurs, and non-traditional norm entrepreneurs. The study of norms and norm entrepreneurs generally centers around advocates acting on international platforms like the United Nations or INGOs. These types of entrepreneurs are not absent, but are supplemented by those working regionally and transnationally.

It is my contention that the norm of the F2C is new and is being developed from both above and below the state level. The study of this independent variable poses a challenge. If indeed the general public is creating new standards for state behavior, how can it be measured? By its very nature, activism on the Internet and through social media might be difficult to pinpoint. Does "The Protestor" on *Time*'s 2011 cover of "Person of the Year"[5] have a face? For laymen, the Arab Spring seemed miraculous in that it sprang from relative obscurity to foment a revolution. The Occupy movements were often criticized for their lack of leadership and concrete goals because it is organized horizontally, some seeing them as even irrelevant. Instead, the importance of individuals manifests itself in multiple ways. Some individuals can serve as the face for organizations' efforts, articulating their own interpretations of freedom on the Internet and a right to access. Additionally, crowdsourcing is a type of direct democracy, contributing to the construction and implementation of norms on a platform that the norms are about. Hyperlinked networks are formal connections among INGOs, local organizations, and individuals. Looking at how individuals operate on their semi-autonomous platforms, observing the direct input of the public on state policies, and how local and transnational movements are linked are ways to tackle the question of how to account for entrepreneurial behavior not traditionally captured by normative analysis.

For the second hypothesis, select state cases will look at the norms' effects on state behavior, both in the development of their domestic policy, rhetoric, and actions in international forums. Three archetypes have been adopted for the study of cases that are borrowed from the Freedom House's outline of Internet freedom: "Free," "Partly Free," and "Not Free." This parsimonious categorization is

[5] The image, pointedly, is of a woman covering her head and face.

based on a score ranging from 0-100 on three measures of Internet freedom: Obstacles to Access (25 points), Limits on Content (35 points), and Violations of Users' Rights (40 points). Countries that are labeled as Free receive a score between 0-30, Partly Free 31-60, and Not Free 61-100. States within these categories vary greatly, but these differences will highlight how differences in size, infrastructure availability, and culture will affect how the F2C is interpreted. Freedom House places greater weight on popular topics like censorship and surveillance, yet, infrastructure development and government control of ISPs are also important indicators of if and how citizens can use the technology.

It must be acknowledged that the choice of Freedom House's rankings is not without its problems. Nils Steiner discusses the reputation for bias that the NGO garnered in the 1980s. Academics suspected that its freedom rankings were skewed towards US allies, despite suspected cases sharing characteristics with states that were ranked lower. Part of the problem was methodology; until 1988, coding was conducted by one person using a checklist. Raymond Gastil's judgment was the only criterion and much like a grading rubric, it seemed to leave "a lot room for motivated reasoning." Steiner concludes that between 1972 and 1988, there was indeed bias, related to both the methodology and political context.

Today, Freedom House's coding is more sophisticated, with measures for both main aspects of democracy—institutional and ideological—and a series of subset questions that feature an ordinal scoring system. *Freedom on the Net* works much the same way, with a series of questions for each of the elements of Internet freedom: Obstacles to Access, Limits on Content, and Violations of Users' Rights. The US has been a leader of Internet development, governance, and ideology, and while the changes in coding are used in the country reports, the potential for bias remains. Polity's Data Set will be used as secondary commentary on the status of each case, though the Center for Democratic Peace does not directly test Internet freedom.

Nine cases have been selected for study, three from each of the categories. More than three regions would be a monumental task, and so for practicality's sake, this study limits itself to three regions and nine cases. Each case has been selected for its representativeness of similar states in their respective category, while across these categories the cases are meant to be in some way complementary to one another. This is a difficult task because as with any case study design, the

inevitable unique characteristics of each case are impossible to ignore. Despite the variety, patterns emerge that can predict how and why each state falls into each category and how they respond to the pressure to conform to global norms.

The United States is the understandable case for the liberal states that fall within the first category. With a constitution and ideology that enshrines liberal values and a foreign policy rhetorically in line with this image, the US exemplifies other Western states which have similar political histories and levels of economic development. Besides the European Union, the US is largest state in this category in several key aspects: population (ranking 4th in the world), annual GDP (1st in the world), and sheer physical size (3rd in the world)[6]. As the birthplace of Internet it would be important to examine how the state has dealt with increasing the availability of this technology. The US is ranked second in volume of Internet users with about 77 percent of its population using the Internet. Two other states, Russia[7] and China, have been chosen with this scale in mind.

Choosing the other two cases from the Free category is not as obvious. Most other states in this category mirror the ideological and cultural characteristics of the US and are European. To increase the internal validity of the investigation, cases outside the West illustrate that the Internet freedom regime and the F2C are not simply by and for the West, and would go far for the argument that the international society is more inclusive.

Latin America is a region that would meet the challenge of this task. For much of its history, it has been subject to the "talons of the eagle" typified by the Monroe Doctrine, the Platt Amendment, military interventions in the Caribbean and Central America, and American overt and covert support of regimes of questionable popular legitimacy throughout the 20th century. Much of the rhetoric from Latin America's political representatives after the fall of bureaucratic military regimes has been economic and political independence, stability, and sometimes overt anti-Americanism. Their legacy with human rights is mixed, so the direct influence of Western liberal norms is unclear. Three Latin American cases will be examined from each Freedom House category.

[6] See Appendix

[7] Between 2014 and 2015, Freedom House downgraded Russia's ranking from Partly Free to Not Free due to increased censorship and monitoring of citizens. I argue that it is an important case nonetheless to include in this study due to its regional influence and unique measures it has taken to assure access to its citizens.

Brazil has been selected from the Free category because of its size and regional importance. The state is the first of among three of the BRICS countries examined in this study, with a population of more than 200 million that is spread over 8.5 million square kilometers. It is also one of the most advanced economies of the region, having an annual GDP of $2.4 trillion that ranks 8th in the world. Like many other states that deal with infrastructure limitations, the state struggles with the capacity to bring access to regions with sparse populations. This problem has been exacerbated by significant discrepancies in wealth between urban and rural regions. While it has vacillated with Internet freedom measures in recent years, the adoption of the *Marco Civil da Internet,* a veritable "civil rights framework for the internet (Freedom House 2014 153)," promises to be one of the clearest and robust articulations of Internet freedom of the last few years.

Asia is the other region selected for this study. African or post-communist states are also relevant, but they were passed over for a region that encompasses the majority of the world's population and some of the most diverse reactions to the issue of access and Internet freedom.

Japan and the Philippines are the only cases in Asia that fit into the Free category. Internet penetration in Japan is relatively high at 77 percent of the population, while in the Philippines it stands in contrast at 39 percent. The main issue over access in Japan is excessive server loads, with populations that use both fixed and mobile technologies so much so that they periodically cause service outages. The Philippines' Internet penetration is hindered by near-monopoly status of its state-owned ICT. Recent political developments point to some ambiguity on how the Philippines views Internet freedom. The Cybercrime Prevention Act, while suspended, would have allowed the government and arrest people based on what they say and do online. Considering these developments, the Philippines is selected as a test of this study's internal validity, being the most superficially different than other cases selected in this category.

The Partly Free category contains a spate of nation-states from various regions, size, and political systems. Russia is the largest state in this category (see footnote 7) by several measures, including geographic area, population, and GDP per year. It also ranks 10th in the world for the volume of Internet users and enjoys high urban penetration of Internet access, yet only around 59 percent of their total population because access is especially limited in the remote regions of the North Caucuses and Siberia.

In addition to this issue, Freedom House reports that content is regularly monitored and controlled by the state under vaguely-defined laws against “extremism.” While Russia is a republic in name, the state's dedication to democratic values is questionable at best. The Putin regime has been effectively in power since 1999 and elements of both domestic and foreign policies can rightfully be seen as illiberal. Though weakened by recent economic sanctions as retaliatory measures after the invasion of the Crimea, oligarchic forces hold more sway over the political process in Russia than the people. The relative weakness of democracy is a somewhat common feature to states in this category, but it is not universal.

There are only several states in this category with readily available information in Latin America: Mexico, Venezuela, and Ecuador. Of these, Mexico is the largest with a population of over 120 million, an annual GDP of $1.85 trillion, and covering an area of almost 2 million square kilometers. Like Brazil, Mexico has recently passed legislation in line with the F2C—a Constitutional Reform Decree—that would increase overall Internet access and the quality of that access. Mexico faces problems of this policy implementation due to its ISP market. Its size, like the other states discussed so far, plays a large role in obstacles to access, but corruption and corporate interests also have a negative impact.

Indonesia is one the many possible cases in Asia for the Partly Free category. Other states include India, South Korea, Myanmar, and Thailand, each with distinctive geographies, histories, and cultures. India is unique case in many respects, and while geographically located in Asia, it is arguable that is too culturally and historically distinct from other cases from this region in this study, the Philippines and China, to be considered. Indonesia is the largest of the remainder of the cases on a number of measures, with the 5th largest population in the world at 256 million people, an annual GDP of $2.84 trillion (although South Korea exceeds this) spreading over 1.9 million square kilometers. It is also the state with the greatest number of Muslim inhabitants in the world, making up over 87 percent of the population. Analysis of the impact of human rights and Internet norms on this country promises to be enlightening in comparison to more authoritarian Islamic states like Iran.

China, as one of the world’s foremost challengers to Western hegemony is also the state that receives the most attention in the Not Free category. It is most populous state in the world, and like most cases in this study, its geographic challenges inhibit Internet access among its citizens spread across 9.6

million square kilometers. It is the final representative from the BRICS states with an economy ranked third in world with an annual GDP of $19.5 trillion.

As is well known, its economic success stems from its break from a state-planned economy to free trade and its support of burgeoning domestic free enterprise. It is arguable that China *must* have a high level of connectivity in order to remain competitive in global trade. It is ranked first in the world for the total number of Internet users, with an estimated 626 million in 2015—a figure that alone is almost twice the population of the US. This number is 45 percent of their total population, but likely more than 70 percent of their urban population, as their telecommunication infrastructure is concentrated within major cities and industrial centers. Nevertheless, the degree of political control it exhibits over its citizens is remarkable, including in the area of access, in which there is "poor infrastructure, particularly in rural areas; a telecommunications industry dominated by state-owned enterprises; centralized control over international gateways; and sporadic, localized shutdowns of internet access to quell social unrest (Freedom House 2014 194)."

Cuba is the only Not Free state in Latin America and is exceptional when compared to the other cases in this study. Although like China it is nominally communist, it differs on almost every other measure. It is small: a population of 11 million that ranks 78th in the world; a GDP of $121 billion that ranks 68th in the world; and an area of 110,860 square kilometers that ranks 106th in the world. Nonetheless, in 2015 it ranked with one of the highest score in "obstacles to access" (22 of 25) with most citizens having little possibility of becoming connected. Cuba is unique in that the service it does provide is mostly in the form of a government-owned and controlled *intranet*; unlike the Internet, this network is closed off from the rest of the world's websites. Access is limited to public places and is prohibitively expensive "with hourly connection costs amounting to 20 percent of the minimum monthly wage (Freedom House 2014 231)."

Being one of the most closed off societies in the world, Cuba's issues with Internet access make it superficially a difficult choice for the study of the F2C. Two reasons circumvent this problem. Cuba's choice to simply cut its citizens off from the world itself is worthy of study; what have been the economic and developmental consequences? It poses a significant challenge to the strength of the F2C and norms

of Internet freedom. Additionally and more importantly, the recent loosening of hostilities between the US and Cuba will provide an ample test of the strength of this norms ability to transform state policy.

The last case for this study is not immediately obvious. However, states in the Not Free category have been exceptional in how they have used the Internet to control their citizens. Iran stands out for these reasons. The state has a large population of over 80 million citizens, a powerful economy with a GDP of $987 billion, and one of the largest states in the region at 1.65 million square kilometers. Comparing Iran to Indonesia, as both states are composed of a majority of Muslims, and Iran being a theocracy, will reveal to what degree Islam or other non-Western belief systems is compatible with the F2C and other human rights surrounding the Internet. Iran is among many states in the Middle East ranked low in Internet freedom by Freedom House (Syria, Saudi Arabia, and small kingdom-states), but received much attention from journalists and scholars after the state jailed its users and tracking dissent online, especially after the "Green Revolution." After the election of Rouhani, there has been some loosening of these restrictions, but the case remains one of the strongest challenges to the efficacy of the F2C.

Considering the choices laid out above, this methodology will meet both of John Stuart Mill's joint methods of comparative study[8]. By using the method of difference within each category, in each case the norm of the F2C will have an effect in state policy. Each case is from a different region in the world that would mean that in every case, the state's history, ideology, political structure will be decidedly different, erasing these factors as reasons why the effect of the F2C might be the same. By using a method of agreement, the use of these three categories used by Freedom House will illuminate what factors cause the norm to be adopted. (Bleijenbergh)

***

This chapter has laid out the research methodology and data collection plans of this study. Framing methodology will explore the normative development of the F2C and Internet freedom above and below the state level, looking at official reports and recommendations by entrepreneurs in a variety of

[8] "If two or more instances in which the phenomenon occurs have only one circumstance in common, while two or more instances in which it does not occur have nothing in common save the absence of that circumstance; the circumstance in which alone the two sets of instances differ, is the effect, or cause, or a necessary part of the cause, of the phenomenon (Mill 463)."

contexts. Second, policy outputs from nine selected case studies will be explored to determine whether this norm has had a noticeable impact on policies and users' ability to access the Internet. It is predicted that regime type and political culture will have strong effects on how the state provides or regulates access and what other measures it takes to strengthen or inhibit the F2C.

Chapter 3: Framing the Freedom to Connect

This chapter will explore the first hypothesis that the F2C is an emerging norm in the international system that is being advanced by traditional and non-traditional norm entrepreneurs. Traditional norm-entrepreneurs are individuals who act through the vehicle of IGOs to convince states to enact policy changes and this is best viewed as a top-down approach. Non-traditional entrepreneurs act outside of the formal policy-making arenas, bypassing IGOs but nonetheless having a noticeable impact on state behavior. This chapter will identify these entrepreneurs and discuss why they are important in the fields of ICTs and Internet policy-making.

Some basic patterns follow: ICT professionals often couch their opinions in optimistic language of the desire for Internet openness and its endless possibilities; Western states rely on civil and political rights, seeing the Internet as a new manifestation of freedoms like speech and assembly and often a right in itself. ICT MNCs are motivated by markets and the drive for profit, but their advocacy adopt frames that are appropriate to particular problems or social contexts often using the rhetoric of human rights. Illiberal regimes have to balance the need to control their population with the need to be connected in a globalized economy. They have used a competing frame, cyberspace sovereignty or cyber sovereignty, in reaction liberal actors' demands.

Some entrepreneurs are working towards Internet freedom in general and may only touch upon the issue of access as part of a package of proposals aimed at accomplishing other goals. Additionally, the adoption of new norms is neither a harmonious nor a linear process; entrepreneurs work within a framework that is constantly evolving. It is a conflict-ridden process in which contemporary issues like net neutrality and corporate mergers are often the center of their agendas that temporarily shadow a larger agenda supporting human rights. Especially among the individuals and the NGOs that they create, there are networked feedback loops that support their complementary yet distinct agendas. Networked NGOs typically associate themselves with traditional norm entrepreneurs.

This chapter will survey the norm entrepreneurs and their writings and activities, starting with the UN sponsored activities, continuing with an assortment of INGOs, followed by the individuals working apart from these traditional platforms, corporate activities, and finally state representatives. It will analyze

how and why these entrepreneurs are making the arguments that they do, and what audience/impact they intend for their message to reach.

UN or UN-sponsored Activities

The World Summit on Information Society. The World Summit on Information Society (WSIS) is a UN activity that deals directly with Internet freedom and access. It is the product of a UN General Assembly resolution from 2001 (56/183) for the promotion of the distribution of ICTs in line the Millennium Development Goals (MDGs). Its origins lay in initiatives from the Secretariat, ECOSOC, and the International Telecommunications Union (ITU) and were first articulated in a 1998 ITU Plenipotentiary Conference by Tunisia to use the UN machinery to promote Internet freedom. The ITU was named as the organizer of the WSIS, which met in two phases: first in Geneva in 2003 and then in Tunis in 2005.

The purpose of the first session that had 11,000 participants from 75 countries was to establish a concretized statement of purpose. An "information society" refers to the integral part ICTs play in the economies and politics of advanced societies. All governments and stake-holders were encouraged to contribute to the Information Society and Internet governance in particular. Bridging the digital divide has been a pivotal goal of WSIS since 2003. Among the "action lines" discussed were the importance of governments in the policy-making process and the promotion of digital literacy. The Summit's outcome document connects its larger goals to infrastructure and access:

> **9.** Infrastructure is central in achieving the goal of digital inclusion, enabling universal, sustainable, ubiquitous and affordable access to ICTs by all, taking into account relevant solutions already in place in developing countries and countries with economies in transition, to provide sustainable connectivity and access to remote and marginalized areas at national and regional levels…
>
> **10.** ICTs allow people, anywhere in the world, to access information and knowledge almost instantaneously. Individuals, organizations and communities should benefit from access to knowledge and information. (WSIS 2003, 13-14)

Governments were directed to build PPPs in order to extend the rollout of broadband and satellite technologies (2G-4G) in order to encourage meaningful access. WSIS's concept of access goes beyond infrastructure to include 1) enabling citizens to access public records in ways previously difficult (akin to the "right to information"), 2) that government should encourage municipalities to use ICTs to improve local governance structures and democratic participation, and 3) that governments should provide publicly accessible spaces that would have free or low-cost Internet access.

The second session held in 2005 in Tunis had 19,000 participants from 174 countries and dealt with implementation of the agenda outlined in Geneva. Primarily, it was concerned with the dual problems of financing in addition to Internet governance.

The outcome document noted that older ICTs (telephone, radio, etc.) were developed by the state, and likewise a greater partnership between the public and private sectors would be necessary for the successful spread of the Internet. It is focused on the state but claims that corporations are "development enablers" and should be partners in the pursuit of the MDGs. The document emphasizes the crafting of PPPs with ICT providers so that Internet penetration can be increased and thereby foster economic and social development. Governments are charged with helping to construct infrastructure while simultaneously creating a policy environment conducive to profit.

Additionally, the Tunis Outcome highlights the need for multi-stakeholder governance of the Internet: "… with the full involvement of governments, the private sector, civil society and international organizations (6)." The F2C does not deal directly with Internet governance, but Internet freedom and governance are routinely linked by entrepreneurs. Each stakeholder is envisioned as having different tasks, such as policy-production (states) technical management (MNCs), and policy-coordination (NGOs). WSIS recognizes illiberal states' interests framed in the issue of national security by acknowledging problems like terrorism and cyber-attacks, but generally human rights and development remain priorities. It is suggested that the Internet Governance Forum (IGF) is the correct institution to deal with the tenuous area between security and openness on the Internet, but the IGF is a source of contention among Internet advocates in the private sector. ICT corporations and professionals are remiss at the idea of a multilateral international organization coordinating efforts to regulate the Internet instead of a decentralized entity, and fear it will lead to the loss of openness and freedom on the net. The IGF model has lost out to a revision of ICANN.

Every year since 2010, the WSIS has produced stock-taking documents reflecting the plans made in the Geneva and Tunis stages. Over a decade since Geneva, it is easy to recognize how the network surrounding WSIS has ballooned, much like the professional networks among NGOs and other individual entrepreneurs. In its latest installment, the WSIS+10 Outcome document of 2014 reads like many other assessments of the UN actions surrounding the MDGs—promise but little progress. The

greatest success has been achieved in areas like awareness and the increase in the availability of information; the “Partnership on Measuring ICT for Development” under the auspices of the UN Statistical Commission has provided the structural indicators of ICT development. The challenges remain far more numerous; most significantly among them are a recognition of the disparities in ICT development between North and South, and the digital literacy gaps between rural and urban, youth and the elderly, and men and women.

The WSIS Outcome document of 2014 is a reflection of the lessons learned from the previous decade about the types of digital divides that exist within states and the connection to equitable development. Meaningful access and human rights were reaffirmed as guiding principles. It also restates the principle that market structures must be competitive and states should use Universal Service Funds (USFs) to attract investment:

> …to connect and cover rural and remote areas with affordable Broadband information and communication infrastructure. To attract private investment, competition and adequate market liberalization policies to develop the infrastructure, financing, and new business models need to be studied and deployed, taking into account national circumstances (WSIS 2014 35).

As others from the Western perspective do, they explicitly connect such freedoms to broader universal human rights norms such as expression and association. By taking this stance from the very beginning of their mandate (WSIS 2003 2-3), WSIS leaves little room for competing ideas about Internet governance and what role the states could or should play in enabling access. It is clear that states should enable access to citizens either directly or indirectly by inducing ICT companies to invest in infrastructure and to be a boon to new companies. The UN’s take on Internet freedom is largely in line with the US and other Western states’ understandings of human rights due to the affinity for liberal norms.

In asserting that *all states* and other stakeholders should have a role in Internet governance, WSIS and the UN step away from the diffusion model the US had operated under since the Internet’s inception. Gjeltn notes that:

> Resentment over the perceived U.S. control of the Internet surfaced at the World Summit…In a direct challenge to the United States, the participating WSIS states resolved that "all governments should have an equal role and responsibility for international Internet governance," and they affirmed that states had a "sovereign right" to enact their own Internet policies (35)

WSIS would like to adopt a more equitable model of Internet governance than the US and ICT professionals had previously been accustomed. The WSIS is a reflection of a process that includes newcomers to ICTs, and it reasonable to expect that while they would desire some of the same goals as early adopters of the Internet, that it would be a reflection of states' desires to accommodate their own security interests. As previously stated, such a state-led model has lost to a new multistakeholder model to be implemented sometime in 2016-2017.

The International Telecommunication Union. The ITU was given direct oversight of the WSIS and its agenda because of its long history with the development of ICTs and their adoption on the global scale. It traces its roots to 1865 when it was International Telegraph Union that was the result of an international effort to standardize telegraph transmissions across the globe. It bears some resemblance to ICANN because its origins lay in the technical management of a developing transnational technology. Among the oldest surviving international organizations, the mission of the ITU has expanded over time to accommodate the adoption of new technologies like radio and telephones. It became the International Telecommunication Union in 1934 and a specialized agency of the UN by 1947. Because of its long history with emerging ICTs, the ITU is considered by the UN as perfectly poised to coordinate global efforts to increase Internet penetration and to deal with technical issues. From its earliest history, the ITU encourages the use of PPPs to develop infrastructure and enable the adoption of new technologies.

The ITU is made up of three "sectors" with different agenda that include the regulation of radiocommunication (ITU-R), standards of ICTs (ITU-T), and a development sector (ITU-D). The final sector is the most relevant for this study's purposes, and works much like other development programs by having a list of "areas of action" in various developing states. Buried within the list of eleven areas lies two of particular interest to the F2C: human capacity building and infrastructure technology development. The former aims to increase the capacity of the public and IT professionals to keep abreast of rapidly developing technologies through established programs, special projects, and partnerships with local IT institutions which provide learning opportunities. The latter seeks to increase infrastructure development in developing states and economies in transition through workshops, conferences, expert training, and the creation of tools and training guides. The ITU aims to improve broadband and mobile technologies, increase the prevalence of rural connectivity, and wants to anticipate how developing states can adapt to

newly developing technologies and networks. It is in the process of creating the world's first map of terrestrial fiber optics—key to understanding how the Internet is accessed by millions and how it might be made more efficient. The visualization of the inequalities of access is compelling, but the map remains tantalizingly incomplete.

Along with UNESCO, the ITU established an international conference and commission in 2010 in accordance with the Millennium Development Goals, and in September 2015, with the newly minted Sustainable Development Goals. The Broadband Commission for Sustainable Development takes the position, much like the World Bank will argue, that development and access are intertwined. One of the Commission's main goals is encouraging states to prioritize the development of broadband infrastructure through the use of USFs.

The ITU's 2014 Plenipotentiary Conference introduced the "Connect 2020 Agenda," which similar to many national broadband plans, set targets for broadband and other ICT penetration for the year 2020. It has four goals. First is increasing Internet penetration, with a goal of 60 percent of the global population being able to use the Internet (the current rate is approximately 40 percent). The second is increasing broadband penetration, a goal that signals an appreciation for meaningful access. Targets vary based on a state's level of development and include considerations for rural populations, gender, and people with disabilities. The third target is about sustainability, including considerations regarding environmental impact and cybersecurity. The final target seems purposely vague and noncommittal; "Innovation & Partnership" encourages market environments that would continue to allow ICTs to be innovative while forming partnerships among stakeholders.

Despite its apparent appeal, the ITU has vociferous critics. Both from the American blogosphere[9] and from MNCs[10], there are allegations that the ITU's actions are at best ineffective and even dangerous. Blue quotes a former ITU chief, Anthony Rutokowski, "The reality is that other than ITU radio spectrum management work, the rest is a worthless institution that does nothing more than flush money into the Geneva economy." She recounts that the ITU has close ties to Russia and Arab countries, intimating that the agenda of ITU that includes the greater involvement of national governments in ICT regulation is

[9] Blue, "Exclusive: ITU 'failed,' says former policy chief." (2012)
[10] BBC, "Google attacks UN's internet treaty conference." (2012)

really a mask for illiberal state interests. This relates to the accusations surrounding WSIS's agenda, which would take the Internet out of the hands of the ICT professionals and put it into the hands of states. The hint in the accusations that the UN is planning a takeover of the Internet at the dictate of anocratic and authoritarian regimes is extreme and inaccurate. Such accusations about the UN in general have been prominent since the 1950s (see the John Birch Society). As the ITU argues, it will not—and physically cannot—take actions regarding governance or development without the support of powerful states; such attempts would be fruitless without support. As Inis Claude argued many decades ago, the UN is a function of its member states, and seldom acts independently of them.

In a more significant critique, the BBC recounts Google officials' remarks regarding the conference that would set international standards on Internet technical specifications. Some of the "leaked" proposals concerned the issue of censorship and sensitive concept of net neutrality[11], and that there was the possibility that users would pay "tolls" for popular websites like Facebook and YouTube. Google officials remarked that the ITU, as a UN specialized agency, can only have nation-states as members, leaving the important and powerful players outside the formal decision-making process. Despite assurances as outlined above that WSIS and ITU works with both nation-states and various stakeholders, without the recognition that the state-centric system is outmoded in this field, Rutokowski's assessment proves valid. Brazil's vision of multistakeholderism and its influence upon the reorganization of ICANN shows how Internet governance necessarily differs from other transnational issues.

Human Rights Council (HRC). Other UN organs and agencies have made similar claims about the importance of the F2C and Internet freedom including the HRC and Special Rapporteurs on human rights.

[11] To clarify the concept of network neutrality and neutrality theory, Tim Wu compares the principle to the development of the electric grid. Innovation was possible because it treated all requests the same no matter the level of demand on the system. As a result, "The electric grid worked for the radios of the 1930s works for the flat screen TVs of the 2000s." Violations of neutrality can take on several forms including, blocking, "playing favorites" as is most familiar in this debate, or a lack of transparency on service parameters. Net neutrality is based on the premise that providers have a choice: use an exclusive, private network where one can discriminate against content and users or use a public network like the Internet. The choice of the latter has spillover effects to the rest of the system. Wu claims it is this problem that led to the spontaneous creation of the norm of neutrality (Wu).

Similar themes run throughout the data available such Special Rapporteur Frank La Rue's 2011 report to the HRC and a 2014 declaration. Each document recognizes that Internet access is fundamental human right that is connected to the realization other rights like the freedom of expression, equality, and socioeconomic rights. La Rue goes further, stating that Internet access can be means to achieve the impossible in illiberal societies; as a relatively cheap technology, the Internet can enable citizens to bypass restrictive, government-monitored and controlled media. He does note that the Internet also enables government to intrude upon their citizens' privacy in new ways (see Morozov), and calls on states to discontinue the practice. Both documents touch upon the issue of digital literacy and calls upon states to provide education, both in schools and beyond, to enable citizens to participate in the digital world in a meaningful way.

La Rue also notes that the digital divide would be perpetuated if states do not develop infrastructure and technology transfers plans. He states:

> Without concrete policies and plans of action, the Internet will become a technological tool that is accessible only to a certain elite while perpetrating the 'digital divide'…The Special Rapporteur is thus concerned that without Internet access, which facilitates economic development and the enjoyment of a range of human rights, marginalized groups and developing States remain trapped in a disadvantaged situation, thereby perpetuating inequality both within and between States (16-17).

These broad and perhaps loose conceptions of human rights are not without detractors. Maurice Cranston, in addressing the concept of the validity of socioeconomic human rights in 1967, wrote that they are philosophically misguided and politically distracting in that they "hinder the effective protection of what are correctly seen as human rights (164)," which are for Cranston political and civil rights. Moreover, many critics doubt the feasibility of the argument that the F2C could be seen as essential as expression or food. The criticism that the F2C and Internet as a right receives is generally based on this basic needs argument. In reality, as the movement to define security and development in contextual rather than absolute terms by people like Amartya Sen makes the view of access as right in the 21st century not only plausible but logical. As the entrepreneurs at each level of this norm's production argue, access is necessary for the realization of many other rights: political participation, education, and work. Perhaps the UN is framing it as a right so that it cannot be arbitrarily removed by governments.

Asia-Pacific Economic Cooperation. The UN is not the sole IO that acts in the name of the F2C. A regional economic forum, the Asia-Pacific Economic Cooperation (APEC), seeks to increase the

sophistication of the ICTs of its member states through its Development Steering Group. Among its goals:

- Expansion of networks to achieve universal access to broadband in all APEC economies by 2015;
- Development and dissemination of strategies to assist developing economies to deploy broadband networks;
- Making ICT more accessible to people with special needs;
- Development/Implementation of advanced technologies (e.g. IPv6, grid computing, and cloud computing) ; and
- Promotion of ICT applications for socio-economic development (e.g., green ICT, smart grids, disaster management, e-Government, e-Health and e-Education).

It is telling that such an organization, which straddles the line between East and West, will openly state that its purpose in promoting the F2C is socio-economic in nature. In a 2011 document, the working group outlines an infrastructure sharing plan that would enable less developed states to access broadband by 2015. Additionally, the 2014 Beijing declaration reaffirmed the importance of ICT development to economic growth and the importance of free trade generally.

World Bank. Though officially affiliated with the UN, the World Bank is not dependent upon the UN for either membership or funding. It has published annual development reports since 1978, and in 2016 the theme was "Digital Dividends," a study on the effect of the digital divide and what policies states could adopt to overcome it. For the report, the digital divide refers to several related but distinct phenomena concerning the uneven distribution of technology and opportunity based on demographic and geographic factors. Divides are most common among urban and rural populations, men and women, young and old, the wealthy and impoverished, and the educated and uneducated.

The World Bank reports that while some forms of technology are becoming diffuse, inequality is becoming greater. While nearly 70 percent of the bottom fifth of the world's population owns a mobile phone, they lack dependable access to clean water and electricity. "Not surprisingly, the better educated, well connected, and more capable have received most of the benefits—circumscribing the gains from the digital revolution (3)." The report reviews the economic benefits that an increase in access would bring through the expansion of markets to cyberspace and reduced information asymmetries. Beyond growth, the Bank's report also touts the political benefits, with citizens better able to track civil service malfeasance and curtail voter fraud.

The report recommends three steps that governments should take in order to bridge the divides and evenly extend the "digital dividends" of Internet diffusion. While the report maintains that the Internet is not a public good (since it is excludable), it argues that it is a club good which benefits anyone that can actually get online. "…public investment or intervention is sometimes justified where the private sector is unable to provide affordable access (27)." Like WSIS/ITU, the report recommends governments use tools like PPPs and USFs to channel investments into areas where the private sector fails to develop necessary infrastructure.

NETmundial. Hosted by Brazil in May 2014, the Global Multistakeholder Meeting on the Future of Internet Governance, or NETmundial was an initiative that was offered as way for states to address the issue of Internet governance. The topic is tangential to the F2C, but has become increasingly divisive among states that see US dominance as a challenge to their own power (as China and Russia do) or a threat (as Brazil does). The non-binding outcome document connected human rights to the Internet, arguing that they should be the same whether people or online or off. Importantly, it states that "Everyone should have the right to access, share, create and distribute information on the Internet, consistent with the rights of authors and creators as established in law."

The document also argues for a multistakeholder model of Internet governance (as opposed to a multilateral model) that includes governments, ISPs, ICT professionals, academics, and users. Such a model is also partially a challenge to the current mechanisms of government, which includes the private, American-based nonprofit ICANN, formerly overseen by the US Chamber of Commerce. Oversight was slated to be turned over to an international body in September 2015, but was delayed because the Obama Administration wanted "more time to work out the specifics (CNBC)." While the CNBC video claimed that such a move may put freedom of expression online in jeopardy, NETmundial argues that the desire to de-Americanize the control over the technical aspects of the Internet stem from the Snowden disclosures and concerns over privacy and security.

The NETmundial initiative's website contains information and links that substantiate the multistakeholder model. Authors highlight the connection between human rights universal access. A Coordination Council, organized among the Brazilian Internet Steering Committee (CGI.br), the World

Economic Forum, and ICANN, met in February 2016 to take stock of the progress of the NETmundial initiative and consider extending funding past the inaugural phase that ends in June 2016.

> The Council reviewed the activities and practices to date, noting how the crowdsourced nature of its endorsed activities, in particular the NETmundial Solutions Map and Collaboration Platform, have the potential to contribute to innovation in bottom-up engagement and information sharing in the Internet governance ecosystem.

The efforts to link individuals, organizations, and the private sector and the attention given to the bottom-up approach is evidence of how norms regarding the Internet can be developed in unique ways compared to norms of the past. There are many of the traditional actors—NGOs, states, entrepreneurs/experts acting from international platforms—as well, but the conscious utilization of the democratic potential of the Internet presents itself through this platform.

Non-Governmental Organizations

There is a diverse range of NGOs working on the right to access and Internet freedom. Some international NGOs are constructing the master narratives of Internet freedom, emphasizing the importance of balancing uninhibited innovation with efforts to increase Internet penetration. Others work regionally to tackle problems relevant within their political context. These organizations are networked together through formal associations epitomized by hyperlinked network analysis.

Internet Society. The Internet Society (IS) is an NGO envisioned by Internet pioneers Vint Cerf and Bob Kahn in 1992. They were among the inventors of the Internet who helped develop ARPANET and software protocols still used today. Cerf is also one of ICANN's founders and served on its board until 2007. The vision of the Internet Society is that "The Internet is for everyone" and works on a range of issues, including the open development of Internet infrastructure and technology education in developing countries. It also serves as a forum for the coordination of international efforts for both technical and practical information about the Internet and its potential, but most importantly, their mission includes: "Foster[ing] an environment for international cooperation, community, and a culture that enables *self-governance* to work (emphasis added)." Unlike the UN's vision, ICT professionals frame Internet freedom through the lens that its development and governance are best left to experts rather than policy-makers and bureaucrats.

Internet development is one of their key areas of work, but it differs in tone from UN approaches. While there is some superficial discussion in WSIS documents about the need for the Internet to be

localized and relevant to cultural contexts its overall approach is dependent upon government policy and encouraging outside investment. The IS insists instead that:

> The Internet works because its governance is distributed, open, inclusive, collaborative, and transparent. We work to keep it this way. Smart Development aims to strengthen this idea. It represents a positive, inclusive, and proven alternative to policies that can stifle innovation and network development. It offers an apolitical, non-interventionist method of building Internet connectivity and engagement that is accessible anywhere in the world and offers proven, cost-effective and replicable results (Internet Society).

In elaborating their approach to development, they emphasize the need for the Internet to be developed by locals, who may receive training on technical infrastructure, but efforts are only successful from the bottom-up. Development of the Internet should aim to be self-sustaining, which would imply that top-down models that depend on PPPs are at best temporary fixes to a long-term problem. The IS is wary of making general recommendations in regard to Internet diffusion.

Within the scope of development, one of the areas of work of the Internet Society is access, claiming that "Together we work to promote policies that sustain an Internet that's open and has a universally accessible platform for innovation, creativity, and economic opportunity." They concentrate on three aspects—infrastructure, user experience (human capacity), and cost—the latter being something mostly ignored by other entrepreneurs explored in this section.

In 2012 they conducted a global survey of 10,000 people in twenty countries about their use and attitudes towards the Internet. Their research revealed that 83 percent of the respondents (the vast majority of whom had Internet access) felt that access should be considered a human right. Eighty-nine percent felt that the Internet was important medium for the freedom of expression, and 60 percent felt that Internet enabled greater political participation and awareness in the country. Eighty percent felt that government had a duty to provide Internet access. While use among Americas was high (over 95 percent), the idea that access was a human right and that government has an obligatory role in its provision was less than the global average. States that are generally wary of government intrusion in the private sector would not be obligated to intervene on behalf of something that is seen as a luxury good rather than a public good.

World Wide Web Foundation. Founded in 2009 by another Internet pioneer, Tim Berners-Lee, the mission of the World Wide Web Foundation is to "advance the open Web as a public good and a basic right." As many NGOs working within states argue, the digital divide is a question about equality,

not only about access, but also employment opportunities, access to medical information, and the ability to have meaningful interaction with government in the 21st century. The Foundation has two main areas of work, affordability and the concept of "open data." Through its Alliance for Affordable Internet (A4AI), they have argued that the UN's guideline for affordability—that entry-level broadband should not cost more than 5 percent of a household's monthly income—is too high because of income inequality. While the 9th SDG envisions universal access should be achieved by 2020, the deadline is fast-approaching. As a result, the Foundation sees an even greater role for the state over the market. Such a position may be due to the fact that as a Briton, Berners-Lee is willing to envision a greater role for states than his American counterparts. "We believe public access options will increasingly be recognised as critical for accelerating the availability and uptake of broadband and achieving universal access." As some states and commentators are pushing back against zero-rated programs as a violation of net neutrality, the Foundation argues that they are essential to "connecting the unconnected."

Digital Divide Institute. The Digital Divide Institute is a fairly old NGO founded by academics, with its origins in the WTO conference of 1999 when its founder, Craig Warren Smith presented along with Bill Gates financial proposals to solve the problem of the digital divide. The Institute settled in Thailand's Chulalongkorn University and has mainly worked with governments and the private sector in Southeast Asia (Thailand, Indonesia, Cambodia, Vietnam, Bangladesh, the Philippines, and Nepal) because of a desire "…to affect the process by which two billion Asian citizens assume their status as a new global middle class."

They advise numerous stakeholders on the improvement of ICT development policies, which include providing corporations (Google, Microsoft, Yahoo) with input on how to improve corporate social responsibility and research and development, coordinating philanthropic efforts around the world (the Gates, Ford, and Rockefeller Foundations, etc.) with academia, advising governments on how to implement effective broadband projects, and presenting at IGO-sponsored events like the WTO, UNESCO, and ITU. The organization conducts five main areas of research in accordance with their work within states which includes how government policy affects infrastructure development, and how to improve collaboration between the public and private sectors for the development, maintenance, and improvement of the Internet. The Institute claims the most important area of research is ethics:

> Ethics: The most important research domain to establish the Meaningful Broadband model concerns ethics: How can a broadband ecosystem produce ethical impacts desired by the nation? To answer this question, researchers are developing a Meaningful Technologies Index, which measures and ranks technologies by their degree of meaningfulness.

The Institute is attempting to gauge which types of technologies would be the most helpful for achieving the stated goals of a particular society. Their use of the term "ethics" is different from the UN's emphasis on rights, and its application is far from universal. Perhaps as a consequence of the NGO's regional concentration in Southeast Asia, putting the F2C into the context of what local states need and want reveals the importance of framing rights though projects that would have local relevance. There is a lack of language about universalism and rights, and the framing of the concept of a divide and ethics may be most amenable in these states.

World Economic Forum. Based in Geneva, the World Economic Forum (WEF) was established in 1971 in order to expand the connections between private corporations and various elements of the public—government, citizens, academia, etc. Its mission is a kind of corporate responsibility, stating that "…an enterprise must serve… the interests of all stakeholders, including employees, customers, suppliers and, more broadly, government, civil society and any others who may be affected or concerned by its operations." Through high-level meetings, research, and digital collaboration, the WEF coordinates efforts on global issues much like UN, but offers itself as a neutral, apolitical platform whose chief concern is to "Build…an International Institution for Public-Private Cooperation."

"The New Internet World" a WEF report (2011) addressed the issue of how late-adopters view the Internet in addition to the issue of whether people around the globe felt that Internet access was a fundamental right. Five-thousand four hundred respondents from 13 countries answered questions contained in the survey[12], which included "an overwhelming majority (over 70 percent)" that felt access was a fundamental right. The study makes an argument that there is a somewhat homogenous Internet culture that is recognizable among the respondents regardless of "gender, age, education, and income groups" across the globe (29). Such a conclusion would support the contention that there exists, at least in some form, some articulated beliefs about the Internet that bypasses the formal policy-making process

[12] The Internet Society's survey was published one year later and covered a greater geographical range with more respondents.

of IGOs. Additionally, there is an emerging subculture on the Internet that is made up of late-adopters (especially in East Asia) that are more active and engaged Internet users than those of the past. One of the main arguments of the report is that: "Users want it all: they desire freedom of expression, privacy, trust, and security without viewing these as mutually exclusive (3)." Often freedom and security are seen as phenomena that are in a balance, whether in the digital world or outside it, but users across the globe overwhelmingly desire the Internet to be a place in which they can feel safe in expressing their opinions without the government invading their privacy while government also making the Web a secure place.

In addition to conducting studies on infrastructure and its need to be properly maintained and upgraded in the decades to come that will result in "hyperconnectivity" (see Data Driven Development 2014) the WEF in 2015 adopted the Future Internet Initiative. Like "Digital Dividends," it claims that the Internet is the most important driver of growth and human progress today, and the challenge today and in the future will be coordinating governments and stakeholders to enable the Internet to achieve its full potential. There are five areas of the Future Internet Initiative that were announced, including policy challenges (such as interoperability), cybercrime, the impact on business, privacy, and access. As to the latter challenge, the WEF is interested in combating the issue of the digital divide (although not so named) through public-private efforts, much the same as both the ITU and the Internet Society express. Their position is not explicitly based on any of the evidence as to what degree governments should be involved, but it is likely that any proposal would be less intrusive on the private sector than what the ITU and the WSIS would propose.

Smaller Initiatives. The Freedom to Connect Association is a US NGO that is comprised of diverse range of individuals, including a managing partner at a NY law firm, the director of US Institute of Peace, a journalism and media expert, and an ICT professional who had previously worked in other ICT-related NGOs. Its vision is based upon the UNDHR's Article 19, "that everyone "has the right to freedom of opinion and expression…regardless of frontiers." Unlike the other organizations explored in this section, its vision of physical access goes beyond having the infrastructure and technical expertise in order for a given population to be able to "plug-in." Instead, the goal of the organization is to enable access when governments attempt to block it by providing and educating individuals about covert technologies. Particularly:

> Freedom2Connect Foundation offers an antidote to this alarming trend. It helps fund technologies—ranging from encrypted chat rooms to secure story-telling apps—that give citizens and journalists the tools they need to circumvent government censors, protect identities and communicate freely online. The Foundation also seeks to educate ordinary citizens and journalists in the use of such tools, and to raise public awareness of the importance of an unfettered Internet for people everywhere (F2CF).

It studies these technologies and funds projects through grants in order for them to be brought to fruition. One wonders if this is a risky endeavor. Many of the issues surrounding censorship and privacy becomes a cat-and-mouse game; while well-meaning NGOs may promote technologies that could enable journalists and individuals to circumvent government censorship methods, it seems likely that new technologies could enable those same governments to break through encryptions, VPNs, and other dark areas of the web[13].

The Dynamic Spectrum Alliance is a global organization founded by companies interested in making more radio spectrum available to ISPs that depend upon it for wireless technology, thereby increasing capacity and therefore access. Among their stated goals is closing the digital divide, enabling the Internet of Things[14], and particularly alleviating the "spectrum crunch." Charter members include American, British, and East Asian companies, and today include members from the Caribbean, Africa, and much of Asia. The most celebrated projects on their website include television white space (TVWS), "…which generates a long-range wireless Internet connection by riding empty television UHF and VHF broadcast channels (Lovegrove)." As a coalition of technology companies, the organization straddles the concerns of consumers and businesses.

Mexico's Fundación Proacceso was founded by a private citizen, and views inequality and the digital divide as inherently linked. By providing access through community centers, the Foundation attempts to democratize access that at least partially bypasses the private sector. The training centers teach basic computer and Internet skills and have almost half a million users; the foundation is supported by Microsoft and Dell. Such NGOs are common in Mexico.

[13] "Despite all the openness of the Internet, there are still places you cannot saunter into on the Web. You must be invited. These are "darknets": exclusive peer-to-peer networks in which membership is based on circles of trust, whose activities are veiled from the general public (Newton 340)." They are mainly for illegal file-sharing of music and other media, but the potential for other politicized uses is obvious.

[14] A reference of the growing number of appliances and objects—everything from fitness trackers to refrigerators—that are connected through the Internet.

Other NGOs work toward Internet freedom in general, and fight for journalistic freedom and against censorship in particular. In Iran, Defenders of Human Rights Center published a report on a recently adopted Computer Crimes law in Iran, and how the requirement for ISPs to record browsing histories jeopardizes freedoms of the press and association. The Asian Human Rights Commission hosted an anti-censorship petition for Thailand. Advocacy for human rights is aided by the Internet, allowing watchdog groups to report on abuses or disappearances that go unreported by traditional media. "'Internet censorship curtails public access to information, academic research, press freedom, business competition, and simple human discourse,' the Bangkok-based freedom of information advocacy group says (AHRC)." The Philippine Human Rights Information Center reported on the Cybercrime Prevention Act in 2014, arguing that the law violated protections of free expression, due process, and equal protection. For instance, the punishment for the crime of libel is enhanced when perpetrated through electronic media. Other violations included mandatory "take down" orders issued to ISPs when material is judged to be in violation of the law, and unchecked surveillance practiced by Philippine law enforcement agencies (PhilRights). While not working for the F2C, there is evidence from the Global South that Internet freedom is not a solely Western or American initiative.

NGOs and civil society have been challenged in Russia in recent months, but the Glasnost Defence Foundation persists in defending expression and journalistic freedom on the web. Roman Zakharov reported on the blocking of a newspaper's website, Novaya of Gazeta v Sankt-Peterburge (NGSP) because the German webhost received a complaint from an unidentified, presumably government-connected person. The Foundation recently came under fire, as reported by Vladimir Golubev, as an organization "performing the functions of a foreign power." As such, they have been the victim of harassment, further claiming that their security can be assured only by making human rights violations public.

Not to be confused with the Internet Society founded by Cerf and Kahn, Internet Society China (ISC) includes ISPs, institutions, and individuals charged with developing the Internet in China. Unlike other NGOs in this arena, the focus is not primarily on civil rights, but on economic development and the coordination of efforts to make Internet policy and infrastructure more efficient. Unlike most NGOs, which are correctly classified as civil society in contrast with the state government, ISC is sponsored by the

Chinese government. Such an organizational structure is unsurprising given the unique nature of civil society in China, and functions as an intermediary among vested interests in Internet development rather than as a check on the state's power.

Individuals and Corporations

By the Internet's very nature, it is difficult to pinpoint which individuals are instrumental to the F2C regime. The disaggregated nature of the demands for increased and unhindered access through collaborative efforts like the signing of petitions proves that the power of users as an engine of change and a source for normative generation and spread. What makes this task more complicated is that the demand for access is embedded in more contemporaneous problems, like the use of social media for political activism.

Facebook and Google. Mark Zuckerberg, founder and CEO of one of the world's most popular social media platforms, has taken a vocal role in the advancement of universal access, the connection to human rights, and the provision of affordable or free Internet to help bridge the digital divide. As the face of the corporation in pursuit of profit for its shareholders, the authenticity of Zuckerberg's message is dubious, but he has made highly visible claims relating to the F2C and the company has undertaken projects in the name of these motivations.

In 2013, Facebook posted the whitepaper, "Is Connectivity a Human Right?" that would serve to justify one of its projects, Internet.org later renamed Free Basics.

> For almost ten years, Facebook has been on a mission to make the world more open and connected. For us, that means the entire world—not just the richest, most developed countries. We've made good progress, and today we connect more than 1.15 billion people through Facebook each month (Zuckerberg 2013).

Zuckerberg claims that the need to serve the unconnected may not be profitable for Facebook "for a very long time, if ever" but is nonetheless necessary. The Internet is fundamental for economic growth and employment and as such it has to be made more widely available. Zuckerberg argued that data plans, which the industry uses in order to build out infrastructure, are out of reach for many. But mobile Internet is a way for the industry's to "serve everyone," creating a vicious cycle. The sketch of the then-proposed plan included cheap or free data, applications that could be accessed for free, otherwise known as "zero-rated" apps, and the creation of non-data-intensive apps that would allow digital immigrants to take advantage of what could be made available.

The resulting Free Basics program has been rolled out in 36 countries, including the Philippines and Indonesia. It is not without controversy; observers argue that zero-rating apps like Free Basics violate the principles of net neutrality because choosing which apps could be accessed cheaply would be at the exclusion of many others. In February 2016 Indian telecommunication regulators banned the app because of its discriminatory nature (BBC 2016).

In March 2015, Facebook tested a technology that would beam Internet to the earth's surface from an unmanned aerial vehicle. Zuckerberg stated in his Facebook post: "Aircraft like these will help connect the whole world because they can affordably serve the 10% of the world's population that live in remote communities without existing internet infrastructure."

Project Loon, so named as a tongue-and-cheek recognition of the fact that many thought the idea ludicrous is one of Google's "X projects," the result of the R&D wing of its Alphabet Corporation. Its goal is to the bring 4G-LTE technology to inaccessible areas via balloons that would to deliver Internet through ISM bands, part of the underutilized radio spectrum of which most mobile devices make use. Unlike Facebook's FreeBasics, Google would be providing infrastructure rather than software. Each balloon would cover 80 square kilometers and would rely on the spectrum to relay traffic from cellphones to high-speed connections to the greater web.

The project is still in its early stages. In 2016, it seeks to establish links around the Southern Hemisphere to further test the reliability of these balloons. In February, the Google team tested a balloon autolaucher in Puerto Rico named "Chicken Little." "Portable autolaunchers allow us to move our whole operation to places that give us access to favourable wind patterns that can help us provide Internet connectivity around the world (Project Loon 2016)." A test has been carried out in Brazil, and memoranda of understanding has been signed by three ISPs and Google in Indonesia.

The frame of the project is couched squarely in the F2C court. While the Internet is commonly understood to be a "global community," the project laments that two-thirds of the world does not have Internet access. The switch from 3G capable balloons to 4G-LTE is that high-speed access is an important consideration for meaningful access. The video hyperlinked above discusses the benefits of access: primary education, access to doctors, helping farmers, and even small businesses. Such emphases are typical of Western frames of development discourse. As some of the commentary upon

the video illustrates, there is skepticism about the motivation behind the project and whether it is truly altruistic or profit-motivated. For both Facebook and Google, and likewise all MNC-supported NGO work, motivation stems from a combination of profit and corporate responsibility that serves to improve their public image.

There is further controversy about Project Loon. First ISPs like Indonesia's Telekom have argued that it has the potential to disrupt their marketplace as Google threatens to replace them. Such concerns might be unwarranted, as Google is working alongside rather than seeking to replace incumbent ISPs, and one of its aims is to bring access to currently underserved areas (Eyerys). Telekom's complaints resemble arguments made by AT&T regarding municipal broadband in the US. Second, Eyerys's authors point out that smartphone penetration in developing countries is uneven. Much of the population that will be served by these balloons do not own the necessary hardware to take advantage of the 10 Mbps connections.

While MNC's motivations are self-interested, framing the service within the scope of the F2C and human rights is evidence of the breadth of this norm, if not its depth. While Facebook and Google fail to mention WSIS and other hyperlinked networks within their project visions, these tactics could be used to avoid potentially controversial political associations. Their association and cooperation with local NGOs is evidence that they are not separate from these networks and are part of the feedback loop of the development of the F2C norm.

David Isenberg and the Freedom to Connect. David Isenberg is the creator of the "Freedom to Connect" conference and is one of the major entrepreneurs in the US, bringing together diverse institutions like the Media Democracy Fund, the Internet Society, Google, among others. Isenberg, who worked for AT&T from 1985 to 1998, gained notoriety for an article he wrote "Rise of the Stupid Network" that subsequently "went viral." It challenged the prevailing notion that any network, be it telephone or Internet, would have to be diligently managed by a telecom firm. His alternative premise was that new technologies could be managed from the bottom-up, and that there would be a gradual but inevitable transition from the older ICTs to the new, which would require a refocusing of telecom corporations. He made some recommendations in 1998 about what telephone companies could do to remain relevant but Isenberg still highlights the importance of "stupid" networks in 2015. Particularly, as the Internet Society

and ICT professionals claim, it is precisely the diffusion of power that enables the Internet to be so innovative and its development fast-paced. The intrusion of corporations or governments into the process would be detrimental to freedom itself.

The "Freedom to Connect" conference has a semi-annual meeting since 2005 that deals with the some of the issues of this dissertation. They state that the "F2C: Freedom to Connect provides a platform for understanding the social utility of infrastructure, for innovation, for creativity, for expression, for little-d democracy. The Freedom to Connect is about an Internet that supports human freedoms and personal security." Isen writes:

> The Freedom to Connect stands on three legs.
>
> The first leg is infrastructure, the rights of way, the poles and conduits, the wires and fibers and binder groups and cables, the electromagnetic spectrum, towers, antennas, receivers and transmitters, how they work, how their economics and business models work, and how the regulation of infrastructure promotes and impedes public telecommunications services.
>
> The second leg is the fundamental nature of the Internet, namely well-specified, well-understood public protocols, universally implemented with universal connectivity and open to all who meet its specifications.
>
> The third is the use of the Internet to promote bottom-up innovation and government of, by and for the people and to counteract anti-innovative vested interests and autocratic power.

Isenberg and the conference seem to be focused on US issues. In the latest conference in March 2015, topics were focused on net neutrality and the idea that the FCC could institute a government-run Internet (scoffed at by the attendees).

Declaration of Internet Freedom. The nature of the connection among these networks is embodied by an online petition from 2012 which is the result of hyperlinked social networks, and is authored by no one organization in particular. The document is here reproduced in its entirety:

> We stand for a free and open Internet.
>
> We support transparent and participatory processes for making Internet policy and the establishment of five basic principles:
>
> Expression: Don't censor the Internet.
> Access: Promote universal access to fast and affordable networks.
> Openness: Keep the Internet an open network where everyone is free to connect, communicate, write, read, watch, speak, listen, learn, create and innovate.
> Innovation: Protect the freedom to innovate and create without permission. Don't block new technologies and don't punish innovators for their users' actions.
> Privacy: Protect privacy and defend everyone's ability to control how their data and devices are used.

2012 is an important year for Internet freedom, with the realization that the Arab Spring did not produce the results initially hoped for, fights over piracy and net neutrality heating up in the US, and further limitations of users' rights in authoritarian states. The signers of this declaration include INGOs, regional NGOs, ICT professionals, academics, and human rights advocates along with anyone who wishes to sign from anywhere in the world (assuming the website is not blocked). It is unclear that it has been directly used to influence state policy.

State-led Initiatives

Generally speaking, the actions of states are rightfully seen as policy outputs and are the appropriate subjects of the subsequent chapters. Yet, at times states act as entrepreneurs by advocating for certain norms to be adopted by other states. Sandholtz and Stiles point out that the process of norm development is in no way linear, but rather is dialectical as states interpret norms to suit their contemporaneous needs. Looking at the speeches of state officials and to a lesser degree policy output is an important node for the perpetuation or the modification of norms like the F2C.

Then Secretary of State Hilary Clinton in 2010 articulated the phrase "freedom to connect" in a speech at the Newseum, a journalism museum in Washington, DC. She begun by addressing the Haitian crisis following the earthquake, and segued into the roles of information technology should have played in mitigating the chaotic response that met aid workers in attempting to bring relief to the area.

She argued that the development of the Internet and other ICTs was unprecedented, concluding that "information has never been so free." Yet connectivity is not an unmitigated blessing. Like any other technology, it can be used for good or ill, remarking that illiberal states often use the Internet as a tool for repression and censorship. "On their own, new technologies do not take sides in the struggle for freedom

and progress, but the United States does (3)." In addition to enabling the long-cherished American right of expression, Clinton argued that access is pivotal to economic growth and the freedom to practice ones religion. Disruptions to the ability of citizens to use the Internet must be combated by stakeholders—governments, corporations, NGOs, and the international community.

> The final freedom, one that was probably inherent in what both President and Mrs. Roosevelt thought about and wrote about all those years ago, is one that flows from the four I've already mentioned: the freedom to connect – the idea that governments should not prevent people from connecting to the internet, to websites, or to each other. The freedom to connect is like the freedom of assembly, only in cyberspace. It allows individuals to get online, come together, and hopefully cooperate. Once you're on the internet, you don't need to be a tycoon or a rock star to have a huge impact on society. (7)

Many of the NGOs and other entrepreneurs have pointed to Clinton's articulation of the F2C here as proof, or at least affirmation, of its global prominence.

Another prominent politician who has advocated for the F2C and Internet freedom has been Brazilian President Dilma Rousseff. After the Snowden disclosures, she and German Chancellor Angela Merkel went before UN General Assembly to introduce resolutions on privacy and condemn the US PRISM program. The circumstances and content of these discussions are analyzed in the section on Brazil.

Some states have enacted various constitutional or legal protections for Internet freedom that are not included in this study. These outputs are clearly intended for domestic purposes, but many entrepreneurs have noted these outputs as proof of the strength of Internet freedom norms generally. Estonia declared Internet access to be a right in 2000, and is viewed by Freedom House as a model for other states who which to achieve rapid infrastructure improvements. The Costa Rican Supreme Court affirmed the right of access in 2010, and Finland confirmed broadband access as a right in 2009.

***

This chapter reviewed the entrepreneurs shaping the various frames of the F2C. While familiar organizations the likes of ITU, the HRC, and the World Bank are active in advocating for Internet freedom and the increase of access, their efforts are supplemented by influential NGOs, MNCs, and state representatives. These actors work together in various ways, including through official platforms like WSIS and through the Web itself.

A review of the entrepreneurs revealed that access is more than the physical manifestations of the Internet like cables, satellites, or Wi-Fi. In addition, access takes on different dimensions dependent on the context which includes digital literacy, speed, cost, and in what way the state intervenes upon access, for good or ill.

Chapter 4: Free Cases

Free states have reacted proactively to the demands placed upon them by the F2C. Each of the selected cases has a positive association with civil and political rights and have extended protections of expression and association to the virtual world. Each of these states face challenges to the spread of Internet access and diffusion is largely the story of their ISPs. Although privately-owned, the concentration of power serves as a hindrance in both the US and the Philippines despite their otherwise considerable differences. However the Brazilian government and various stakeholders together have taken steps to assure the marketplace is diversified in that case.

United States

The US's relationship with the Internet penetration is complex. As its place of origin, policy-makers and ICT professionals have shaped the preliminary norms surrounding Internet freedom and the relationship among the government, private sector, and the public. Yet the case is challenged by geographic barriers and an inhibitive market environment. It favors incumbent providers and limits the role the state can play in the provision and extension of access to underserved communities. The ICT professionals' narrative grew up in the US and continues to shape Internet policies domestically and internationally as in the area of Internet governance. Additionally, the state has directly challenged norms of anonymity and privacy on the Internet through the PRISM program and the 2016 dispute among Apple, the FBI, and the Department of Justice. Disparate elements of the state work towards different ends in regards to Internet freedom and these breaches of freedom are often justified as temporary or as exceptions to otherwise appropriate rules on the Web.

Background

Since the 1970s, the US's identity as the world's indomitable superpower has been challenged but remains, as of yet, unmatched. As reported by the CIA's World Factbook, the US has a population of 321 million (ranking 4th in the world) and land mass that spans 9.8 million km^2 (3rd in the world). The state has an urbanization rate of 81.6 percent, with 7 major metropolises with populations approximately 5 million or more[15]. It has the third largest economy in the world with a $17.97 trillion GDP following China

[15] New York-Newark 18.591 million; Los Angeles-Long Beach-Santa Ana 12.308 million; Dallas-Fort Worth 5.603 million; Chicago 8.739 million; Miami 5.771 million; Philadelphia 5.571 million; WASHINGTON, D.C. (capital) 4.896 million (CIA 2014)

and the European Union. This equates to $56,300 GDP/capita, but is now second to China in purchasing power parity.

Looking at its ICT technologies[16], the US has 129.4 million landlines, ranking 3rd in the world; one phone is plugged in for approximately every 2.5 people in the country. The number of landlines is decreasing in absolute and relative terms, having dropped by nearly 10 million from 2013 estimates and causing the US to slip from 2nd to 3rd in the world. Yet, the figure escalates for cellular phones, with 317.4 million in the country, ranking 5th. Freedom House reports that 90 percent of US adults own a cell phone and 64 percent a smartphone. In total, there are 276.6 million Internet users in the US which makes the state second only to China in absolute totals but encompasses 86.8 percent of the population. Broadband penetration rates, smartphone ownership, and other ICT statistics are widely available through the Federal Communications Commission and through NGOs like the Pew Research Center.

The United States inherited much of its tradition of political and civil rights from England. Cherished rights like the freedoms of expression, press, and association were written into the Bill of Rights, but as in England, American interpretation of these rights has varied throughout its history. Struggles have centered on balancing the rights of citizens with the state's interests, especially security, a problem that other cases in this study also consider in regards to how they frame Internet freedom.

The line between journalism and media on the Internet is becoming blurred and can be subject to rancorous debate. Yochai Benkler wrote an extensive article, "A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate" in 2011, categorizing the ways in which the US government and traditional media attempted to dismiss or discredit the site and Julian Assange. The leak of the several hundred embassy cables in addition to the Snowden disclosures regarding the PRISM[17] program were viewed as problematic by the White House. While Wikileaks continues to publish, Assange remains under the protection of political asylum at the Ecuadorian embassy in London to avoid prosecution regarding perhaps overblown charges of sexual molestation in Sweden. Benkler illustrates

[16] CIA Factbook 2015

[17] The PRISM surveillance program was unveiled by NSA contractor Edward Snowden in June 2013. The program is designed to track foreign Internet traffic in the name of national security through the analysis of metadata. With the cooperation of major companies like Facebook, Google, Yahoo, and Skype and the legal mandate of Protect America Act, surveillance of email, chats, search histories, and other such digital communication became a tool available to the federal government. It has since received must criticism over its lack of oversight and broad scope. (Von Drehle)

the lengths that the US government was willing to go to discredit the "Networked Fourth Estate," and shows that the fight between media freedom and security is far from over.

A fruitful area for information on how a state deals with human rights is to review its periodic reports. The US has had a meaningful dialogue with the Human Rights Committee regarding Internet freedom and the F2C. The Committee is the UN treaty body responsible for the oversight of the application of the International Covenant on Civil and Political Rights (ICCPR) to states parties; the US signed the ICCPR in 1977 but did not ratify it until 1992. Initial reports typically include legal and judicial explanations of how the state already meets, or must endeavor to meet, the articles of the ICCPR. The following articles are applicable to this study and received close attention:

> Article 17.1.: No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> Article 19.2.: Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
> Article 21: The right of peaceful assembly will be recognized.
> Article 22.1.: Everyone shall have the right to freedom of association with others, including the right to form and join trade unions for the protection of his interests.

Many states' relationship with obligations under human rights instruments are instrumental in nature. They often will frame their actions that might appear as violations of human rights as either temporary aberrations or a necessity limitation of an otherwise broad concept. For example, freedom of speech is limited in the US to the likelihood of imminent harm it can cause; the same principle is often applied to international human rights obligations.

In its initial report, the US affirmed that US law guarantees the freedoms of expression, association, assembly, and privacy. The US frames Internet access as a complementary right to its body of civil rights, yet the idea of equal access to the media is not conceptualized as a right. For instance, the Supreme Court "…has stopped short of suggesting that there is a constitutional right of access to the broadcast media, and has never extended a guaranteed right of access or fairness doctrine to the print media (587)." At least according to US jurisprudence, the right to media such as broadcast television or the Internet has been seen as a "value added service" rather than something essential to full participation in political society. While such a view may have been reasonable in 1994 when Internet access was uncommon, today the same view might be considered outdated. As politicians' campaigns heavily use

social media and personal websites, as government services become available online, and as information on public policy becomes easily accessible from the Internet, the reasonableness of the hands-off approach by Congress and the courts is suspect. In none of the following reports does the US offer proof that it is seeks to change its position on seeing access as a right protected by law, regardless of the rhetoric used by US foreign policy practitioners.

The inviolability of correspondence is assured in the initial report with the exception of mail from overseas as argued in *US v. Ramsey* (1977). It is reasoned that government may search correspondence as one would search persons who physically cross borders for national security (526). Such logic can surely be applied to electronic surveillance under the rubric of transnational terrorism. Additionally, under article 17, the report reviews the judicial circumstances for obtaining wiretap warrants, their limitations, and the narrow circumstances in which people can be recorded without their consent (a "consensual conversation"). At this early stage, the US Privacy Act (1974) forbade "federal agencies from using information collected for one purpose for a different purpose (539)," and required consent and/or notice that computer databases containing bank records or credit scores could be shared. While not directly linked to the F2C, the lack of sharing of information was commonly cited as one of the missteps that allowed the 9/11 terrorists to hide in plain sight, which set the tone for the Patriot Acts.

The next available report was published in 2005. In addressing privacy, it reiterated the standards laid out in the US Privacy Act and the inability for agencies to share computer databases while touting the successes of the Patriot Act (2001) that allowed the intelligence and law enforcement communities to break down the "wall" between them. It also "…updated federal anti-terrorism and criminal laws to bring them up to date with the modern technologies used by terrorists, so that the United States no longer had to fight a digital-age battle with legal authorities left over from the era of rotary telephones."

The fourth periodic report focused on infrastructure development—including broadband—to Native American lands, stating that "[b]oth the Department of Agriculture and the Department of Commerce have programs to do so and have awarded loans and grants worth over $1.5 billion for projects to benefit tribal areas." Rural, tribal lands are among the most underserved in the country. The

US recognizes that in some circumstances the government must work to overcome marketplace failures to provide the services necessary to bring certain populations on par with average services in the country.

In the US, the changing standards on electronic surveillance can be traced from the benchmark case of the *Katz v. US* (1967) on wiretapping and privacy to the responses it gives the HRC on the Patriot Act and its implication for Internet users. The Protect America Act (2007) was cited in the 2012 document which extended surveillance performed by Foreign Intelligence Service Act to any person located outside of the US.

> 333. In 2007, Congress enacted the Protect America Act, P. L. 110-55, which excluded from the FISA definition of electronic surveillance any surveillance directed at a person reasonably believed to be located outside the United States. In particular, it allowed the Attorney General and the Director of National Intelligence to authorize, for up to one year, acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States if the Attorney General and the Director of National Intelligence determined that five criteria were met: (1) reasonable procedures are in place for determining that the acquisition concerns persons reasonably believed to be located outside the United States; (2) the acquisition did not constitute electronic surveillance as defined by FISA; (3) the acquisition involves obtaining the communications data from or with the assistance of a communications service provider, custodian or other person that has access to communications; (4) a significant purpose of the acquisition is to obtain foreign intelligence information; and (5) the minimization procedures to be used meet the requirements of the FISA. By the terms of the Act, a number of its provisions lapsed 180 days after the date of enactment.

The Act has been cited as the beginning of the PRISM program, which has created a maelstrom in the world of Internet freedom and governance.

In recognizing this, the Committee, in its List of Issues (LoIs) in 2013, asked the US to explain oversight mechanisms (CCPR/C/USA/Q/4) and to justify "roving wiretaps." The US response claimed that the FISC court not only authorized the collection of data, but oversaw the operations of the NSA, and that modifications to the law "enhance[d] judicial and Congressional oversight and protect individuals' privacy and civil liberties." Roving wiretaps allow officials to track the communications of individuals who often switched providers or means, targeting the person rather than the phone. Quoting Obama, the report claimed that such measures reflected the changing political climate that makes standards of the past inapplicable to the present. "…in the years to come, we will have to keep working hard to strike the appropriate balance between our need for security and preserving those freedoms that make us who we are…" The Committee has continually questioned the legitimacy and the necessity of the extensive measures the US has taken in the name of security, especially as they apply to Internet freedom. While

not directly connected the F2C, the US's policies on surveillance has led many to question its place as a leader of Internet freedom. The argument that the relationship between security and freedom are in flux due to terrorism and technological changes bolsters the credibility of policies in Not Free and Partly Free states like China and Russia.

US jurisprudence has continually shown that freedoms like expression, privacy, and association are balanced with security. No rights can ever be absolute, but the occasions when the state can rightly intervene into individual liberty are contested. The relationship is on a continuum, with the power of the state expanding in times of crisis, and contracting as public demand asserts itself. While the US pursues policies to increase access under the rhetorical frames of the F2C, the state simultaneously monitors access in the name of security in the age of sleeper cells and mass shootings. The most recent challenge (February and March 2016) to privacy was the FBI's demands that Apple create a backdoor to its own security measures to access the information stored on an iPhone used by one of the perpetrators of the San Bernardino attacks. While the FBI claimed that it cracked the phone's security without Apple's help, the episode illustrates how the demands of Internet users, providers, and ICT companies often clash with security interests.

The Internet in the US

Background. The Internet was invented in the US as a collaboration between academic ICT experts and the US military. ARPANET was built as a network of networks so that in the case of a nuclear attack there would be built-in redundancy of the US's networks that would enable communication between different locations even if a major telecommunications portal was destroyed. Blum recounts:

> They weren't only trying to get two or three or even a thousand computers talking, but two or three or a thousand different kinds of computers, grouped in all sort of ways, spread far and wide. This metalevel challenge was known as "Internetworking (42)."

Almost paradoxically, the military's academic partners at UCLA were largely part of the counterculture of the 1960s that was anti-establishment and pro-peace. The open attitude that emphasized sharing, decentralization, and "improving the world" survived the end of the decade and came to influence the ICT professionals' narrative that persists today (Rosenzweig 1545). Nonetheless, Rosenzweig insists that equating radicalism with the Internet's pioneers would be a mistake; instead, they were young faculty and

graduate students seeking an open *technical* community with a passion for ICT, not changing the world (1547).

Cerf, Kahn, and others succeeded in meeting the challenge, and ARPANET was later joined by other military and academic computer networks. While ARPRANET existed alongside these intranets (some of which persist today) problems arose because first, none of these networks were able to communicate with each other, and second, their use were relegated to academic institutions. The invention of TCP/IP protocols in 1983 changed this some of this dynamic and allowed computers on different networks to understand each other's data. It was the Tower of Babel in reverse in that the protocols granted the ability for networks to communicate rather than being wholly incompatible which each other. The transition to TCP/IP was gradual at first, but as Blum reports the number of autonomous networks increased exponentially after 1985, from 15 in 1982 to over 400 in 1986 (by 2011, there were 35,000 such networks). In the fall of 1985, 2,000 computers had access to the Internet, and in four short years it grew to 159,000.

Despite the ICT professionals' narrative that the Internet's early and best days were entirely driven independent of the state, the problem of exclusive availability of the Internet became apparent in the 1980s. The technology was expensive, and only the institutions that could afford to maintain the computing and infrastructure necessary to the Internet could enjoy the benefits. Larry Smarr, a UCSD professor of ICT, wrote a grant proposal in 1983 for the National Science Foundation, which became known as the "Black Proposal." It advocated for greater coordination among federal, state, academic, and business partners that would allow for increased access to these sought-after technologies. The Proposal lead to the National Center for Supercomputing (NSCA) at the University of Illinois, which helped to increase access across academia and produced one of the earliest web browsers, Mosaic. While the browser used protocols that today are outmoded, its inventors later developed Netscape, one of the most popular browsers in the early days of popular Internet access in the US, and its components (better graphics, a URL loading bar, and forward/back buttons) are used by contemporary browsers like Chrome and Microsoft's Edge. Netscape employees also developed Mozilla's Firefox, its "spiritual successor." One of the most popular web browsers today owes its existence to the NSF and the coordination of efforts among federal, state, and private enterprise.

Growing up alongside the spread of supercomputing in academic and military settings in the 1980s, corporate providers were working to tap into commodity services like e-mail, news reporting, forums, and gaming, which have become mainstays of Internet use today. Public access was made possible when the government lifted restrictions on Internet for commercial and private use, as a consequence of the increased capacity for telephone infrastructure:

> The increasing connection speed of T1 lines brought with it increasing demand, particularly from private sector businesses. By 1991, when all restrictions on commercial use of the Internet were lifted, the National Science Foundation (NSF) -- who from 1987 to 1995 helped the U.S. make the transition from the ARPANET to today's Internet -- had its entire network backbone connected to 45 Mbps T3 lines. In 1994, a year before the private sector assumed responsibility for the maintenance of the Internet backbone, the NSF upgraded the Internet backbone to Asynchronous Transmission Mode, 145 Mbps (FCC).

Between 1993 and 1995, adoption of the Internet in the US began to pick up momentum alongside the growth of personal computer (PC) ownership. In 1984, the first year the US Census asked about PC ownership, 8.2 percent of the US population owned a PC; 15 percent of those polled reported "yes" in 1989, 22.9 percent in 1993 and 36.6 percent by 1997. The US Census first asked about Internet penetration in 1997, and 18.0 percent of respondents had connections in their homes (File 2013). Within 15 years, the number of PCs in households jumped almost 4.5 times, and the market was subsequently ripe for widely available Internet access.

CompuServe, the earliest ISP, soon had to compete with America Online (AOL) which made at-home Internet access its business model. While CompuServe, AOL, and Prodigy had histories that spanned the 1980s such services were expensive. These included connectivity rates that would cost $10 for 5 hours of connection, and $3 for every hour after that (ForeverGeek). This model would eventually be replaced by AOL's monthly service plans; while more cost-effective, they still limited users to an allotment of hours online. CompuServe and others switched to a monthly service plans by 1996. While AOL began as a platform for providing email and other applications, it was also an ISP that would enable users to access the World Wide Web through browsers like Netscape and Internet Explorer. Internet speed, which is one of the most important markers of access's "meaningfulness," was maxed at 56 kilobytes per second (Kbps)[18]. AOL is still used today as a dial-up provider by 2 million US users who

[18] For example, a low-quality mp3 of 3.50 Mb would talk a half hour to download (Eha). Average broadband today would mean that such a download would take mere seconds.

have few other options (Pagliery). As AOL is dependent on extant telephone technology, it is one of the only options that remain to those where broadband is unaffordable, where contemporary high-speed ISPs have no viable marketplace, or "do not care to switch."

Speed and cost. Broadband[19] is currently the greatest measure of the sophistication of citizens' access. It is arguable, as seen in Finland, Costa Rica, and Estonia that meaningful access requires broadband. Its popular adoption in the US began in the late 1990s. Today, the FCC defines broadband as minimally 25 megabits per second (Mbps) downstream and 3 Mbps upstream[20]; for relative comparison, Akamai, however, reports that in Q4 2015 the average download speed in the US was 14.2 Mbps. When Pew (2013b) began collecting statistics in 2000, just 3 percent of US households had broadband while 34 percent used dial-up; in a little over 13 years, those figures jumped to 70 percent and 2 percent, respectively. While the US is enjoys speeds that far exceed most other cases in this study, it trails behind its Western counterparts; for example, France enjoys 43.8 Mbps downstream, Romania 69.0 Mbps, and Japan, 100.3 Mbps (Ookla). The 25/3 Mbps standard replaces a 2010 benchmark of 4/1 Mbps, something which at the time could be considered substandard.

The following are some observed speeds among large and small cities spread throughout the United States.

[19] "Today's common definition of broadband is any circuit significantly faster than a dial-up phone lines. That tends to be a cable modem circuit from your friendly local cable TV provider, a DSL circuit, a T-1 or an E-1 circuit from your friendly local phone company. In short, the term 'broadband' can mean anything you want it to be so long as it's 'fast.' In short, broadband is now more a marketing than a technical term (Newton 209)."

[20] Download speed and upload speed, respectively.

Table 1 Reported Internet Speeds in US cities
(testmy.net 12 April 2016)

City, State	Downstream	Upstream
Los Angeles, California	25.5 Mbps	6.8 Mbps
New York, New York	24.6 Mbps	7.6 Mbps
Chicago, Illinois	24.4 Mbps	7.9 Mbps
Anchorage, Alaska	18.0 Mbps	4.2 Mbps
Mountain View, Wyoming	8.6 Mbps	1.1 Mbps
Heyburn, Idaho	8.6 Mbps	3.1 Mbps
Navajo Utility Authority, Arizona	8.1 Mbps	8.1 Mbps
Hatton, North Dakota	5.3 Mbps	1.8 Mbps
Summersville, Kentucky	2.4 Mbps	435 Kbps

Major cities with populations in the millions enjoy the best average speeds while small communities in rural areas or tribal lands fare poorly, far below the minimum definition of 25/3 Mbps.

Freedom House reports that broadband penetration among US households is low among OECD countries, ranking 16th, while it had been 7th just a year prior. The FCC took note of this trend in its January 2015 report, stating that 17 percent of the US population has no access to broadband and rural Americans make up 53 percent of that total. Tribal lands are most adversely effected, with a total 63 percent of people living there lacking broadband access, and 85 percent of rural tribal lands lack high-speed (FCC 2015). The lack of broadband in schools is another statistic that sets US students back from their counterparts in developed states.

> Approximately 35 percent of schools lack access to fiber, and thus likely lack access to broadband at the Commission's shorter term benchmark (adopted in its July 2014 E-rate Modernization Order) of 100 Mbps per 1,000 users, and even fewer have access at the long term goal of 1 Gbps per 1,000 users (FCC).

Numbeo[21] provides statistics for broadband costs across all states in this study. The price for 10 Mbps downstream serves as the baseline for comparison. In the US, this speed will cost a consumer $50.03 per month, or 1.82 percent of the average net salary. The UN established a benchmark cost for broadband of less than 5 percent of a monthly salary, and so

[21] A website reliant on crowd-sourced data on consumer prices. For the United States, the number of contributors is close to 16,700. Each other case has at least 350 contributors.

while the US average cost is below UN standards, such a broad stroke does not take into account either income inequality or projected speeds versus experienced speeds.

National broadband plan. The US has adopted a long-term program designed to increase access, and the US case, broadband in particular. The FCC published "Connecting America: The National Broadband Plan" in 2010 after Congress mandated a plan be drawn up in late 2009 so that every American had "access to broadband capability." It is also a reflection of the F2C norms articulated by WSIS. This mandate emphasized the importance of last-mile access and community broadband, which reflected an appreciation for the socioeconomic causes of the digital divide. The plan has four nodes: robust competition, ensuring efficient use of extant infrastructure, funding through universal service mechanisms[22], and increased broadband availability at public locations. In addition to connecting broadband to other needs, like first responders and the monitoring of energy consumption, the plan includes two hortatory long-term goals. First, having 100 million US households with 100/50 Mbps speeds, colloquially known as 100^2 ("one-hundred squared"), and second creating the "biggest mobile network in the world." Such concerns reflect the realization that the US is behind much of the developed world in broadband deployment according to availability, top speeds, and cost. The report assured readers that the measures are not believed to cost taxpayers or ISPs extra money; instead, by expanding radio spectrum for mobile broadband use, new and increased business—and profits—were expected to result.

Internet penetration and geographic divides. The F2C is challenged by the geography of the US, but there are other factors at work. Both the US Census Bureau and the Pew Research Institute argue that demographic characteristics are predictors Internet access and use. As of 2015, Pew (Rainie) records that while 87 percent of adult Americans use the Internet that number declines according to two predominant factors: socioeconomic status and age. For example, this number declines to 78 percent for those earning less than $30,000 per year, and climbs to 97 percent for households that earn $150,000 or more. Less than half of households that earn $25,000 per year have Internet in the home, at 48.5 percent versus 94.5 percent for their richer counterparts. Educational attainment, as one of the markers of SES

[22] Similar to Universal Service Funds. Funds collected from telecommunications companies to increase service availability for low-income users, rural users, and community institutions. Companies may choose to pass on this cost to consumers.

also shows a great gap: those with less than a high school degree use the Internet daily far less than those with a college degree, 68 percent versus 97 percent in 2015. In some cases, this might be correlated with literacy. Rainine also reviewed reasons people gave for not using the Internet; while 34 percent of respondents stated they did not see it being relevant for their lives, 32 percent claimed it was the lack of know-how that was inhibiting use. Price and lack of availability were also significant reasons, at 19 percent and 7 percent of non-Internet using survey respondents. Sixty-three percent would need assistance if it were made available to them, while only 13 percent would not want to begin using the Internet. The digital divide continues to impair the economic and political viability of the Internet as tool for development.

Smartphones have enabled many Americas to access fast Internet in areas where fixed broadband connections are unavailable. Pew (2015a) reveals that among US adults, 64 percent own a smartphone but 10 percent have no fixed broadband service in their home. Fifteen percent have limited options for access other than a cell phone, and 7 percent of US adults have no viable options beyond a smartphone data plan to access the Internet.

This brief look at Internet access across a range of US geographic and demographic spectrums reveals a new problem: how to account for the variability in meaningful access for the country that invented the Internet. As some F2C entrepreneurs would argue, PPPs would be instrumental to improving the equality of access. Indeed, it is the ISPs that reign supreme in the US dictating who can buy—and afford to buy—reliable, fast service.

The FCC published its "2016 Broadband Progress report," as a reflection on the progress made to the long-term goals of the National Broadband Plan. Unlike other cases whose reports tend to be optimistic about how infrastructure rollout is approaching stated goals, the FCC is critical of the significant gaps that remain. While 10 percent of all Americans lack access to minimum speeds, that percentage climbs according to location: 4 percent of urban Americans compared to 39 percent of rural Americans, 41 percent living on Tribal lands, and 68 percent living on tribal rural lands. US territories have it the worst, with 66 percent lacking access to 25/3 Mbps and 98 percent of those living in rural areas in US territories. Chairman Wheeler's statement on the report is illuminating:

> When Americans increasingly rely on broadband for job opportunities, healthcare, education, public safety, and civic participation, but nearly 34 million Americans couldn't

> get high-speed fixed broadband even if they wanted it; when rural Americans are nearly ten times more likely than their urban peers to be bypassed by online opportunities; when 47 percent of our students don't have sufficient bandwidth at school to use the latest digital learning tools, we cannot say that we are meeting the standard Congress set forth. We have a moral and statutory obligation to do better.

Internet Service Providers

At this point, it would seem appropriate to attempt to gauge the availability of access by detailing the Internet's infrastructure—the nationally-operated US Internet backbones, data centers, networks, servers, storage, and applications—which make up the "tubes" of the Internet that allow it to operate. It would then be useful to compare such statistics to the other cases selected for this study. However, such information is difficult to come by, mainly because these records are not in any centralized database and this equipment is regulated by the ICT industry and is associated with trade-related secrets. While they could prove indicative of the quality of access in a given case, the market characteristics for ISPs is predictive of the level of access and disparities that persist.

ISPs provide the Internet to consumers' homes, businesses, and mobile devices by connecting their servers to the national servers or gateways that connect PCs and other devices across the globe. ISPs own the infrastructure and networks upon which the Internet is dependent, but they typically have arrangements that allow traffic to be shared on particular cables or lines. According to Freedom House, five ISPs dominate 70 percent of the fixed-line US market: Comcast, AT&T, Time-Warner, Verizon, and CenturyLink. Sixty million customers are served by these five companies, but such numbers are deceiving, as not every service is available in every location, even in urban and suburban areas. Most consumers actually have as little choice of 2 or 3 broadband providers, if any at all.

For example, in my own suburban town of Linden, New Jersey, 13 miles from Manhattan, three of five fixed ISPs—Time Warner, AT&T, and CenturyLink—are outside of the service area. The two major ISPs available that provide broadband are Verizon's FiOS service and Comcast's Xfinity service, each with comparable service plans. As of July 2015, entry-level broadband service of "up to" 25 Mbps/5Mbps (the minimum standard as defined by the FCC) would cost $44.99 and $34.95, respectively, while the fastest plans, 500 Mbps for FiOS and 105 Mbps for Xfinity, would cost $274.99 and $59.99 per month. These speeds are state-of-the-art, and consumers pay hefty sums for them. Yet they fall short of those that Finland seeks to guarantee for its citizens in the near future. The only other option for central

suburban NJ is a local ISP, Optimum Online from Cablevision, whose plans cost $39.95/month for 25/5 Mbps, and $94.95 for 101/35 Mbps. While it is comparable to other providers at lower broadband speeds, it simply cannot compete with FiOS or Xfinity for state-of-the-art connectivity. Service areas are determined at the discretion of the provider, and that this service is directly correlated to SES and demographic indicators. This location illustrates the limitations that result from little competition. Only one provides a service that would be considered sophisticated; more reasonable speeds that range from 50-100 Mbps downstream would cost a subscriber over $700 per year. For minimal speeds, the cheapest rate is $419.40, and the cost of this service is only likely to increase with perhaps marginable increases in speed.

Competition in the mobile ISP market is also hindered by a small number of players. Fierce Wireless reported that in Q3 2015, Verizon Wireless and AT&T had the largest number of subscribers amounting to 35.3 percent and 32.4 percent of the total market, respectively. Far behind are T-Mobile and Sprint with 15.7 percent and 14.9 percent, with US Cellular, C Spire, Shentel, and NTelos each serving less than 1.5 percent of the market. Unlimited data plans cost the average consumer between $75 and $100 per subscription, not including set up, the price of a smartphone, and other fees and taxes (Sprint), but average revenue per user ranges between $40 and $51 per month (Fierce Wireless). Anyone dependent upon wireless broadband might be forced into the higher priced plans or will have to limit their use. More problematic is the issue of the sustainability of such practices. Eli Noam (2011) warns that while governments are dependent upon wireless technologies to fill in the gaps of the digital divide, wireless broadband speeds and dependability will be adversely affected as the number of users grow, and that the ability to upgrade the infrastructure lags behind wired connections, "…fiber and cable are 20 to 100 times as fast as optimally projected 4G rates (475)..." While both governments and providers might see wireless as a the most efficient way to provide access to less economically appealing areas, Noam asks "Would rural areas accept for long the 4G mobile communications as their broadband platform–at a lower speed, higher price, and with less openness (481)?"

Public Provision of the Internet in the US

Public-private partnerships have been stressed by F2C advocates, especially from the UN, as a way to address problems of access but PPPs have largely been bypassed in the US. There are two main

ways in which the government assists in providing Internet to citizens. First, public libraries provide free access and training for citizens across the country. Yet this access is purchased from the ISPs at the cost to taxpayers, and funding for such public institutions continually decreases. Second, municipalities have attempted to provide their own broadband access directly to their constituents, but this process has had multiple legal, financial, and political setbacks.

Bertot et al. conducted a nationwide survey of Internet access and use in public libraries. A trend that began in 1990s with the spread of Internet use in general resulted in the fact that by 2011, 100 percent of public libraries were providing free access to their patrons. Over 90 percent offered free Wi-Fi. While these statistics seem promising, the rest of what the report has to offer is less optimistic. Sixty-five percent of public libraries report that they are the only provider of free Internet access in their communities, and 60.2 percent reported increased usage of workstations, which on average amount to 16.4 stations per library. With increased demand, 64.1 percent of libraries reported shortages of available workstations while simultaneously facing cutbacks in funding and hours. While they offer free access, the meaningfulness of that access is compromised because of low connection speeds; in 2012, 61.9 percent of libraries reported speeds of 10 Mbps downstream or less, with 6.9 percent of having less than 1.5 Mbps. While these numbers are better than previous years, by 2012 less than one third of public libraries had speeds greater than 10 Mbps downstream meaning that these institutions are still well under the new standard broadband speed of 25 Mbps. Taken together, the limitations in hourly availability, workstations, and speed adversely affect the meaningfulness of public access.

Some municipalities currently underserved by private ISPs have attempted to establish government-owned networks (GONs) through municipal broadband projects. Like infrastructure development of the past such as electricity and telephones, these projects are neither initially profitable nor viable for private enterprise to undertake alone, but nevertheless serve private citizens and corporate long-term needs. They face numerous limitations and barriers, including practical issues like financing and a lack of technical expertise, but more importantly, there is pushback from ISPs and lobbyists against the projects. What could become a meaningful public provision or PPP is largely absent in the US. ISPs contend that municipal broadband would adversely affect the private sector by reducing incentives for efficiency and competitive pricing and hurting the job market. Brodkin (2013) recounts the many legal

and policy barriers that ISP lobbies have been successful erecting that hurt PPPs in this area: laws that would require municipal broadband only to serve government purposes (Kansas), laws to protect private-sector jobs (North Carolina), and laws that require short-term profitability (Florida). There are dozens of other examples in Brodkin's reports, including Virginia, where one of the most successful municipal broadband projects, in Bristol, took place.

> In 2010, BVU added 388 route miles to its current 10Gbps fiber network, building out a middle-mile network to eight rural Appalachian counties thanks to a $22.7 million BTOP grant. Seven of those counties were classified as economically distressed; bringing high-speed broadband to those areas could be the economic boost they need (Fierce Telecom)

The rest of Virginia faces similar legal hurdles to that of other states, such that its municipal broadband providers must offer competitive rates to private ISPs, but Bristol's GON was grandfathered in before those laws came into effect. FreePress's 2005 report on the subject argues that ISP's arguments against GONs are faulty: municipal broadband is not overly costly, and that as with other "market failures," government can provide broadband to citizens who would otherwise not be able to purchase these essential services (Scott and Wellings 2).

A 2014 report by Allan Holmes reveals the fiscal and legal extents to which AT&T has gone to gain legal protections against municipal broadband. A municipal broadband project in Tullahoma, Tennessee met with extensive lobbying efforts to block the proposal. A Republican state senator remarked that "We don't quarrel with the fact that AT&T has shareholders that it has to answer to…and I believe in capitalism and the free market. But when they won't come in, then Tennesseans have an obligation to do it themselves." Instead, AT&T blocked the measures as a hindrance to the free market. An unidentified lobbyist remarked "On a scale of 1 to 10 on who is the most powerful lobbying presence in Tennessee, AT&T is a 12," and is evidenced by the millions of dollars the company has spent campaigning in Nashville and around the country.

That same year, AT&T submitted commentary on GONs to the FCC, asking that the FCC apply standards developed in the Telecommunications Act of 1996 that limited state assistance to encouraging private sector development of ICT infrastructure. Heimann, Philips, and Fink state that "AT&T shares petitioners' desire to ensure that all Americans, including, but not limited to, those living in and around Chattanooga and Wilson, have access to world class broadband infrastructure." While this rings of the

F2C, the representatives emphasize that the private sector is better suited to deploy new technologies and innovate in general, and that municipalities are not well-suited to upgrade networks on a consistent basis. While the commentary concedes that there are cases that the free market fails to deliver broadband, allowing municipalities to provide buildouts must come with "safeguards:" a right of first refusal, GONs would operate according to the same laws and regulations, and that they would receive no preferential tax rates. "Without these protections, there is a real risk that the deployment of GONs will harm competition and consumers by deterring private sector investment that otherwise would occur."

Brodkin reports on the continuing difficulties faced by municipal broadband projects (2016b). Efforts in Chattanooga, Tennessee to extend the broadband provided by its electric utility, for example, have been prevented by state law, as has been the case in 20 other states. State senators Todd Gardenhire and Kevin Brooks are a part of bipartisan efforts to overturn the law but face pressure from incumbent ISPs. While AT&T contends such schemes would put them at a "competitive disadvantage," politicians warn that we must not "…fall for the argument that this is a free market versus government battle. It is not." While the Tennessee House Speaker Beth Harwell is not supportive of project as of yet, she argues that if the market fails to deliver to the rural areas, "then I do think it becomes necessary for the public to enter [the market]…" Why Harwell is willing to give the market more time than it has had already is not explained in the article. Instead, Brooks argues that "This is about Tennesseans having access to the 21st century."

GigU, a project maintained as a collaboration between research universities and local communities, released a report in 2015 regarding the viability of municipal broadband. Grant Gross of *PC World* magazine initially misleads readers describing municipal broadband as an unviable option for unconnected communities because of long-term costs and inefficiency. The bias from an industry-related magazine aside, what the report and the article reveal is an alternative type of public-private partnership. Publicly built municipal networks can be subsequently *leased* to ISPs. Such arrangements are not unusual in other industries, in which a municipality or state may subsidize corporations in order to encourage growth. Such a model would undoubtedly be appealing to the tech industry, but does not circumvent the problem that ISPs are primarily motivated by profit; if such an arrangement could not promise to make money, it would be unlikely that it would take place.

Challenges to the Norm of the F2C

The increasing availability of publicly provided high speed Internet connections through libraries is among the obvious ways in which the US complies with the spirit of the norm of the F2C. As paltry as the offerings at these locations at times can be, they reveal the power of the idea that everyone is entitled to be connected, and that government should help to provide that access. The fight over municipal broadband projects illustrates the difficulty of state involvement in the provisions of services normally provided by marketplace. Such a limited view of who should provide access results in infrastructure development driven by the pursuit of mainly short-term profit. In this case, the American affinity for private enterprise and the pursuit of profit trumps the ideologies of equality and the enrichment of political rights in the 21st century.

ISPs' pursuit of profit has led to two major controversies in the realm of access. First is net neutrality, a term that describes efforts to control which types of traffic should receive priority and that the sources of this traffic should pay premium prices for that privilege. The concern, in short, is that ISPs could speed up or slow any website according to their ability to pay and the amount of traffic they use. Second are the mergers among major ISPs in the US, first the attempt between Comcast and Time-Warner, and second, the successful 2016 merger between Time-Warner and regional ISP, Charter Communications. The debate continues to rage about whether increased competition or reduced economies of scale would give the market the impetus to increase efficiency, speed, and customer service.

Net Neutrality. At first glance, the controversy over net neutrality in the US is unrelated to the F2C. In the absence of net neutrality, "…ISPs such as AT&T, Comcast, Time Warner, and Verizon to charge content providers for access to a 'fast lane,' enabling some websites to load more quickly than others (Rassool)." Yet, net neutrality is a story of both content and access; if undermined it would allow providers to pick which content could be accessed in meaningful ways. It could also be a template for illiberal states to slow down undesirable content and thus inhibit meaningful access to its citizens.

The story of net neutrality also exemplifies the relationship between government and private enterprise. The FCC struggled to establish itself as the legitimate oversight agency of ISPs' pricing,

quality of service, and other policies, and while it has succeeded in giving itself authority, its impact is not guaranteed. There are two schools of thought; on the one hand, it is believed that ISPs and ICTs should be free from government oversight under the belief that such regulation would lead to significant compromises in innovation and competition. On the other, the FCC claims since 2010 in multiple documents that it intends to enable innovation and an open Internet that would not be unfairly dominated by the few powerful ISPs and established "edge providers" like Netflix and Skype that could afford to pay for the faster service.

Efforts to control the flow of the Internet resemble a cat-and-mouse game between ISPs and the federal agency. It began in 2007 with Comcast's efforts to slow peer-to-peer file sharing and the FCC's attempt to block these actions. A federal court declared in 2010 that the FCC did not have jurisdiction, and ever since the agency has been trying to redefine its relationship to ISPs. In the same year, the FCC adopted the "Open Internet Order" based on normative standards it outlined for consumers in 2005 which were meant to ensure freedom of speech on the web (balanced of course with the needs of law enforcement). In 2010, these normative ideals were joined by the premise that ISPs could not limit access or content in any way, and were transformed from promises into law. These laws were challenged on multiple occasions, and were dismantled in yet another series of court rulings.

Verizon v. FCC (2014) ruled that most of the provisions of the Open Internet Order were inapplicable to private ISPs as they were scheduled under Title I of the Communications Act of 1934. ISPs were classified as information rather than communication services, and thus not under the jurisdiction of the FCC, and that the only providers subject to the 2010 rules were "common carriers" like municipal ISPs. The court upheld the transparency provision of the Open Internet Order, maintaining that plan prices had to be made easy to understand and publicly available. In reaction, the FCC released a statement in 2014 that in part read:

> Today, there are no legally enforceable rules by which the Commission can stop broadband providers from limiting Internet openness. This Notice begins the process of closing that gap, by proposing to reinstitute the no-blocking rule adopted in 2010 and creating a new rule that would bar commercially unreasonable actions from threatening Internet openness (as well as enhancing the transparency rule that is currently in effect).

Despite the ruling, the FCC continued to pursue net neutrality (or to wrest control of the Internet from private enterprise, depending on one's interpretation). By February 2015, the FCC narrowly adopted new

rules to reclassify ISPs under Title II of the 1934 act, classifying them as common carriers and a public utilities rather than an at-will information service. By considering it a telecommunication service, the ruling from *Verizon v. FCC* becomes null, and that:

> …the new rules are an à la carte version of Title II, adopting some provisions and shunning others. The F.C.C. will not get involved in pricing decisions or the engineering decisions companies make in managing their networks. Mr. Wheeler [FCC chairman], who gave a forceful defense of the rules just ahead of the vote, said the tailored approach was anything but old-style utility regulation. “These are a 21st-century set of rules for a 21st-century industry,” he said. (Ruiz and Loeb)

Many members of the Internet-related business community in the US, including Google and Facebook, considered the ruling a win for protecting innovation. ISPs like Comcast and Verizon challenged the reclassification but have been unsuccessful as of June 2016.

Much of the rhetoric surrounding the Title II ruling, including Wheeler’s, is a reflection of the belief that the policies on net neutrality the US adopts are going to influence the relationship between providers and governments elsewhere in the world. While some see the intervention of the government into the private sector as a model that should not be emulated, others see it as a necessary component of responsible Internet policy:

> Freedom on the Net project director Sanja Kelly notes, "In less democratic countries, where most online content providers are state-owned and censored, authorities would have the perfect excuse to begin giving faster lanes of access to pro-government outlets, skewing the ability of democratic opposition to get their message across (Rassool)."

The outcome of the US-centered debate over net neutrality directly affects content and meaningful access. Cyrus Rassool of the Huffington Post in his editorial “The United States Must Lead in Upholding Net Neutrality,” argues that failing to do so would undermine the “United States as an international leader on internet freedom,” and that “as the birthplace of the internet, the United States has a special duty to preserve equal access.” Associated with Freedom House, Rassool expresses a new version of a century-old idea of American exceptionalism; this strand of thought that defines the US’s role as setting the bar for state behavior survives today in Internet policy.

The reassignment of ISPs as common carriers in the US, allowing the FCC to extensively regulate them under Title II, was supposed to be the end of the fight over network neutrality. Indeed, one of the NGOs fighting for the open Internet has a page that has not been updated for six months; the issue about encouraging the reclassification is now moot (see CommonCause.org). Instead, ISPs are working

to find ways around the reclassification that would nevertheless result in the promotion of particular websites over others. T-Mobile introduced its “Binge On” program in December 2015, which “throttles nearly all video content” to 480p and does not count the streaming service towards users’ data caps (Brodkin 2016c). Users enjoy lower quality video, but streaming content does not count towards monthly data allowances. Such “zero-rating” policies resemble Facebook, Google, and other providers’ free but limited web browsing that is prevalent in developing states. T-Mobile in the words of its senior VP for Government, that

> …the [FCC] has to tread lightly—and certainly more lightly than it would in the wired world—in the wireless space when there is so much experimentation happening, so much differentiation happening, and a lot of it customers responding to," T-Mobile Senior VP of Government Affairs Kathleen Ham said at an event in Washington, DC. "We do have to be transparent about it, we do have to make sure that the customer has choices, but I think it's wise to tread lightly in this environment when there's so much going on that I think customers are benefiting from."

While customers seem to like the program (92 percent according to T-Mobile’s own statistics) and can turn it off, signifying an ability to choose whether to take advantage of the free data, others claim it still violates the spirit of net neutrality. Barbara van Schewick, Director of Stanford Law School’s Center for Internet and Society, claims the policy has "substantial technical requirements" in order for content providers to qualify, leaving less established, more innovative efforts out of the loop.

Mobile ISPs are fighting against proposals that would increase competition and enforce net neutrality. Preimesberger of *E Week* noted in March 2015 that the FCC has included mobile ISPs under their net neutrality rules, which means that zero-rating practices will soon fall under the scrutiny of the regulators. AT&T was cited for having ‘deceptive business practices’ for throttling customers who had been grandfathered into unlimited data plans. Dano remarks that the industry has been slow to adopt services that would allow users more efficient means of communication, including Wi-Fi calling and making video calling services interoperable. Wi-Fi calls would use wireless Internet services to place mobile calls, much like VOIP does for landlines. Dano is dismayed:

> And what did most other wireless carriers do? Generally they argued their networks were so great that users didn't need Wi-Fi calling...In the meantime, Wi-Fi users with poor or no cellular coverage simply couldn't place voice calls from their phones -- despite the fact that Wi-Fi calling technology has been around for eight years. Eight years! It's difficult to listen to operators extolling the benefits of 20 Gbps 5G technology when they have a history of being unable to make relatively simple concessions to coverage solutions outside their direct control.

Companies are reluctant to make services like FaceTime and WhatsApp (a messaging service now owned by Facebook) interoperable, forcing users to adopt certain technologies or services over others and thereby limiting choice.

Despite that the FCC's announcement that it would be looking into zero-rating practices, Verizon announced that it would be providing its own streaming service, Go90, through its FreeBee Data 360 program. "…it will exempt its own video service from mobile data caps—while counting data from competitors such as YouTube and Netflix against customers' caps (Brodkin 2016d)." Such a practice incentivizes subscriptions to a particular service and simultaneously discourages subscription to others. Additionally, "If those rivals in the video market want the same benefits afforded to Go90, then Verizon would still benefit by taking money in exchange for data cap exemptions." Readers of the *Ars Technica* article reveal that users are skeptical about such arrangements: isparavanje asks "Would this not breach anti-trust regulations even without net neutrality rules?" 0megapart!cle writes:

> This is absolute bs, and the Comcast stream thing is even more BS. The effect on competition is the same whether the data goes over the public internet, or over Comcast pipes only. The effect on competition is what the FCC is looking at when deciding if a policy is legal or not. Therefore, whether it goes over the public internet or over Comcast pipes only should have no effect on whether it is legal or not.

Reviews of the commentary on such articles yield similar results: there seems to be little support for the idea that corporations should be able to throttle or control content flows without significant considerations made for consumer opt-outs or alternatives. They also recognize that the ISPs are directly challenging the FCC and are cautiously optimistic that the latter will declare zero-rating policies illegal.

Brodkin (2016f) reports on the case of *US Telecom Association v. the FCC* that was decided on June 14, 2016 in the US Court of Appeals in the District of Colombia. The decision upheld the FCC's reclassification of fixed and mobile broadband providers as a telecommunications service under Title II. The court also upheld steps taken by the FCC to protect edge providers like Netflix in the name of net neutrality. Wheeler said:

> Today's ruling is a victory for consumers and innovators who deserve unfettered access to the entire Web, and it ensures the Internet remains a platform for unparalleled innovation, free expression and economic growth," Wheeler said in a statement issued shortly after the ruling. "After a decade of debate and legal battles, today's ruling affirms the Commission's ability to enforce the strongest possible internet protections—both on fixed and mobile networks—that will ensure the internet remains open, now and in the future.

AT&T has already promised to appeal to the Supreme Court.

While largely being a story of the struggle between ISPs and government regulation, net neutrality is also one manifestation of the F2C in the US. Should providers be able to control the speed of content, thereby making it possible for certain organizations or individuals to make meaningful access possible? More generally, the question becomes whether or not private entities are able to determine the quality of content for consumers, and is a reflection of whether or not equitable Internet access is a right for both users and innovators.

Mergers. Mergers among ISPs and cable providers also receive tremendous attention among the proponents of the F2C and Internet freedom in the US. Those in favor of such mergers view them as avenues for increased efficiency and wider service areas. Opponents see them as a threat to competition and fair pricing. If the industry became too consolidated, then there would be little incentive for ISPs to put fair pricing and equitable infrastructure rollout before profits.

In 2014, Comcast announced a bid to purchase Time-Warner Cable for $45 billion in stock exchanges. As two of the five largest ISPs, this meant that consumer choice would have been narrowed in locales where both of these ISPs operate, or that expansion into new territories to increase competition would halt. FreePress, an Internet freedom advocacy group, supported efforts to stop the merger that would have "consolidated power against consumers." The Department of Justice opened an investigation against the merger in 2014 and announced that it would bring an antitrust lawsuit against Comcast in April 2015. The suit indicated that Comcast's justification of improving DSL speeds to current Time-Warner subscribers was a fraudulent claim, and that there was no meaningful way to invest in the infrastructure of a sub-par technology. Comcast announced that it would abandon its bid that same month.

Soon thereafter, Charter Communications announced plans to acquire Time-Warner. Unlike the Comcast deal that emphasized both improved Internet and cable television services for its customers, this merger asserts that it would increase broadband availability to new consumers. Charter's customer base would be quadrupled by such a deal, and Steelmay reported that it will give the merged companies "more resources and incentives to introduce innovation and competitive services." The idea of a near-monopoly status may be far less acute: "The Charter acquisitions would give it control of less than 30 percent of the

country's high-speed Internet market, compared with 57 percent for Comcast." However, the outcome would still mean a duopolistic broadband national marketplace, with Comcast and New Charter controlling 70 percent of the 25 Mbps and up broadband market (Brodkin 2016a). The deal has been approved by the FCC and Department of Justice on April 29th, 2016 with Charter paying $56.7 billion for Time Warner and $10.4 billion for Bright House, a content provider and ISP. One of the blockages from the Comcast-Time-Warner "mega deal" has been overcome with pledges that the merger will not result in the tightening of restrictions on content providers, specifically video-streaming platforms like Netflix and Hulu.

The result of the merger is too soon to tell, but like the Comcast deal, it has proven divisive. Time-Warner's May press release argued that there would be multiple benefits: faster speeds, better video products, more affordable phone service, increased competition, and faster customer and financial growth. The latter two things would benefit both employees and shareholders. Free Press CEO Craig Aaron is quoted as saying that these benefits are window-dressing. Instead:

> "Thanks to this merger both Charter and Comcast now have unprecedented control over our cable and Internet connections," he added. "Their crushing monopoly power will mean fewer choices, higher prices, no accountability and no competition. Conditions won't lower the monthly bills for those who'll be hit hardest by these rate hikes: low-income households and communities of color (Farivar)."

The sincerity of the belief that that the merger will result in better service is impossible to prove. Yet the intersection between to the main issues related to ISPs in the US, mergers and neutrality, within the FCC's caveats to this deal signals the necessity of ISPs to use the language of the F2C even if solely pursuing profits.

The story of the F2C in the United States is highly connected to its ISPs. Even considering the US predilection for free markets and unencumbered free enterprise, telecom companies have a remarkable amount of power. The spread of broadband will be largely determined by markets and profitably, but efforts to increase access to broadband also recognize that it is a necessity in the 21st century and an inherent right. There has been an honest attempt by the FCC to realize this dream, but it is a battle that will be played out in the courts for years to come.

Frames and Action on the F2C

The following section discusses some of the rhetoric that US politicians, corporations, individuals, and NGOs have used in discussing the F2C and Internet Freedom in general, for both international

relations and domestic policy. These entrepreneurs routinely connect access to civil rights and liberties in addition to arguments about equality of education and employment opportunities.

Politicians' Rhetoric. President Obama held a town meeting in China in November 2009 which addressed students whom he called "China's future leaders." In a carefully-worded speech, he remarked on the uniqueness of Chinese culture as compared to the US; the former ancient and rooted in tradition, the latter a relative newborn that is setting out to continuously define itself. One of the principles underlying America's political vision is its foundational documents, and how they in turn reflect the relationship between the people and its government that is based on inalienable human rights. The president danced between universalism and cultural relativism by stating that the US was not trying to enforce a belief system on others, but that these rights are broadly applicable. One student asked about the use of Twitter in particular and China's Great Firewall in general. The president's response is lame in its lack of more open critique but nonetheless indicative of the type of government-citizen relationship he outlined in his speech: "I actually think that that makes our democracy stronger and it makes me a better leader because it forces me to hear opinions that I don't want to hear." He argues that like every right, openness is in a balance with other governmental interests like security. The good of openness, he claims, outweighs the bad.

President Obama's sentiments were taken up by the First Lady in 2014, when she argued in a speech during a goodwill tour to China that Internet freedom was fundamental to the relationship between citizen and state. Only by having the Internet freedom and free speech is it possible to "…learn what's really happening in our communities, in our country and our world." Additionally, the newly minted Ambassador to China Max Baucus also commented on the "virtues of Twitter and Facebook," and their ability to hold governments accountable.

Legislators have also promoted Internet freedom in the international realm, if not as a domestic manifestation of the F2C. Former Representative David Wu (D-Oregon) introduced the Internet Freedom Act in February 2010, which would have directed the National Science Foundation (NSF) to establish the Internet Freedom Foundation to promote Internet freedom through education, advocacy, and research. The bill died in Congress, but more interesting subsequent bills with the title of the "Internet Freedom Act" have taken on very different purposes. As recently as 2015, the Internet Freedom Act, sponsored by

Marsha Blackburn (R-Tenn.), would seek to roll back the regulations on ISPs recently enacted by the FCC, with similar bills dating back to 2011.

Senator Dick Durbin (D-Illinois) sought to introduce an Internet Human Rights Bill in March 2010, which would seek to impose penalties on US-based companies that violated the rights of users abroad:

> With a few notable exceptions, the technology industry seems unwilling to regulate itself and unwilling even to engage in a dialogue with Congress about the serious human rights challenges that the industry faces," Durbin said. "In the face of this resistance, I have decided it's time to take a more active position (Kang)."

It is unusual for sitting American politicians to frame their agendas in terms of international human rights as they tend instead to emphasize domestic values. Nevertheless this bill, which also died in Congress, appears to be a step in the right direction, especially ahead of the Arab Spring.

Senator Chris Coons (D-DE) endorsed Clinton's remarks in an editorial for the *Huffington Post* in 2012 that ran under the headline "Internet Freedom is a Human Right." His thoughts did not focus on access *per se*, but instead on the popular issues of censorship and repression. Like Clinton, he sees Internet freedom as fundamental to the exportation of democratic values abroad, and adds that the US has invested "tens of millions" of dollars into attempts to allow those who sought to get around government censorship to do so through technological innovations, much like the Freedom2Connect foundation. Additionally, he noted complementary caucuses in the House and Senate for Global Internet Freedom.

Lifeline Program. In addition the discussed National Broadband Plan, the FCC has undertaken plans to spread access to underserved populations. In March 2016, it announced that it would be extending its Lifeline program. Established in 1985, the program has provided poor Americans with basic phone service. Wheeler and Clyburn acknowledge the program has had its problems, including burdensome administrative requirements alongside fraud and waste. The newly designed program has a National Verification Program with a nationwide database so companies cannot admit unqualified applicants. In line with the F2C, the program extends free voice and broadband service vital for employment, healthcare, and education, at speeds that other citizens are lucky enough to enjoy through the marketplace. Reader commentary on the plan is mixed, with some accusing the FCC of wanting to provide "broadband welfare," and misconstruing the original purpose of the Lifeline program, which was to

provide access to emergency services. Yet others are more welcoming of the move, arguing that government has an appropriate role to play in providing access:

- Broadband allows access to goods and services at reduced rates because the "Internet ecosystem" is based on competition. Among other things, lack of affordable broadband makes it harder for poor citizens to spend their limited income more efficiently...because they can't access the competitive market. Bravo on this initiative! (Ivan Stephanovich)
- And the mobile telephone...All citizens in this country should have inexpensive and easy access of Wifi. It should be a right in our nowadays society where you cannot participate in our Democracy without a computer and Wifi. (liaisonsus)
- (Wheeler and Clyburn 2016)

Domestic Attitudes on Internet Use and Internet Freedom

Two methods are used to determine whether there is evidence of support for Internet freedom among the larger US population. First a review of survey results with questions can paint a fuller picture of typical Internet users in the US and how they feel about how the Internet can or should be regulated[23]. Second, a unique source of dialogue can be found in commentary by readers of these survey results. While sometimes the online commentary on news articles can be a morass of partisan rhetoric, those who comment have shown to an apparent professional and informed interest in the technical policy analysis offered by these surveys. While this commentary is not meant to be representative of general American opinion, it can reveal how industry experts feel about issues like Internet freedom and net neutrality.

Pew and Gallup perform extensive surveys that normally center around American attitudes on a multitude of subjects. One way to gauge the importance of the Internet to Americans is to reflect upon how often it is used and how indispensable it is believed to be. Perrin reports that 73 percent of Americans go online daily, 21 percent reported almost constant connectivity while only 13 percent of adults report going online several times a week or less. The digital divide between SES indicators also predict frequency of use, with those earning more than $75,000, with at least a college degree, or living in urban locales reporting even higher rates of “constant” connection, with 28 percent, 29 percent, and 23 percent figures, respectively. In the commentary on this poll, “Carol F.” recounts that while her mother does not use the Internet herself, she indirectly takes advantage of the technology when Carol acts as her proxy user. “So I’m wondering how many of the 13% of adults that never go online are like my mother, who doesn’t go online herself but enjoys all the benefits that being online can provide?” The scenario

[23] Surveys in the US are quite abundant; outside of this case, however, such information is more difficult to come by.

reflects some of the causes of the digital divide, with users unable to use the technology due to their lack of know-how or their inability to access the necessary hardware.

The questions in Pew's poll, "US feelings on the Internet: the Internet at 25" (2014a), reflect how users feel about the importance of the Internet in their lives. For the question of how hard it might be to give up the Internet, the percentage reporting "very difficult/impossible" substantially grew between 2002 and 2014, from 31 percent to 53 percent. Only 12 percent of the respondents said it would be "not at all" difficult to do so. When asked why, survey participants answered either that it was essential for work or some other reason (61 percent), that they really enjoyed being online (30 percent), or both equally (7 percent). The trend shows that the percentage of US Internet users seeing it as essential to life and work continues to grow, and those that see it as a luxury or amusement decreases. The survey also queried the meaning of the Internet, asking whether it was a good thing for both society and the respondents themselves. Seventy-six percent saw it as good thing for society and 90 percent saw it as a good for themselves, the difference reflecting perhaps a more optimistic view of personal habits than perceptions of society at large.

Horrigan and Duggan (2015) of Pew reported on the perceptions on broadband at home. Nearly 7 in 10 Americans feel that "not having a home high-speed internet connection would be a major disadvantage to finding a job, getting health information or accessing other key information – up from 56 percent who said this in 2010." Forty percent felt that it would inhibit access to government services, and 37 percent said it would mean missing out on "learning new things that might enrich their lives," up nearly 15 percent from merely 4 years earlier. Taken together, these surveys reveal that Internet penetration in the US has brought with it the belief that access is a necessity for life in America, at least among those who are able to access it in the first place. Many who are constantly connected would find it difficult to give up, and view the lack of meaningful access as inhibiting their rights as citizens and as human beings.

World opinion surveys conducted since 2008 have included American beliefs about the connection among Internet access, use, and human rights. GlobeScan (2010) reported that 76 percent of Americans viewed access as a fundamental right, and Internet Society's "Global Internet User Survey" (2012) recorded this percentage as 72 percent. Only 8 percent strongly disagreed with this sentiment. Surveys also included inquiries about the connection of the Internet use and civil rights. GlobeScan

found that 55 percent of respondents believed that the Internet better enables free speech (versus 48 percent worldwide), while 78 percent believed it should be guaranteed on the web in 2012. Sixty-eight percent saw social media as an enhancement to the rights of assembly and association. In 2015b, Pew reported that 91 percent of respondents believed it was either very or somewhat important that Internet use should be unhindered by censorship. In the Kull et al 2008 study, 27 percent of respondents said the government had the right to hinder freedoms to assure security, while the Internet Society 2012 poll recorded that only 23 percent would accept control or monitoring of the Internet if it increased security, with 38 percent saying that would accept little or no such action. Many thought the government should intervene more into the market, with 63 percent saying that the government is obligated to provide access and 67 percent arguing it should provide cheaper computers. Sixty-three percent also said the government should encourage competition among ISPs.

There are some disagreements about the viability of labeling Internet access as a human right, despite the large public support of doing so. Vint Cerf, one of the creators of the ARPANET and an active norm entrepreneur through the Internet Society, penned an editorial in the *NY Times* after the Special Rapporteur's report on Internet access was published. In in the opinion, Cerf draws a distinction between human rights and civil rights, saying that human rights are intrinsic to being human, while civil rights are conferred by law. While Cerf admits that if the US government tries to guarantee "universal service" for the Internet as it has done with telephony, which should be available in the most remote regions in the country, than it might be safer to label it as a civil right. Nevertheless, the point of Cerf's argument was that "technology is an enabler of rights, not a right itself." Further, he sees the role of engineers—and not the state—as central to ensuring the protection of users' rights online.

Scott Edwards of Amnesty International criticizes Cerf's position from a philosophical perspective, arguing that such an interpretation of rights is "exceptionally narrow." Because culture, technology, and politics are not static, the understanding of human rights must expand accordingly. While the denial of access may be an annoyance in the US, for sub-Saharan African users it can be "an immediate threat to their lives and their livelihoods," the direct result of financial dependence on mobile technologies. He draws a parallel to other rights, arguing that while the denial to access of a town square through martial law or a curfew is not a direct violation of human rights, it does severely limit the meaningfulness of rights

of association or assembly. Edwards draws a parallel to the enumeration of human rights in instruments like CEDAW and the CERD despite the existence of the ICCPR and the ICESR, explaining that the latter were not enough to guarantee the rights of women or children: "Because someone, somewhere said 'that's not a human right.'" In the commentary on Edward's article, many readers expressed sympathy for Cerf's position, while others argue that considering the Internet as right is appropriate considering the direction of technological progress. Robert Alberti, a long-time ICT professional who helped to pioneer email, chatting systems, and interactive gaming in the 1980s with GamBit MultiSystems and Internet protocols,[24] commented in support calling access a right. "Asking Mr. Cerf whether Internet access is a human right is as foolish as asking Gutenberg whether a free press is a human right." Comparing Cerf's narrowmindedness to his own experiences, Alberti is adamant that such labels are at best premature and that users of new technologies will take it in directions unforeseen by their creators. "Internet access is simply COMMUNICATION, and the ability to communicate… widely, IS a human right, or else speech is the domain of the wealthy and powerful and the rest of us are muttering to ourselves in a closed room." That Internet access appears to be a "first-world problem" is an acknowledgement of economic injustice rather than remarking that access itself is unimportant.

There have also been polls that query the substance of Internet policy in the US regarding the PRISM program and the fight over net neutrality. First, Frank Newport of Gallup (2013) reported on the respondents' feelings about government surveillance programs that monitor citizens' communications, including email and social media. Snowden's leak to the *Guardian* was reported on 9 June 2013, and the survey was conducted over the following two days. Only 37 percent of all adults approved of the program, while 53 percent disapproved and 10 percent had no opinion. The results were partisan, with more Democrats (49 percent) approving of the program and most Republicans and Independents disapproving of the program (63 percent and 56 percent). Those who approved of the program mostly argued that terrorism was more important than civil liberties (23 percent of all respondents), while only 11 percent thought it did not violate civil liberties. Of those who disapproved, 21 percent argued there could be some circumstances that would justify its existence, while 30 percent of all US adults thought there

[24] According to his Linked In profile: https://www.linkedin.com/in/robertalberti

would be no circumstances that could be dire enough to justify the violation of such civil liberties[25]. The participants were split about Snowden's actions (44 percent to 42 percent), but more thought that once the information was available, newspapers had the right to publish the story (59 percent to 33 percent). Newport remarked that "Results from the Gallup poll indicate that Americans have somewhat flexible views about the government's surveillance program and/or that they are still forming their opinions on the issue."

The question is taken up again in January 2015 by Pew (Ranine and Madden). In the approximate year and a half that elapsed since the Gallup poll, 87 percent of the respondents had heard about the surveillance program, with 31 percent saying they had heard "a lot." Men and college graduates were more likely to have answered the latter.

> In this survey, 17 percent of Americans said they are "very concerned" about government surveillance of Americans' data and electronic communication; 35 percent say they are "somewhat concerned"; 33 percent say they are "not very concerned" and 13 percent say they are "not at all" concerned about the surveillance.

The proportion of those who were very concerned was high among those who also reported knowing more about the program. The survey also looked for qualitative responses. Those who were concerned expressed that it was over privacy; for example: "The fourth [amendment] originally enforced the idea that each man's home is his castle, secure from unreasonable search and seizure by the government." Those who showed little concern emphasized two major points. First was the "nothing to hide" sentiment, which argued that surveillance in itself is not harmful to those citizens who are law-abiding. Second was the idea that the impingement upon civil liberties was a necessary price to pay for security. "Terror" or "terrorism" was often a term used in these open-ended responses. The survey also asked under what circumstances it would be acceptable to monitor a citizens' communications and Internet use; the majority see it acceptable for certain groups. For instance: 82 percent saw it acceptable to track suspected terrorists; 60 percent saw the monitoring of leaders, both foreign and domestic, as acceptable; 54 percent said the tracking of foreign citizens was acceptable; 68 percent thought monitoring someone who had exchanged emails with an imam who preached against infidels was acceptable, and 49 percent saw it acceptable for those who had friends or followers on social media that used "hateful" speech against

[25] Newport did not account the participants' age. Such numbers would likely be swayed if the majority were young adults, whom I have informally observed are more willing to trade rights for security, closer to 50%.

American leaders. Such exceptions paint an uneven portrait of how Americans feel about surveillance and the relationship between the Internet and civil rights. While in the abstract, over half of the respondents were somewhat or very concerned over surveillance, almost all would accept the monitoring of suspected terrorists. Large portions also support the surveillance of powerful politicians or foreign citizens. While such opinions do not speak directly to the issue of access, they do reflect a larger belief in the need to balance meaningful access with apparent security demands from the state.

In addition to the opinions on access and the importance of privacy and security, there are also polls on the issue of net neutrality. These polls were not conducted by Pew or Gallup, but on the behalf of two business coalitions, the Internet Association and the Internet Freedom Business Alliance. Made up of members such as Netflix, Yahoo, Dropbox, Uber, Linked In, and others, the Internet Association asked 550 individuals their opinions on wireless net neutrality in 2014. Only 24.6 percent of the respondents, of whom 80 percent were white and earning between $50,000 and $99,999, reported 'very or extreme familiarity' with the concept, with almost half reporting that had no familiarity with it. Nevertheless, respondents strongly disagreed with the idea that ISPs should have arbitrary power over consumer choice of the websites they visit, saying they should neither able to block access to legal websites (56.1 percent) nor be able to slow websites that are not preferred (76.4 percent).

A similar poll for the Internet Freedom Business Alliance was conducted by Vox Populi Pollling. Eighty-one percent of voters agreed that "'it is critical to maintain' an Internet where service providers cannot block, discriminate against, slow down, or charge content providers." Eighty percent agreed with the FCC Chairman's proposal that there should be rules in place that say "no blocking, nor throttling, or paid prioritization." While conservative voters generally dislike government interference in the market, they are willing to seek protection from large ISPs like Comcast and Verizon due to the concentration of power these companies enjoy. In an opinion submitted to the FCC on the reclassification of ISPs as common carriers, the group highlighted how there was unprecedented public participation embodied by four million comments from people, companies, and groups interested in preserving net neutrality. Culbertson argues that "…the Internet has become an essential platform for innovation, investment, competition, and democratic discourse as well as the importance of unfettered access."

NGOs and Norm Entrepreneurs

Connecting for Good is an NGO serving the Kansas City metropolitan area that straddles the states of Kansas and Missouri. The city was the first to benefit from the Google Fiber program that provides 1 Gbps connections to users for $70 a month, or basic broadband for free. The organization was founded in 2011 by Michael Liimatta to combat the digital divide, claiming that "it is one of the most important social justice issues of our day," demonstrated by 25 percent of the city's residents not having broadband at home. They frame meaningful access as enabling economic and social opportunity, allowing users to look for jobs, connecting with family, access virtual libraries, having access to health and medical information, and access to online education. Their core values contain three related premises:

- Internet connectivity equals opportunity. It is an absolute necessity in order to fully participate as a productive citizen in a digital society.
- Education is the number one thing that lifts people from poverty. In a digital society it is impossible to pursue a quality education without access to the Internet.
- In-home Internet access is as essential as any modern utility; like phone service, electricity and running water.

In addition to Wi-Fi, the foundation also provides community technology centers, sells low-cost, refurbished computing equipment, and offers free digital literacy courses. Of the 2,000 participants in these courses, 25 percent had never used a computer, 75 percent had incomes under $20,000, 75 percent were 50 or older, and 80 percent were minorities, all traditionally disadvantaged segments of the population in terms of digital literacy. Two-thirds in these classes were comprised of women, half of whom were 60 or older with minor children living with them. Because the ConnectforGood program emphasizes the pivotal role of digital access and literacy for education, connecting these women would help to assure that she could pass on that knowledge to the children with whom she lived. Parental involvement and what happens outside of school are well-known to be one of the most important factors in educational outcomes; enabling access helps to close widening opportunity gaps for the urban poor.

Google Fiber also oversaw another first for Kansas City in February 2016, wiring housing projects with 1 gigabit fiber Internet connections—for free—through HUD's ConnectHome program. HUD Secretary Julián Castro commented that "For families here, at West Bluff, the days when young folks had to research a paper using the Wi-Fi at McDonalds, or research a paper using a library computer, are over (Morris)." Kansas City was chosen as the first among 28 pilot cities and one tribal nation due to its history

with Google and trying to combat the digital divide through ConnectforGood. In November 2015, Liiamatta was appointed manager of the program. Castro connects the program to the issue of equality of opportunity, claiming that it will help more citizens achieve the "…high-speed access to knowledge and opportunity that millions already enjoy." The program reveals the disparities among those of various socioeconomic status of access to broadband and how that gap can be narrowed through similar means in Kansas City. The gap could be narrowed first, by making broadband accessible in public housing through discounted or free terms; second, by training in digital literacy; and third, by providing computers and technical support. HUD argues that poverty in the worst-off communities in the US, so-called "Promise Zones," can be partially alleviated by broadband. "As the President has said, 'Today, high-speed broadband is not a luxury, it's a necessity.'"

American hypocrisy?

The F2C and Internet Freedom are challenged by two dominant themes. First, official policy appears to belie messages promulgated from the upper echelons of the Executive branch. The widely-criticized PRISM program undermines the notion that a citizen's conduct online is free from government intrusion. Second, the continued debate over the state's role in providing access is contradictory to the model supported by the UN and other F2C entrepreneurs. The relationship between the public and private provision of access in the US is highly skewed to the private sector, leaving consumers vulnerable to the limitations and whims of the market.

Unveiled to the public in 2013 by National Security Agency (NSA) contractor Edward Snowden, the legal (Protect America Act) yet covert program that allowed the NSA to collect "metadata"—email, texts, video conferences, and the like—in order to uncover threats to US national security, especially radical, religiously-motivated terrorism. In the time after its initial disclosure, it was revealed that the US government was collecting information not only on its own citizens, but also on foreign governments, including long-standing US allies. Von Drehle describes the metadata collection as a process in which virtually all data from participating providers would be collected and later analyzed looking for key terms or markers that could be indicative of security threats. Such data would not be connected to individuals, and if threats were discovered, there would be judicial oversight. Despite assurances that the government was not looking for minor crimes, that US citizens were not valid targets, and the argument

from President Obama that security and privacy are in a balance (Baker and Sanger), the PRISM program is seen as an affront to the idea that the US can rightfully claim to be a leader in Internet freedom. Access itself could be compromised by those who may fall into the category of suspected persons, thereby discouraging the technology's use.

Attempts by the FCC and municipal ISPs to further integrate the public and private sectors in the realm of Internet access also challenge the view that the US is a leader in Internet freedom. Unlike other states with public oversight the provision of access and its diffusion, the US has taken the opposite approach. Because of a long history of market liberalism, coupled with the industry's rapid-paced growth, a culture among Internet and ICT professionals and those in favor of private enterprise have long been wary or defiant of government policy and oversight of the industry. ICT professionals favor the idealist notion that unhindered innovation is the best way to continue along the path of faster and better access, but such a narrative ignores the real connections the Internet's development has had with government, from ARPANET in the 1960s, the "Black Proposal" to the NSF in 1983, to legislative moves to further allow the NSF to assist in funding technological innovation. Private enterprise, including corporate ISPs often argue that government intrusion hurts the industry's ability to provide ideal service, and perhaps more importantly, profit. Left to its own devices, however, the industry has been slow in providing customers in unprofitable regions reasonable speeds.

Martyn Roetter (2013) comments that broadband development in the US has been hindered because of the "…failure to appreciate the need to blend and integrate business entrepreneurialism and public sector stewardship (632)." The government should be "referee, loan guarantor, source of grants, and anchor tenant (632)" in order to assure the market is viable for competition. He also recounts that the FCC is in itself due for introspection, given that Commissioners and senior officials often are grossly intertwined with the corporations they are meant to administer. Despite Chairman Wheeler's extensive history working for the telecommunications industry, he has done remarkable work putting the F2C first.

***

Despite being the origin of the Internet, study of access in the US reveals a complex relationship among the state, ISPs, and NGOs. While the Internet is largely seen as indispensable for everyday life, it is seldom conceived of as a right in itself, and the state's role in the provision of that access is minimal,

lest “Internet welfare” be the result. The preference for the free market and lack of regulation has allowed several ISPs to dominate the broadband market, largely able to determine who can have what type of speeds and at what price. Nevertheless, while chasing after their bottom lines, ISPs must clothe their demands in the context of the F2C if but skimpily. Additionally, Internet freedom is seen as an extension of civil rights entrenched in the Constitution and the violations of these rights in the PRISM program are framed as temporary aberrations of otherwise valid principles.

Brazil

Brazil is positioning itself to be a leader in Internet freedom as evidenced by its rhetoric and policies to increase access and to promote privacy and net neutrality. Fallout from the Snowden revelations and US spying on President Dilma Rousseff has cemented Brazil's place as a defender of the F2C and Internet freedom. The multi-stakeholder approach to Internet in Brazil dates back to the adoption of commercial Internet in 1995 and the Brazilian Internet Steering Committee (CGI.br) and forward to the five-year public debate resulting in the *Marco Civil da Internet* (Civil Rights Framework for the Internet). As a result, the provision of Internet is considered a public good which could be considered one of the most direct manifestations of the F2C in which the state is held directly responsible for citizens' access.

Background

Brazil is a large and powerful state by most measures. It has a population of 204,259,812 (6th in the world), and takes up an area of 8,515,770 km^2 (5th in the world). As is common among BRICS states, it is has a high urban population, totaling 85.7 percent, with 6 major metropolises with populations of 3.7 million or more,[26] including São Paulo, one of the largest cities in the world. The state is characterized by a diverse topography, with major cities concentrated on a narrow strip of coastline, and is divided into 26 states within five officially designated regions. Regions are associated with important differences in demographics and economics. While the Brazilian economy is quite large, with an annual GDP of $3.276 trillion, ranking it 8th in the world, São Paulo accounts for nearly one-third of that total. GDP per capita is $16,200, ranking the state 100th in the world.

Brazil has 44.1 million landlines, ranking 8th in the world; one phone is plugged in for approximately every 22 people in the country. The figure escalates for cellular phones, with 280.7 million in the country, placing it 6th in the world. In total, there are 108.2 million Internet users in Brazil which ranks 6th in absolute numbers, and totals 53.4 percent of the population. Users are concentrated in major cities where infrastructure is widely available.

[26] São Paulo 21.066 million; Rio de Janeiro 12.902 million; Belo Horizonte 5.716 million; Brasilia (capital) 4.155 million; Fortaleza 3.88 million; Recife 3.739 million (2015)

As a former colony and part of the 20th century Latin American experience of bureaucratic military regimes, Brazil has a complicated history with liberal norms. The 19th and 20th centuries were characterized by a string of military leaders that at times coopted peasants, political bosses, bureaucrats, and labor. By the 20th century, military leaders faced mounting pressure to release control due poor economic performance and hyperinflation, and the economy was liberalized in 1995. The Brazilian experience with human rights norms is a mixed bag. Recent efforts to increase Internet penetration and meaningfulness are part of greater effort to balance the needs of economic growth, foreign interests, and the alleviation of poverty. The Workers' Party has had some success lifting people out of poverty and creating social safety nets under former President Luiz Lula da Silva, but economic recession has reversed some of these successes during the administration of Dilma Rousseff. Many Latin American countries are trying to come to terms with legacies that include oligarchy, repression, and violence. Additionally, the influence of the US, especially its role as a co-conspirator in Brazil's military coup of 1964 and as part of the greater global economic institutions like the IMF and the World Bank, is the backdrop for analyses of contemporary problems like the PRISM program.

The Internet in Brazil

Background. The development of early informatics in Brazil was hindered during the 1970s and 1980s by the bureaucratic military regime. In 1975, Embratel, a subsidiary of the state-owned telecom Telebras, had exclusive control of nation-wide data transfer systems, and could have as a consequence signaled a similar path that other authoritarian states had taken in the development of their Internet. Further, under the guise of import controls, TCP/IP, which had been widely gaining acceptance elsewhere in the 1980s was banned by the government in order to develop domestic industry. This techno-nationalist sentiment was not to last. The collapse of the regime signaled the spread of the Internet, and in 1987 the first connections to hosts in the US were made possible by the research foundation FAPESP. At the behest of the academic community in São Paulo, the Ministry of Science and Technology set up the National Research Network (RNP), which similar to CGI.br, coordinated efforts for increasing Internet access in Brazil. The RNP made the first connections within eleven of Brazil's states, with points of presence (POP) in their capitals. The RNP faced hurdles because it was dependent on state funding for

infrastructure development and its task of creating Internet backbones took longer than expected, and only first became operational in 1992.

That same year, Internet development received a push in the lead up to the Earth Summit. The presence of thousands of journalists prompted Embratel to make investments in TCP/IP infrastructure and for the first time enabled non-academics to use the Internet in Brazil. In the following years, infrastructure development increased and the RNP backbone had 10,000 hosts by 1995. That year was also the first for commercial Internet by Embratel. Then President Fernando Cardoso and the Minister of Communications Sergio Motta were concerned that Embratel would have a monopoly on Internet service in Brazil, and established Norm 004-1995 that stated that Embratel could not charge higher fees to Internet users. In turn it encouraged the development of small and medium-sized ISPs which have come to define access in Brazil. The same year, the CGI.br was established to monitor infrastructure developments and coordinate privatization and increased access. It is comprised of members of the government, telecom companies, backbone operators, ISPs, universities, and users (Virtual Brazil) and to this day provides extensive reporting on access, quality, and innovation.

In 1997, Brazil created Anatel under law 9472 "as the regulatory agency charged with defending the interests of the State and the citizen, encouraging competition, universalizing telecommunications services, and updating telecommunications technology (Knight 829-831)." When Embratel was privatized, MCI purchased the company and expanded backbones at a much faster rate. Commercial Internet quickly expanded, and Peter Knight, author of the *Internet in Brazil* (2014), explains what the Brazilian ICT market today looks like:

> There is considerable competition between the four major mobile providers (Oi, TIM, Vivo, and Claro), and in some states smaller operators. But for fixed-line telephone and internet service the regional incumbents, Vivo/ Telefônica and Oi, enjoyed near monopolies in their regions for some years, having extensive fiber and microwave backbones and last mile copper networks in the richest markets. Like incumbents in the United States and many other countries, they find ways to resist "unbundling", to maintain market share, despite legal obligations to do so. (849-853)

Instead, Anatel has encouraged the development of small and medium-sized ISPs in order to provide service in markets that otherwise would go underserviced. Both Anatel and CGI.br carried out consultations on the Marco Civil da Internet.

Internet Penetration and geographic divides. Freedom House (2015) reports that while access in Brazil is increasing rapidly, it is still relatively low compared to OECD states. Estimates among different agencies report similar figures; the ITU reports a rate of 57 percent in 2014 compared to the CIA's estimate of 53.4 percent. The CGI.br's 2015 report (Barbosa) on Internet access gives a base figure of 50 percent of households having Internet access. These figures have grown considerably; in 2014 the ITU reported 51 percent, a significant increase from 40 percent in 2009.

Mobile broadband is gaining traction in Brazil as the preferred method of access, with only 2 percent of users dependent on slower dial-up service (a figure comparable to the US). Fifty-three percent of users had 3G connections, with 6.8 million lines capable of 4G-LTE. By May 2015 mobile phone use grew at a rate four times the global average, increasing 12.5 times between 2010 and 2015 (Mediatelecom). While the state touted the rollout of 4G in anticipation of the 2014 World Cup, the success of such advances were limited. Instead, it was used in mainly urban centers like São Paulo because of the lack of available infrastructure and the fact that users would have to purchase new mobile phones in order to take advantage of 4G.

Internet penetration is hindered by various manifestations of the digital divide. Alexandre Barbosa of the CGI.br reports in 2014 that significant portions of the Brazilian population are excluded from meaningful access "due to barriers such as cost of access, lack of coverage and lack of skills (175)." Increasing numbers of Brazilian youth and rural populations are becoming connected through mobile devices; 76 percent of the population uses their phones to connect to the Internet, and 84 percent of those users access the Internet almost every day. Socioeconomic status (SES) is a good predictor of access:

> Inequalities by social class and areas persisted: In class A, the percentage of households with Internet access was 98%; in class B, 82%; in class C, 48% and in classes D and E, 14%. In urban areas, the percentage of households with Internet access was 54%, while in rural areas this figure was 22% (176)[27].

Geographical barriers to access are compounded by SES markers that exacerbate the digital divide.

Figures for Internet penetration are based on the five regions in Brazil that date back to colonial times. The North is the second least populous state, characterized by an agrarian economy that

[27] Social classes are based on gross monthly income. Class A: over 10.200 BRL ($2,717), Class B: over 5,100 BRL ($1,359), Class C: 2,040 BRL ($543), Class D 1,020 BRL ($272), and Class E: below 1,020. (Novais)

contributes the least to the GDP and is comprised of indigenous tribes. The Northeast was important in Brazil's early history, with Portuguese colonists traveling there to harvest sugarcane using slave labor. Today, its economy stagnates but like the North region, industries are migrating to the region in search of tax breaks. The Center-West is least populated with a mixture of indigenous populations and *bandeirantes*, or scouts, that came in search of gold in the 19th century and depends on commercial livestock. The Southeast is the economic heart of Brazil, comprised of both São Paulo and Rio de Janeiro, "operating in segments of steel, metallurgical, automotive, computer technology, food, petrochemical, and many others (Duran)." It is also ethnically diverse, being the destination of immigration flows from Europe through the 19th and 20th centuries. The South was controlled by landowners, and is still characterized by agricultural production along with other forms of industrial production.

Table 2 Brazil ICT Household Survey with Access to the Internet 2014
(Barbosa 322)

Household access of the Internet?		**Yes**	**No**
	Total for Brazil:	50	50
Area	Urban	54	46
	Rural	22	78
Region	Southeast	60	40
	Northeast	37	63
	South	51	49
	North	35	65
	Center-West	44	56
Family Income	Up to 1 Minimum Wage (MW)	17	83
	More than 1 and up to 2 MW	37	63
	More than 2 and up to 3 MW	59	41
	More than 3 and up to 5 MW	89	11
	More than 10 MW	95	5
Social Class	A	98	2
	B	82	18
	C	48	52
	DE	14	85
Base: 65, 129,753 households. Data collected between October 2014 and March 2015			

With the background of these regions accounted for, analysis of the proportion of households with access begins to come into focus. The region with the largest percentage Internet access, 60 percent, is the Southeast, comprised of many of Brazil's major metropolises (São Paulo, Rio de Janeiro, Belo Horizonte, along with 7 others with populations ranging from approximately 700,000 to 1.2 million). The next is the South, with 51 percent, that has traditional sources of wealth and sophisticated industrial capacity. The

North, Northeast, and Central-West regions comprise large swaths of land with underdeveloped economies and large portions of their population falling into “C” social class and below. Combined, these factors easily predict these regions to have lower rates of access.

Wood and Mourão pose several questions regarding digital inequality in Brazil, highlighting the indispensable nature of Internet access and technological literacy to employment and political participation. They ask: “Has the increase in computer ownership and Internet access widened or narrowed the digital gap between geographic regions of the country, and between the rich and the poor subgroups of the population (120)?” Such a question reflects the disparate theories of Internet penetration from Sujarwoto and Tampubolon (2013), particularly the diffusion thesis that theorizes differences in SES will be reflected in Internet access rates. While Wood and Mourão concede that geographic and SES disparities in access remain intact during the course of the longitudinal study (between 2004 and 2009), the gap is decreasing. The authors’ apparent positive bias is shown in their argument about Brazil’s emerging role in global trade and a harbinger of Internet freedom characterizing the “breathless excitement” that surrounds outsiders’ perspectives of Brazil, at least until 2013. The validity of such a study’s conclusions is therefore questionable.

Speed and cost. Knight reports that the price of access in Brazil is relatively high for the region and the globe. The average cost per megabit of data is $25, while in the US it is $3.33. Additionally, quality is often at issue with dropped calls and slower speeds than advertised. In 2012, the state intervened on the behalf of consumers, and by 2014 ISPs are required to provide 40 percent of contracted download and upload speeds at any given moment (called instantaneous speed), and 80 percent of the contracted speed on average as measured over a month (Knight 1615). Numbeo reported that a 10 Mbps wired connection, either through cable or DSL, would cost $19.80, or 4.3 percent of an average salary. Costs may have gone down since Knight’s study, or the self-reported nature of Numbeo statistics might be skewed to urban populations.

Akamai reported average speeds in Brazil to be 4.1 Mbps (Q4 2015), which is far below the recommendations made by the FCC. Peak speeds for users topped at 30.3 Mbps, which was a 38 percent increase from the previous year.

Table 3 Reported Internet Speeds in Brazilian cities
(Testmy.net 12 April 2016)

City (Region)	Downstream	Upstream
Rio de Janeiro (Southeast)	8 Mbps	1.5 Mbps
Belo Horizonte (Southeast)	7.9 Mbps	1.8 Mbps
Curitiba (South)	7.9 Mbps	1.8 Mbps
Fortaleza (Northeast)	7.4 Mbps	938 Kbps
Manaus (North)	5.9 Mbps	632 Kbps
Natal (Northeast)	5.0 Mbps	862 Kbps
Campo Grande (Central West)	4.4 Mbps	625 Kbps
Araripina (Northeast)	1.1 Mbps	1.1 Mbps
Ipatinga (Southeast)	899 Kbps	303 Kbps

Speeds for fairly populous cities remain rather consistent, though they are in fact slower in traditionally disadvantaged regions. Users running a 5.0 Mbps connection in Natal may not notice much of a change if they found themselves in Rio. Cites observed with smaller populations generally have connections that are poor with average speeds of 1 Mbps or less.

State Policy Regarding Internet Penetration and Use

Despite the digital divide that persists in Brazil, is it possible to account for its dramatic narrowing and the relatively uniform and fast speeds of which Brazilian infrastructure is capable? There are many government-directed or coordinated initiatives that address these issues, including a National Broadband Plan, tax incentives, a rural broadband campaign, and partnerships with social media giants like Facebook. As a preliminary comparison, the difference between Brazilian and the US's political culture is evident in the acceptance of the enlarged role of the state in assisting the private sector.

National Broadband Plan. The Ministry of Communication initiated a "National Broadband Plan" (Programa Nacional de Banda Larga [PNBL]) in 2010, decree number 7,175/2010. Its goals were to increase broadband access in rural and remote areas and to incentivize ISPs and telecoms to make appropriate investments to make 1Mbps available for R$35 for 40 million households by 2014. By June 2014, they report 3,406 cities with broadband access and 118 cities with 4G. The relative success appears impressive if slightly uneven, with growth ranging from 702 percent increase in the South to 969 percent increase in the North (Ministry of Communication 11-12). Critics state that while the plan had good intentions, only 7.9 percent of the increases in broadband availability could be traced back to

contracts with participating ISPs to PNBL and only 0.6 percent through mobile phones. According to a lawyer for a consumer watchdog group, these plans were "hidden" because they were economically unappealing to ISPs, and that it is the direct responsibility of the state, rather than telecoms, to provide meaningful access to its citizens (Bruno). It is unsurprising that the Brazilian ISPs might balk at the plan that promises users increased access at the potential expense of providers (Knight 1474-1479).

Tax incentives. The state has used the power of taxation in ways that are meant increase innovation and access. Part of the PNBL's methods to increase access using tax incentives; early 2013 the REPNBL[28] reduced taxation on ISPs that were building infrastructure. A decree further used taxes to incentivize the increase in hardware ownership through a decree (7981/2013) that exempted select smartphone technologies from taxation at their point of sale. In order to encourage ISPs to make meaningful connections available to public schools, cost deferment and lowered tax obligations are provided by the state in order to connect both underserved urban and rural schools (Knight).

A rural broadband plan was launched in July 2015 in order to introduce 4G in the isolated areas of the state of Goiás and the Federal District, both located in the Center-West region. While Brasilia was created in this region in 1960, it is in an otherwise desolate place in Brazil. Access is carried out by Oi, one of the country's leading ISPs, and matches efforts in other states of the country, including Maranhão, Rio Grande do Sul, Mato Grosso and Mato Grosso do Sul, at a total cost R$526.4 million, or $141 million. Under the PNBL, this project is projected to serve 1,611 municipalities (Grossman).

Free Basics. Facebook CEO Mark Zuckerberg made an agreement with President Rousseff in April 2015 to introduce Free Basics into one of São Paulo's populous but poor areas, Heliópolis. By offering free access to basic services like e-government, e-health, and social media, Facebook would benefit from increased advertising revenue in addition to perceptions of corporate social responsibility. "[T]he Minister of Science and Technology, Aldo Rebelo, said the initiative is one of the symbols of democratization efforts must be made to transform science, technology and innovation in accessible services to the population (Castro)." But as elsewhere, the program is criticized for violating the principles

[28] Regime Especial de Tributação do Programa Nacional de Banda Larga para Implantação de Redes de Telecomunicações

of net neutrality, and perhaps even the control of powerful actors (be it state or social media giant) over what users can access for free. Such a model could be replicated by states to limit users' experiences.

PPPs. The Brazilian state, along with other stakeholders, has taken steps to overcome the digital divide in rural settings. The "Piraí Digital City" project celebrated a 10-year anniversary in 2014, which transformed the small city (population 24,000) that struggled with economic crisis and unemployment to becoming "one of the world's most fascinating Intelligent Communities (Jung 2014)." The municipality partnered with educational centers, federal, municipal, and business entities to improve digital literacy and provide access to necessary technologies. Intel provided 5,500 Intel classmate PCs and worked with school administrators and teachers on how to transform pedagogy to teach students to use and innovate with technology (Coelho et al).

In the same year, Carvalho et al report on the experience of a public-private partnership in Northeast Brazil. The Cinturão Digital do Ceará Network (CDC), or Cinturão Digital Belt was an infrastructure project aimed at building out a WiMax fiber cable system capable of speeds between 30-40 Mbps. Since the government financed the cable's construction, the usual private industry concern of cost outlays and immediate profitability were not present. The arrangement called for small to medium ISPs to lay new cable for last-mile service, provided they conformed to technical standards. By 2014, "the network initiated by ETICE has been expanded by about 25 percent through this type of arrangement (11-12)." The authors argue that such arrangements can be replicated outside Brazil in order to overcome geographic divides.

Due to economies of scale, the larger the number of partners between the public and private sector the easier and cheaper it is to provide infrastructure to underserved areas thereby increasing Internet penetration. Knight relates the story of Adilson Klaffke, who runs a small-scale ISP in Nova Guarita, a town of 2,500 in the Central West region.

> "I provide better quality service than Oi", says Adilson. "With this I can win clients in the *agrovilas*." Even the Transportation Department (Detran) in the town uses my service. Previously, Detran would not issue documents because it had no access to the Internet." Now the farmers use their connections to order agricultural inputs and to access technical information, weather forecasts, news of Brazil and the world and to maintain contact with relatives and friends in the South of Brazil (987-991)

By purchasing licenses from Anatel—the independent government agency in charge of granting, regulating, and supervising telecommunications in Brazil—entrepreneurs are able to provide service in

areas that otherwise go unnoticed. While Knight implicitly argues that this model could also be replicated in the US, he fails to account for the limitations in American ideology regarding political economy.

Marco Civil da Internet

For nearly two years, the Civil Rights Framework for the Internet had been the topic of discussion for Brazilian Internet policy and its implications for the world. Conceived in 2007, the bill entered into law in April 2014 and is called by some "The Internet Constitution" of Brazil. While it has received some criticism, it is viewed as a new model for domestic Internet policy that champions net neutrality, privacy, and a multistakeholder approach into ICT development and governance.

The push for the law came from an article by Professor Ronaldo Lemos of the Rio de Janeiro State University Law School that criticized steps being taken by the Brazilian government regarding cybercrime. The proposed bill would have criminalized certain activities on the web that he theorized would have had a spillover effect into the entire industry. Without a civil framework in place he argued the bill would harm entrepreneurs and end users, crushing innovation and efficiency.

> …it is increasingly clear that the criminalization and the restriction of "access", as does the bill in question, is contrary public and collective interests. Consumer protection associations worldwide, together with librarians, universities, companies and academic institutions, among others, have spoken out consistently in raising the barriers and red tape access. One example is the successful consumer pressure exerted on the Apple company, which is progressively abandoning the use of measures that hinder access to your content (so-called "technological protection measures") (Lemos).

Lemos questions the legality of surveillance and finally suggests that any new measures that could threaten Internet freedom should require multistakeholder input. The law's initial proposals were the result of coordinated efforts between the Fundação Getúlio Vargas,[29] of which Lemos is member, and the Ministry of Justice.

While the draft of the Civil Framework contained extensive protections for users, its exceptional nature is due to the invitation for direct public input. It consisted of two rounds on *Pensando o Direito*[30] that were not supposed to be either "chats" or referenda. Instead, it called for meaningful contributions to the various axes of the laws regarding Net Neutrality, Privacy, Data Log Records and Other Topics (Pensando o Direto; Gatto). The dedication to liberal norms on the Internet was explicit and

[29] A nearly 70 year-old institution, the Getúlio Vargas Foundation mission was to prepare for public and private administration, economics, psychology, accounting, education, and ICTs (FGV).

[30] Thinking Directly/Right/Straight. Run by the Ministry of Justice.

unmistakable: “Once more, we count on your contribution to strengthen internet democracy!” The first round took place in 2009 and received 800 comments, while the second phase took place in the following year and received over 1,200 substantive comments (Pensando o Direto 2015). On the one hand, these numbers are low considering that they are worldwide statistics and that São Paulo has a population of 21 million people alone. But on the other hand, the call from the Ministry of Justice was for substantive commentary that would be seriously considered when drafting legislation, and typically such responses were to be from stakeholders or those that truly cared about the outcome of the bill. Despite the relatively small amount of comments, even with thousands of page hits, the potential for public input on Internet legislation is remarkable.

Different articles received varying amounts of attention. For article 2 on guaranteeing the freedom of expression, citizens were concerned that privacy and anonymity should be aligned with other high-level civil rights like the freedom of expression. By aligning freedom of expression with privacy, users emphasize a frame articulated by Frank La Rue and the Human Rights Council in 2013 that aims to guarantee that freedom of expression is protected from state intrusion.

After these two rounds of consultations, the law was enacted in April 2014. The timing was in line with the revelations that the US was monitoring Rousseff and her aides’ communications through the PRISM program. Demanding both an apology and an explanation but receiving neither, Rousseff cancelled a diplomatic trip to Washington, DC planned for November 2013. During the Brazilian-led world forum on Internet governance, NETmundial, the law was enacted in an apparent attempt to set Brazil apart from other global leaders. The resulting law, 12.965, was enacted on 23 April 2014. Article 2 states:

> The discipline of internet use in Brazil is founded on the basis of respect for freedom of expression, as well as:
>
> I – the recognition of the global scale of the network;
> II – human rights, personality development and the exercise of citizenship in digital medias;
> III – plurality and diversity;
> IV – openness and cooperation;
> V – free enterprising, free competition and consumer protection; and
> VI – social purpose of the network.

Significant for this study, the framework asserts a multitude of rights and duties surrounding the F2C. These include: a right to access (Art. 4§1.), the diffusion of new technologies and types of access to all

(Art. 4§3.) which addresses the digital divide, inviolable rights to privacy except by express consent (Art.7 §2, §7.), that the maintenance of quality of access are part of what makes access meaningful (Art.7 §5.), and that the state is obligated to develop and promote the Internet and ICTs (Articles 27 and 28). The document further provides protections for net neutrality, data retention including foreign entities, and judicial requests for records.

The development of the Marco Civil continues as the state encourages public input for advancing strategies for implementation of the laws. The proposals were open between February and May 2015, and encouraged "Any person, institution, company or government agency… [to]…make a proposal on how to be the regulatory decree Civil Marco." The Secretary of Legislative Affairs Gabriel Sampaio called for implementation to be a similar democratic process. According to "The Debate by the Numbers," 339 guidelines were proposed and 1,109 comments were received over 17 weeks. The largest concerns reflected the issues of privacy and user safety, followed by inclusion and net neutrality. Concerns over the guarding of records ranked only 9th, perhaps evidence that safe harbor rules and who has control of whose information is a concern of states and international relations, and has little apparent direct impact on users.

Soprana reports that in April 2016, a new proposed cybercrime bill could "mutilate" the legislation. Like the Stop Online Piracy Act that was before the US Congress in 2011, the bill is meant to protect intellectual property but extends police powers on the web. The proposed bill is the result of the parliamentary commission and demonstrates a pluralistic tendency highlighted by liberal IR theories generally. It is possible to have the Marco Civil da Internet and such a bill develop in the same country. Tim Berners-Lee wrote an open letter encouraging the tabling of the bill, and if the development of the Framework is any indication, it is likely that this bill will receive extensive revision to bring it in line with the greater vision of Internet freedom in Brazil.

The Marco Civil da Internet is one of the most direct articulations of the Freedom to Connect and larger Internet freedom concerns in the world. It expressly guarantees access, places the duty on the government to overcome the digital divide, and encourages the equal development and implementation of new technologies. Moreover, it forbids the powerful actors—the state and ISPs—from controlling the net or circumscribing access by assuring privacy, guaranteeing net neutrality, and encouraging fair

competition. The successful implementation of these guidelines is far from assured—politics has a stubborn way of intruding into the utopian world of norms—but the multistakeholder approach has invited public participation at nearly every step of this process. It may lead to feedback loops that would allow space for continued public critique of government failings to live up to the Framework. "…the real challenges come in interpretation and enforcement. It's up to Brazil's engaged citizens to make sure that the law and upcoming legislation upholds the high standard its creators set (Pinho and Rodriguez)."

Domestic attitudes

There is something inherently unique about Internet policy in Brazil, including its early history of ICT professionals promoting coordinated multistakeholder efforts to develop the Internet in the 1990s and more recently the Marco consultation process. Most analyses have focused on government policy to coordinate these efforts, but have not touched directly on the source of the apparent public enthusiasm. Knight (2016) suggested in response to this query that "multistakeholderism in Brazil is the result of early efforts of Internet pioneers which reflected "the best of the vision of the Internet's founders in the US and Europe." They were able to force reluctant government embodied in Embratel to provide the necessary linkages to the Internet at an early point in its history in Brazil. CGI.br, as a multistakeholder institution, was created three years before ICANN, and is reflected in continued efforts to incorporate private enterprise, NGOs, and the government.

While there were notable efforts in the US against controversies like net neutrality and ISP mergers, the inclusion of the public in Internet policy is absent. Indeed, Forbes reported on a WSIS+10 meeting taking place in December 2015 discussing Internet governance, subtitling the story "But Nobody Seemed to Care." The inattention may be the result of contemporary high-level events, terrorist attacks and climate talks, but also may be the result of the lack of concern on the part of the American public about Internet governance. What makes Brazilians apparently so different? Knight argues that the US and Brazilian models are not so different, as both pursued Internet development under the multistakeholder model. Yet such a broad view ignores the lack of NGO and governmental input on later Internet infrastructure development in the US as there has been in Brazil, and the fact that no such framework of Internet rights has been proposed in the US still begs the question of why. Knight indirectly argues that the NETmundial and the Marco Civil da Internet was enabled by the window of opportunity

presented by the Snowden revelations, but the fact that they were pursued at all is left unexplained by mere circumstances. An examination of survey data proves helpful.

The CGI.br, in conducting its analysis of Internet access in Brazilian households determined that the growth in Internet access, particularly via mobile phones, meant primarily that people would be more connected with each other through instant messaging and social media outlets like WhatsApp and Skype. While receiving phone calls, taking photos, and sending text messages are the most common activities, more users are using their phones to access the web and send emails. The only other useful indication of how users in Brazil use the technology was how many used e-government services. Unfortunately, such studies do not appear to conduct surveys about how people feel about the importance of access or policies that the state undertakes concerning access.

Two other sources are tangentially relevant. First, ahead of the World Economic Forum in Zurich in January 2015, Microsoft Executive VP Mark Penn presented a survey of 12,000 Internet users across the world. His conclusion was that there is a clear dichotomy between Internet users in the developed and the developing world, with users in the latter tending to be more optimistic and trusting of the information. For Brazil, Penn reports that 63 percent felt the Internet had a positive impact on social bonds, 42 percent thought it had a positive impact for trust in the media, 54 percent thought technology negatively impact privacy, 53 percent thought current legal protections were insufficient, and 76 percent felt they were not aware of all the activities associated with collecting personal information. Thus, while Brazilian Internet users, like the rest of the developing world as labeled by the study, were optimistic about the role of the Internet in improving everyday life, they were increasingly wary of the risk it poses to civil liberties.

Several studies dating to 2010 touch on Internet users' appraisal of the importance of the Internet in their lives, its relation to human rights, and the role of government that facilitates access. GlobeScan's 2010 survey revealed that most Brazilians felt that Internet access should be considered a human right, with 91 percent of respondents saying they agreed with the idea. Unlike Mexico, however, in that 71 percent said they could cope with out it (compared to Mexico's 17 percent). Fifty-three percent argued that the Internet's content should never be regulated by the government, a similar figure to those who argued it was "Very important" in the Internet Society's 2012 survey. In that same survey, Brazilians

revealed their belief in the appropriate proactive role of government provision of access, with 91 percent arguing that government should provide or enable cheaper computers, 90 percent arguing that it should encourage competition among providers, and 87 percent arguing that "My government has an obligation to ensure that I have the opportunity to access the Internet." In relation to rights, 86 percent argued that that access should be considered a right, 85 percent agreed that expression should be protected on the medium, and 87 percent saw social media playing a positive role in assuring freedoms of association and assembly. Slightly less than half (49 percent) would accept any or significant increases in government control in the name of security, and 70 percent thought that the government had the right to govern the internet the way it sees fit, making Brazilian opinion about average. In surveys in both 2014 and 2015,[31] Brazilians consistently expressed the idea that content should remain uncensored, at 80 percent and 84 percent, respectively.

Pew (2015c) asked directly about American spying. Overwhelmingly, Brazilians disapproved the collection of data by the American government on them (94 percent), their politicians (83 percent), and on American citizens (84 percent). Most approved surveillance on terrorist suspects (67 percent), and in the wake of the string of terrorist attacks across the world in recent months, that number would likely increase if users were polled again.

Ruling the Internet? Domestic and International Rhetoric Surrounding the Internet in Brazil

USA Today published an article "Why Brazil May Rule the Internet" in June 2014. Such a provocative title may grab a reader's notice, but the idea of "ruling" is in itself misleading. One state cannot rule the Internet as it functions today, but the frame harkens to state-centric analysis of international relations. Instead, Brazil is presenting a challenge to states that claim norms of cyber sovereignty like Russia and China in addition to the apparently hypocritical policies of openness proclaimed by United States and the United Kingdom alongside extensive surveillance programs. Although not examined in this study, Internet governance is often aligned between the multistakeholder model of ICANN and the state-centric model of the ITU. Brazil is presenting itself as a champion of norms

[31] Pew 2014b and Pew 2015b

surrounding Internet freedom, unsullied by accusations of spying and itself a victim of the disparity of power on the web, at least for now[32].

While Brazil has a long history of trying to conform to Internet freedom norms—Cadei points back to early popular adoption that was enabled by Brazil's ICT professionals in 1992—it was the Snowden revelations that set Brazil's alternative apart from dominant views. For many states, including Russia and China, the NSA's spying and the lack of apparent privacy protections on the perceived US-dominated Internet was a window of opportunity to take action. For illiberal states, this action reinforced cyber sovereignty norms under the rubric that the US was pursuing its own national security interests on a relatively open network which needed to be reined in and controlled directly by states. Brazil, and particularly Rousseff, took an alternate approach, calling for stronger protections to Internet freedom in the face of its violation by powerful states.

In September 2013 of Rousseff and Angela Merkel, another high-profile victim of PRISM surveillance, went before the 68th session of the UN General Assembly to decry the US program and call for the protection of Internet freedom norms. They asserted first that privacy was directly related to freedom of expression, and that in its absence it would severely inhibit democracy. Second, the pursuit of national security aims never justifies the violations of human rights in another country (Donahoe and Canineu). They introduced the first resolution on privacy in the General Assembly in 25 years (68/167). In April 2014, Brazil hosted NETMundial in order to establish a multistakeholder model of Internet governance. Cadei reports that the substance of such an argument is not much different from the model of ICANN, but perhaps a more sincere one which invited true discussion and critique of the abuses by other states.

By November 2014, another resolution was adopted (69/166) relating to "privacy in the digital age." Minárik reports that this resolution coincided with other reports that had been filed the UN, like La Rue's reports to the HRC, and that it took tentative steps chastising the "Five Eyes" of the Internet[33]. The resolution connected privacy on the web to the UNDHR, the ICCPR, the ICESCR, the Vienna

[32] A bill entered the Brazilian Congress in October 2015 that would increase penalties for libel and defamatory speech on the web and allow prosecutors access to users' personal data. It has not entered into law (Aviles et al.)

[33] An intelligence sharing arrangement among the US, UK, Canada, Australia and New Zealand based on the collection of metadata typified in the PRISM program.

Declaration, and an HRC resolution from June 2014 call for the protection of human rights on the web. It called upon a need to analyze how rights can be protected in the digital age, the need for domestic oversight, and the lawfulness of surveillance. Even the F2C is directly commented upon: "*Stressing* the importance of full respect for the freedom to seek, receive and impart information, including the fundamental importance of access to information and democratic participation." Finally, the resolution calls upon states to assure that domestic legislation, particularly on surveillance, conforms to international human rights law.

As a critic of powerful states' surveillance practices by sponsoring these resolutions, speaking before the General Assembly, hosting NETmundial, and finally passing the Marco Civil da Internet, Brazil is positioning itself as champion of Internet Freedom. Several journalists agree[34], calling it a "leader," "ruler," and "champion," in turn. Alves reports that Rousseff claimed that the Obama Administration itself was not to blame for the lapse in human rights in the wake of the Snowden revelations. She recognized that the policies that enabled surveillance were put in place in the post-9/11 era of legislative disregard for civil rights. It is common for many to consider civil or human rights as secondary concerns in an age where national security is placed in the forefront.

***

Brazil is a global leader in Internet freedom and the F2C due to its long history of partnership among the state, private sector, and NGOs. The Civil Rights Framework, the continued importance of the Internet steering committee, its record of collecting Internet penetration data, and tax incentives are all measures that illustrate the effects of the F2C. One can attribute the success of Internet freedom in Brazil to the social democratic norms that characterize the Brazilian economy and relationship among the government, private sector, and citizens. However, while many sectors of Brazilian society champion freedom on the web, there are others that move to strike it down. The April 2016 cybercrime bill could harm the implementation of the Marco Civil da Internet, but first, the outcome of this legislation is uncertain, and second, Brazil would not be alone as state whose disparate agencies worked at cross-purposes. The US, the Philippines, Mexico, and Indonesia all, in different ways, go through similar processes.

[34] See Bertoni (2013) Cadei (2014a 2014b), Engel (2014)

The Philippines

While the Philippines is categorized as Free in Freedom House's ranking, there are numerous challenges that inhibit Internet access across the state. Unlike cases in the Partly Free and Not Free categories, with some minor exceptions, the Philippines does not regularly limit content or violate users' rights. Instead the limitations on Internet penetration that plague every case examined are exacerbated in the archipelago, as a consequence of geography, duopoly, and government malfeasance. Partly a result of history, and partly the effect of the continued concentration of power and the lack of government regulation, the Philippine telecom industry is inefficient, unreliable, and ultimately inadequate for the state's economic development goals. Nonetheless, there are signs that both the government, and more importantly, Filipinos themselves, are demanding more access, better speeds, and lower costs.

Background

The Philippines is a relatively small and developing state, struggling to overcome the dual legacies of colonialism and two decades of martial law. It has a population of 100,998,376 (13th in the world), and takes up an area of 300,000 km^2 (73rd in the world). It is an archipelago with more than 7,000 islands, much like Indonesia, which complicates the dispersion of information technology. It has the lowest urban population in this study, totaling 44.4 percent, with only four major metropolises with populations of about 1 million or more[35], although metro Manila dwarfs other cities with a population of nearly 13 million. The administration of the state is complicated, with 81 provinces composed of cities, municipalities and barangays (villages), 145 independently administered cities, and one autonomous region of Muslim Mindanao. Additionally, the state is informally divided among three island groups (Luzon, Visayas, and Mindanao) along with 18 nongovernmental regions. Its annual GDP is $693.4 billion, ranking it 31st in the world with a GDP per capita is $7,000 ranking 153rd in the world.

The Philippines has 3.09 million landlines, ranking 47th in the world; one phone is plugged in for approximately every 3 people in the country, a figure that has vastly improved in the past several decades. It escalates for cellular phones, with 111.3 million in the country, placing it 13th in the world. There are 112 subscriptions to mobile service for every 100 people, and the Philippines has been colloquially referred to as the texting capital of the world. There are 39.2 million Internet users in the

[35] Manila (capital) 12.946 million; Davao 1.63 million; Cebu City 951,000; Zamboanga 936,000 (2015)

country which ranks the state 17th in absolute numbers, and totals 39.4 percent of the population. Users are concentrated in major cities where infrastructure is widely available. The World Bank reports that 63 percent of Internet users in the Philippines rely exclusively on mobile connections for access.

Human rights in the state have a mixed history. As first a colony of Spain and then ruled by the US in the 20th century, it is a state long associated with and influenced by the West. The 20th century was marred by a "soft" dictatorship that truncated rights in the name of stability and security from the threat of violence posed by communists, Muslims, and Christian extremists. Today, the Fifth Republic is rife with criticism: politicians promise much and deliver little. Accusations of corruption and a tendency to be more responsive to entrenched interests continue the legacy of cronyism that has existed since before the Marcos regime. The failure of the Ramos, Estrada, and Arroyo administrations to meaningfully address poverty and inequality are correlated to the nature of the ICT market today. The legal structure for substantive democracy and the protection of human rights exists in the Philippines, but it is up to its citizens to demand the necessary changes in order to break down the system that keeps small portions of the population rich and powerful. Indeed, things seem to be getting worse: "… most countries in South-East Asia, including Indonesia, Thailand and the Philippines, saw their scores [on our crony-capitalism index] worsen between 2007 and 2014, as tycoons active in real estate and natural resources got richer (The Economist 2014a)." This legacy is also reflected in the telecom industry.

The Internet in the Philippines

Background. The Philippines is unique in this study where computing was not pursued under the auspices of a university or even as the hobbies of ICT enthusiasts. Instead, IBM introduced the first computer system to the Philippines in 1960 for a government office, the Bureau of Lands, "to handle the country's land survey computations." In the following decades, IBM installed computers in some university settings, but largely in the industrial and financial sectors. In 1969, Marcos and IBM World Trade Chairman Arthur K. Watson officiated at "the dedication of a new headquarters for IBM Philippines in Makati, outside Manila," suggesting some personal connection or benefit for the dictator.

The Internet was preceded by online bulletin boards, the first of which went online in 1986. FidoNet Exchange was created one year later to connect several boards across Manila. In 1990, the Ateneo Computer Technology Center of Ateneo University in Quezon launched an initiative exploring the

possibility of setting up an academic network among Philippine universities and government offices, but it was never pursued. Between 1991 and 1993, email gateways and UCCP protocols were introduced by MNCs like Intel, Motorola, and Texas Instruments. Initiated in 1993, the Philnet project connected university students via email through Ateneo's gateway, preparing for the launch of the Internet in 1994. Jim Ayson of the University of Ateneo recounted the first connection to the Internet on his blog. Philnet, the Department of Science and Technology, and the university joined the Internet through SprintLink's connection in California.

> Subject: The Philippines is In!
> As of March 29,1994 at 1:15 am Philippine time, unfortunately 2 days late due to slight technical difficulties, the Philippines was FINALLY connected to the Internet via SprintLink. The Philippine router, a Cisco 7000 router was attached via the services of PLDT and Sprint communications to SprintLink's router at Stockton Ca. The gateway to the world for the Philippines will be via NASA Ames Research Center. For now, a 64K serial link is the information highway to the rest of the Internet world (Ayson).

Internet penetration and geographic divides. As reported above, Internet penetration in the Philippines is slightly less than 40 percent of the total population, the lowest overall rate in all the cases explored, save Cuba. The CIA and ITU figures agree, at 39.4 percent and 39.69 percent respectively. The total has grown considerably since 2000 when the ITU reported a rate of just 1.98 percent; it climbed to 5.4 percent by 2005, and to 25 percent by 2010. While mobile penetration is high, smartphone penetration is low at 15 percent.

"Nonetheless, the term 'unlimited' needs a qualifier," according to Ferraz, "the internet is naturally limited by a given person's relative patience for its stop-and-go, spotty nature (Ferraz)." In 2011 Smart Communications controlled 52 percent of the mobile market, which is a subsidiary of the Philippine Long Distance Telephone Company (PLDT), followed by its closest competitors, Globe and Digitel each having a 16 percent share of the market. When PLDT acquired Digitel, PLDT's market share grew to 67 percent of the mobile market (Paul Budde Communication Pty Ltd), nearly mirroring its control of landlines. There is a possibility of a shakeup of this situation. Venzon reports that San Miguel, one the Philippines largest corporations, bought Vega Telecom with the hope of challenging the duopoly. It plans to launch mobile broadband early in 2016, and "[a]mid rising smartphone usage, PLDT and Globe have offered free Internet access to win subscribers in a market where there are more mobile phones than users."

Due to the complex structure of the Philippine state, it is difficult to the pinpoint the areas of weakness of Internet penetration across the archipelago. The Philippines Statistic Authority presents statistics for Internet penetration in cities, provinces, and municipalities and the level of its sophistication, reproduced below.

Table 4 Internet penetration and sophistication in the Philippines
(Mitra and Miraflores)

Percentage of cities with web presence						
	2011	**2012**	**2013**	**2014**	**PDP target for 2016** [36]	**Probability of reaching PDP target**
At least Stage 1 (emerging)	72.39%	80.85%	85.42%	87.5%	100%	
At least Stage 2 (enhanced)	53.73	53.73%	56.25%	56.94	N/A	
At least Stage 3 (interactive)	22.39%	22.39%	15.97%	15.97%	N/A	
At least Stage 4 (transactional)	2.24%	0.00%	5.55%	5.55%	N/A	
Percentage of provinces with web presence						
	2011	**2012**	**2013**	**2014**	**PDP target for 2016**	**Probability of reaching PDP target**
At least Stage 1 (emerging)	73.75%	76.25%	65.85%	68.29%	100%	
At least Stage 2 (enhanced)	51.25%	51.25%	36.60%	39.02%	N/A	
At least Stage 3 (interactive)	18.75%	23.75%	24.39%	23.17%	N/A	
At least Stage 4 (transactional)	1.25%	0.00%	1.22%	1.22%	N/A	
Percentage of municipalities with web presence						
	2011	**2012**	**2013**	**2014**	**PDP target for 2016**	**Probability of reaching PDP target**
At least Stage 1 (emerging)	23.47%	34.02%	35.72%	37.51%	100%	
At least Stage 2 (enhanced)	10.76%	16.00%	16.80%	17.64%	N/A	
At least Stage 3 (interactive)	1.74%	3.42%	3.60%	3.78%	N/A	
At least Stage 4 (transactional)	N/A	0.00%	1.50%	1.56%		

[36] Philippine Development Plan, 2011-2016

Sophisticated web presence[37] is nearly absent in all of the Philippines, and the division between urban and rural is pronounce. Cities appear to have the most sophisticated web capabilities in the state. The images of frowny faces are a unique attribute to an official government document, and are meant to indicate whether or not the projected figures developed in the Philippine Development Plan will be met by 2016.

There are no statistics for Internet usage according to province; a close approximation exists between fixed landlines located in rural provinces. When comparing poverty percentages to the ratio between population and the number of fixed lines, the correlation coefficient was 0.34, indicating a moderate relationship between poverty and fixed line availability—and therefore the prospects of having dial-up or broadband Internet connections (Tambasen).

Speeds and cost. Mobile access plans are relatively inexpensive and have unlimited access, with less than 3 percent of users paying more than $41 per month and nearly a third paying less than $12 per month. On the other hand, wired 10 Mbps broadband is far more expensive, averaging $44 per month or 14.28 percent of the average net salary (Numbeo)

Internet speeds in the Philippines are among the worst in the world and especially Southeast Asia. Akamai reports that the average speed in Q4 2015 was 3.2 Mbps, an 18 percent improvement from the previous year, while peak speeds topped out at 27.0 Mbps, which would meet the FCC's minimum standard for broadband. Only 0.8 percent of users regularly enjoyed speeds of 15 Mbps or more.

[37] "United Nations Department of Economic and Social Affairs (DESA) studies the idea of connected governance as the means to achieve maximum cost savings and improve service delivery. The concept of connected government looks towards technology as a strategic tool and an enabler for public service transformation, innovation and productivity growth.
DESA identifies five stages for connected government:
(1) emerging, (2) enhanced, (3) interactive, (4) transactional, and (5) connected.
According to DESA definitions, the "emerging" stage includes a basic web presence.
The ability to present documents or forms would be more advanced and, therefore, be part of the "enhanced" stage. During this second stage, users are not yet able to interact electronically with the administration. The establishment of interactive portals, websites or mobile applications would be representative of the third, "interactive" stage, while "transactional" relations would be part of DESA's fourth stage. The final stage of e-government combines vertical and horizontal integration with other capabilities, such as interoperability and the establishment of connections among several stakeholders (government, businesses, academic institutions, NGOs and civil society). E-participation – that is, the involvement of different individuals and groups in forming opinions and the decision-making processes through electronic means – is representative of the final "connected" stage (ITU OECD 27)."

Table 5 Reported Internet speeds in Philippine cities
(testmy.net 12 April 2016)

City (Region/Island Group)	Downstream	Upstream
Manila (National Capital Region/Luzon)	2.9 Mbps	1 Mbps
Quezon (National Capital Region/Luzon)	2.5 Mbps	787 Kbps
Davao (Region XI / Mindanao)	2.2 Mbps	573 Kbps
Baguio (Cordillera Administrative Region / Luzon)	2.2 Mbps	573 Kbps
Cebu City (Region VII/Visayas)	1.9 Mbps	705 Kbps
Dumaguete (Region XVIII / Visayas)	994 Kbps	286 Kbps
Cotabato (Soccsksargen / Mindano)	482 Kbps	193 Kbps

The major cities of Manila and Quezon enjoy the best speed capacities. Despite the size of Dumaguete and Cotabato cities with populations over 120,000 and 270,000, respectively, they lack of even minimal broadband speeds.

The Philippines has numerous submarine fiber optic cables (as with Indonesia), with ten landing points that connect with foreign sources and one domestic cable with thirteen landing points, owned by the PLDT. The landing points are concentrated in or around major cities like Manila, Cebu, and Davao. The PLDT owns the domestic cable linking Luzon, Visayas, and Mindanao, and it touts both this project and underground cables as ways to enhance *its own* network and offer little in the way of seeing these improvements as a manifestation of the F2C. Underground cables were adopted because of the prevalence of natural disasters, especially typhoons that routinely threaten the network and potentially disrupt communications in times of national emergency (Rapper). In 2014 and 2015, the PLDT rolled out separate networks in Northern and Southern Luzon along with submarine cables totaling approximately 1,000 kilometers (Agcaoli). The improvements are also framed in terms of competitiveness, “Nazareno said 2014 brought home the message that transformational shifts are taking place in the industry as the PLDT Group faces price competition in the cellular business as well as the impact of a new digital communications services offered by over-the-top players.” It is not likely that the PLDT upgrades, perhaps reflected in speed capacities recorded in Table 5, will benefit other telecoms or their customers.

The World Bank’s “Digital Dividends” report suggests three reasons why the Philippines lags behind the rest of the world in speed and availability. First, OECD countries had the advantage of preexisting fixed line access, with infrastructure that could be adapted to address changing needs. As shall be discussed, the ICT market in the Philippines has lagged in terms of infrastructure development

due to the nature of the marketplace. Second, while the government has taken steps to reform the ICT market, it is not enough for the World Bank, which advises making increasingly favorable conditions for competition. Third, the digital divide persists because of the lack of both basic and technological education. "...teaching advanced cognitive and critical thinking skills and foundational training in advanced, technical information and communications technology (ICT) systems will be key as the Internet spreads (Ordinario)."

Internet Service Providers

As has been argued elsewhere in this study, one of the keys to understanding access in particular states is to analyze its providers—who they are, whether they are privately or publicly run, or some combination thereof, and the ways they are regulated. The answers are often a reflection of the nature of the government and a state's political economy. When the ISP is the state, as is the circumstance for many states in the Not Free category, meaningful access is circumscribed for a multitude of reasons: political and economic control, cultural unity, etc. In the case of the Philippines, the ISPs are a reflection of the cronyism that typifies many sectors of the Philippine economy. The PLDT currently controls 70 percent of the telephone and ISP market.

Mary Mirandilla-Santos presents the story of the reformation of the telecom industry since the Marcos regime. Between 1967 and 1985, the PLDT was a *de facto* monopoly of the telecom market and was owned by an influential family with connections to the government. The PLDT was partially owned by an American company that helped rebuild the industry after WWIII, and in 1967 was set to sell 28 percent of its controlling shares to Pedro Cojuangco, the brother-in-law of Benigno Aquino. As the latter was Marcos's rival, he blocked the sale and instead sold it to Cojuangco's cousin, a political ally and crony. The PLDT's dominance was assured by this arrangement as "…its competitors were kept at bay… (101)." In particular, it owned 94 percent of the telephone network, and all other companies had to use this infrastructure for any voice calls. Others could try to compete with the PLDT, which proved fruitless, or developed niche businesses, like pagers. "PLDT would choke calls to other telecommunications companies…driving smaller companies into bankruptcy (101)." Under a presidential decree, users were forced to "invest" in the company—by paying a tariff of 900-1500 pesos—in order to get a line installed. While some in Congress tried to regulate the PLDT as a public utility, Marcos and the PLDT argued that it

was natural monopoly that could best provide and expand service based on the faulty interpretation of the American experience with AT&T.

After Marcos resigned, some reform was possible. Congress was empowered to enfranchise new operators, and the freedom of the press enabled freer criticism of the lack of efficiency and progress in the industry. Developments in mobile technology allowed "cracks in the dam" to appear, and new licenses were granted to Global and Eastern Telecom. However, in 1992 while companies like Islacom were selling GSM technology cheaply, PLDT clung to its fixed line service and had not expanded mobile technology beyond car phones, which cost users $6,000. By the time Fidel Ramos got in office, he had lobbied to liberalize the industry, and had Congressional support:

> In civil society, Ramos's government encouraged the formation of the Movement for Reliable and Efficient Phone Service (MORE Phones), a broad coalition formed in 1993 that gave a face to the disorganized public uproar against PLDT's poor performance and drummed up the consumer clamor for better telecoms services. (107)

Additionally, he instituted two executive orders that encouraged connections among local telecoms, lower subscription rates, and mandated that service be provided in remote areas. In 1995, the Philippines enacted Republic Act No. 7925, still in place today, to promote the development of the industry:

> Section 4. Declaration of National Policy. - Telecommunications is essential to the economic development, integrity and security of the Philippines, and as such shall be developed and administered as to safeguard, enrich and strength the economic, cultural, social and political fabric of the Philippines.

The act claimed that telecoms must expand into underserved areas, that the public would regulate radio frequencies, that the industry must be competitive and that it was providing a public good, not just a value-added service. It empowered the National Telecommunications Commission (NTC), established in 1979, to qualify service providers, assure interoperability, and investigate unfair practices, monopolistic powers, and customer complaints.

Nonetheless, the PLDT stuck to its ways, concentrating on urban populations with fixed lines, letting companies like Globe and Smart develop the mobile phone market. This prompted a buyout of PLDT and the dislodging of the son of Cojuangco as director of the company. He was also stripped of his shares in PLDT by a special anti-graft court because they were considered "ill-gotten" and were awarded to the Philippine government. Despite the changing of the guard, a dispute between Globe and PLDT arose over mobile interoperability. Globe and PLDT customers could not call each other, with the latter

accusing the former of not paying mandatory fees, which resulted in the intermittent stopping of connections of Globe customers to PLDT landlines. Then-President Joseph Estrada solved the matter rather ingeniously: "Both Pangilinan and Ayala were reportedly caught flat-footed in the press conference-style meeting, where Estrada asked the two to resolve the interconnection impasse 'as soon as possible' in front of the media (116)." Rather than proceeding with lengthy court battles—and bad press—the stalemate ended that day in November 1999.

Despite the progress achieved—teledensity increased 800 percent in the ten years after the reforms that took place after Marcos's departure—the Philippine telecom industry remains a duopoly with the PLDT as the dominant player. New ISPs have a convoluted process to navigate in order to launch their business: obtaining a Congressional license through parliamentary hearings, a certification from the NTC, and the requirement that the company be 60 percent Filipino-owned (Freedom House 2015 642). This discourages foreign investment in the industry, which has bolstered the dismantling of monopolies in other states, as with Mexico's América Móvil.

The Internet, unlike telephony, is considered a valued-added service, so it remains under regulated, and speed and availability are left to the discretion of providers. Attempts to reform the industry further had languished in the Philippine legislature since 1987. House Bill 5286, the Philippine Fair Competition Act (PFCA), is commonly referred to as anti-trust legislation, was undertaken under the premise that it would better prepare the Philippines for highly technological industries that dominate Southeast Asian economies (Dalangin-Fernandez). It passed in the Senate in December 2014, and was set to create "a Fair Competition Commission will be created to oversee all matters related to fair trade in the country (Sy)." There is no evidence that the Commission has been created or the law has had any effect on the industry thus far.

Instead, controversy over the telecom industry continues. A journalist for the *Manila Times* claims that the "PLDT mocks the Constitution" because the makeup of PLDT's ownership. The Supreme Court determined that the company violated the requirement that 60 percent of any public utility be Filipino-owned. Instead, the company argued that the non-voting shares were owned by enough Filipinos to justify the company's structure, but in reality "According to PLDT's disclosures to the US SEC, all these firms [six interlocking companies owned by First Pacific] are represented by only one man: Manuel V.

Pangilinan, who owns only less than 1 percent of these firms, but is Salim's [Indonesian owner of First Pacific] chief representative (Tigalo)."

Additionally, the merger of PLDT with a former rival, Digitel, was controversial but permitted by the Congress. Neal Cruz argued that it was the Congress's duty to regulate radio frequencies so that no one company controls the entirety of a range in a particular region, but by purchasing not only Digitel's equipment but also its franchise, PLDT was violating the spirit of RA7925. Further, Neal argues that the state did not prepare smaller providers to compete with entrenched companies. Without an open-ended transition period with price controls, new competitors are forced to use the infrastructure and purchase services from the leaders of the industry, essentially becoming customers rather than rivals.

Shahani Ramos (2015), in an opinion piece for the *Philippine Star*, offers additional reasons why the Internet is "so bad" in the Philippines. She begins by citing the 2011 HRC report, asking if it is a human right "…shouldn't Filipinos be more outraged with the quality—or lack—of service we get from our internet providers?" She outlines several glaring problems. First, in most states that have multiple ISPs, providers practice peering[38] in order to make the flow of information efficient. Instead, providers in the Philippines use tolls, even for its IXs, and the "PLDT…resists efforts to dismantle for-profit IXs—to maintain private control of these connections." Therefore, all ISPs, including Globe, must pay PLDT for its IX services. Second, the influence of the PLDT on the government and the regulation of the ICT market stagnates growth of the sector. The unfriendly and lengthy process for entry into the sector discourages competition, and Ramos attributes the influence of the PLDT on the NTC for keeping it this way. Third, she cites the NTC itself as pursuing projects that will not solve speed, cost, or dependability issues.

> Unfortunately, rather than mandating a national broadband program or even demanding IP Peering between Globe and PLDT, the legislation now taking shape looks like a disappointing, stop-gap measure: mandating a service minimum of a mere 256 kbps—that's .256 Mbps, ten times less than the public expectation for a 2 Mbps standard!

[38]"Once upon a time America's entire phone system was run by AT&T and a bunch of independents who served subscribers in areas AT&T wasn't. Essentially the whole gigantic thing was a monopoly, with monies for transmission and switching changes hands under rulers run by government regulators and essentially administered by one company. The Internet is different. There are many companies providing telecom and switching service. These companies have to move traffic of the Internet between them. Hence they established something called peering. It's a relationship between two or more ISPs for the purpose of exchanging traffic directly, rather than doing so through a backbone Internet providers… (Newton 847)."
"So the Internet is public because it's handmade. New links don't just happen according to some automated algorithm, they need to be created: negotiated by two network engineers, then activated along a distinct physical path…Peering allows information to flow freely across the Internet— by which I mean both liberally and at low cost. Without peering, online videos would clog the Internet's pipes— YouTube might no longer be free. (Blum 118-119)."

While there are others pursuing decentralized Internet access, she suggests that peering agreements would be the most effective way to increase speed and quality. In an advocacy paper, the Joint Foreign Chamber summarizes what is wrong in the Philippines:

> In particular, the country fared very low in terms of infrastructure environment and readiness of the government to modernize its entire structure. Burden of government regulation, length of procedures in starting a business, performance of legal institutions, education investment, and quality of research institutions are cited as major dampeners to its relative global position (168).

Efforts to Increase Access and Overcome the Digital Divide

Like Mexico and Brazil, the Philippines is concentrating on providing additional access through government programs, public-private partnerships, and NGOs.

Government programs. The ICT Office, part of the Philippine Department of Science and Technology, runs several projects relating to the implementation of technologies for "development, policy, infrastructure development, research and development, capacity building of the public sector, and the administration of the E-Government Fund." The most noteworthy among its several projects is the Tech4ED project, whose motto is "A Community eCenter [CeC] in Every Municipality." Taking shape in the barangays, priority is given to areas where public Internet facilities are absent. The program ties Internet access to education, such as in San Carlos City, "to provide its citizens a more accessible education, and more entrepreneurship opportunities, hence demonstrating what a progressive society is." Among Tech4ED's proclaimed "successes" are numerous conferences and workshops, the training of CeC personnel and the mapping of 153 CeCs. The latter refers to putting these facilities into widely available database, but it appears that this is not currently available. The ICT also highlighted the recipient of the first DigiBayani [Digital Hero] Award from the Foundation for Information Technology Education and Development, a Philippine NGO. Dr. Mary Ann Cortado "a simple lady from North Cotabato whose advocacy is to help her humble town to become a digitally literate community, was recognized as one of the outstanding champions in the digital realm," runs one of the CeCs and started a digital literacy program in 2009 with 20 enrollees. That number ballooned since, with 1,500 graduates including special programs for women and children.

PPPs. In "Shared Prosperity: An ICT Manifesto for the Philippines," (2015) authors from a Singaporean school of public policy and Microsoft examine the problem of low levels of Internet

penetration and speed and offer their suggestions for a way forward. They argue that the workforce will have to catch up to the digital revolution in order to compete, and that means education and technology must be pursued together. They advocate for increased use of PPPs so that the Philippines can "leap not walk" towards more complete Internet penetration. States that are developing new ICTs are not dependent on the methods of access that others had gone through decades before, citing the explosion of 2G in lieu of the PLDT's failure to expand landlines. Their suggestions include: the promotion of peering, cost-efficient infrastructure rollouts (if building a road, add a telephone line), incentivizing Internet exchange point[39] (IXP) production, releasing more radio spectrum, and updating and improving regulations and the responsible institutions. Connecting provincial cities would have a spillover effect in the Philippines's rural areas, creating jobs and helping to alleviate poverty.

One of these PPPs is an effort spearheaded by the government to use TV White Spaces (TVWS). In a method that is becoming more common among developing states, "The [SSG] Partnership deployed Microsoft's TVWS technology, which generates a long-range wireless Internet connection by riding empty television UHF and VHF broadcast channels (Lovegrove)." It was first tested in 2014 in the province of Bohol to coordinate efforts to reduce overfishing (PNA). The Department of Science and Technology Secretary Mario Montejo headed the project and planned to provide 600 towns with free Internet access in 2015, serving 20,000 people. The Secretary indicated that it plans to make use of the TVWS for future attempts to increase the levels of connectivity in the Philippines. Such attempts are logical facing the difficulties surrounding attempts to reform the marketplace.

MNCs and NGOs. Facebook has its own initiative to provide access in developing states, its Internet for All campaign. For Filipinos Free Basics is a downloadable app for smartphones that allows users to freely access select websites: healthcare, educational websites, job listings, Wikipedia, Filipino newspapers, weather, sports, and of course, Facebook. It partnered with Smart Communications, one of PLDT's subsidiaries, and through a freely supplied SIM card since March 2015 users can have access to the listed sites. The project is not without criticism, with many citing that it violates net neutrality; in India,

[39] "An internet exchange point (IXP) is a physical network access point through which major network providers connect their networks and exchange traffic. The primary focus of an exchange point is to facilitate network interconnection through an exchange access point instead of third-party networks (Technopedia)."

this viewpoint led to the service being declared to be illegal, but so far it has been well-received in the Philippines.

Efforts to establish norms about Internet freedom have been undertaken in the Philippine legislature. The controversial Cybercrime Law of 2012 outlawed online libel, and for Freedom House, signified possible future abuses of users' rights. The Magna Carta for Philippine Internet Freedom is the result of an initiative begun by a group of Internet freedom advocates made up of lawyers, bloggers, and human rights activists gathering commentary from social media platforms. They state:

> We are no different from you. We are Filipinos from all walks of life. Some of us are gamers. Some of us are parents. Some of us are software designers. Some of us are bloggers. A number of us are on Twitter and Facebook. We are Filipinos.
>
> We believe in Democracy. A place; a shared idea where rights and obligations are crucial parts of society for it to grow and prosper (Democracy.Net.Ph)

Much like the Marcos Civil da Internet of Brazil, the bill seeks to strengthen freedoms on the Internet. It contains provisions for the freedom of expression on the Internet, the advocacy of universal access, defines cybercrime and in what circumstances the state can intervene into the use of the Internet, the promotion of innovation, the right to privacy, and the promotion of better governance though transparency and freedom of information. It contains criticism of the current state of the ICT market, claiming that the Internet should be an open network and affirming the importance of net neutrality. The bill has been introduced to both the House and Senate, but has not been voted upon.

Domestic Attitudes towards the Internet

Filipino-conducted research or surveys on the demand for Internet access in are difficult to come by, yet global surveys have included the Philippines among other states, and data is available highlighting the digital divide along lines of urban/rural residence, education, and socioeconomic status. There is ample evidence that Filipinos care about Internet access and quality. First, quantitative evidence is found in GlobeScan's 2010 survey and Internet Society's 2012 survey. Compared to the US and Latin American states, few Filipinos view the Internet as a fundamental right, at 73 percent, and 79 percent report that they could manage without it. Most view social connections—enabled by the likes of WhatsApp, Skype, and Facebook—as the most valued by survey respondents at 48 percent. The figures were higher as reported by the Internet Society in 2012, with 88 percent of respondents claiming that the Internet should be considered a basic human right, 86 percent arguing that freedom of expression should

be guaranteed on the Internet, and 91 percent saying their rights of assembly and association were enhanced by the technology. Filipinos view the state taking a proactive role in the spreading of access, with 96 percent arguing that it should consider ways to provide cheap computers, 92 percent arguing that competition among private ISPs should be encouraged, and 85 percent arguing that the state is obligated to assure citizens' ability to access the medium. Only 60 percent would accept increased control in order to assure security, and 86 percent argue that the state has the right to govern the Internet as it sees fit.

Second, qualitative evidence is available from several sources. As discussed, the Magna Carta bill was a crowdsourcing effort that involved not only NGOs but input from the public—at least those that had Internet access. Like the Marcos Civil da Internet, it is evidence of how the public perceives the importance of Internet freedom and the relationship among customers, ISPs, and government regulators.

Journalists in the Philippines have interviewed users on their perceptions about the status of the Internet in the Philippines. Michelle Toh, reporting for the *Christian Science Monitor*, interviewed a self-described "gamer" in Manila:

> "Our country's internet speed isn't 'slow' in an absolute sense," says Isaac Javellana... "Emails, social networking and some light streaming isn't an issue. In a relative sense though, we pay more for what we get. This is where the problem lies. HD streaming and quick gigabyte downloads are luxuries only accessible to a select few."

Javellana is correct in asserting that current average speeds are adequate for basic Internet use—email, web surfing, etc.—and connects it to the larger problem that most developed states have moved past basic Internet, and that in order to remain competitive, basic is not adequate. Senator Francis Escudero is correct in asserting that "The state of Internet speed is pathetic, and unless we remedy this situation, our IT sector is likely to suffer in the long term," because the lack of IT readiness will inhibit economic growth in the coming decades. Several articles have discussed the integral field of business-process outsourcing (BPO) to the Philippine economy (See Ordinario, Joint Foreign Chambers, Montenegro and Araral). Javellana also points out how the lack of competition and technological know-how of local technicians inhibits meaningful growth of the Internet.

There is also evidence of both the dissatisfaction with the service in the Philippines and the idea that users are entitled to better speeds and more responsive providers. Toh cites two tweets from Filipinos regarding Internet speed complaining about its unreliability and slowness. Such examples are easy to find when reading the commentary on articles about the PLDT and other matters related to the

Internet access in the Philippines. In response to the Ramos Shahani's article that discussed the lack of peering amongst Philippine ISPs, many users seemed well-versed in what ails the Philippine ICT market—and what could fix it.

> the ultimate solution is for the government build a national broadband system (a very fast one and huge capacity) and let the players (PLDT, Smart, Globe. etc.) compete for access for their network service system -and pay toll fee to the government. PLDT and Globe can no longer monopolize network access and at the same time do away with the toll fee when calling from one network to the other. all players will be using a singular network controlled and managed by the government. NTC as is, is useless and can not even dictate on the two giants (Globe & PLDT) (User ed1151, Shahani).
>
> This is a timely article, slow and high cost internet is affecting our country's productivity. I just hope the government, through the National Telecommunication Commission will do something concrete to address this problem. As mentioned by Ms. Shahani, internet access is a basic human rights. Effective internet plays an important role to human and economic growth (User GWC, Shahani).
>
> Anchoring on UN's declaration that internet access is a basic human right, we should be outraged at the current situation of the internet in the Philippines. Asec Lila here has pointed out necessary policies that should be legislated if the Senate truly wants to improve our internet. Props to Asec Lila for shedding light on PLDT's apparent "monopolistic opportunism." It is our duty as netizens of the Philippines to demand for our right to a decent (minimum of 5Mbps) and inexpensive (at Php243 per Mbps) internet service (User Pierre-Luc, Shahani).

While formal domestic surveys do not seem to be available, in a country that used to be known as the texting capital of the world, social media and the interaction between readers and journalists provides evidence of how local people view the Internet, ISPs, and their rights. Using the UN's declaration that access is a human right shows that the feedback loops of normative development.

It also appears the love of social media translates well into Filipino politics. Zuckerberg hailed President Aquino's signature to a Connectivity Declaration on December 10, 2015, which happens to be International Human Rights Day. The following day the President's page posted a video, likely produced by Facebook, which told the story of how a college graduate used Internet.org to complete her thesis in computer science while marooned on an island after a typhoon. There is an argument to be made that pursuing PPPs is easier, or more politically feasible, than reforming the ICT industry.

***

The Philippines is a challenge to its Freedom House categorization. While it does not regularly violate civil rights on the net, it faces some of the most problematic issues in terms of the F2C that are not directly a consequence of state activity. Nevertheless, there is ample evidence that the state is not

violating the spirit of the developing norm, and that Filipino demands are line with the idea that access should be equitable and that it should be conceived as a right.

Chapter 5: Partly Free Cases

States contained within this category are largely moving in one of two directions, either towards greater meaningful access on the heels of the F2C's normative development or are being pursed simply for economic development. Regime type and political culture are good predictors of this reaction. Mexico and Indonesia's placement within this category are the result of malfeasance and asymmetric marketplaces, but there is evidence of the acceptance of the F2C by both states and their societies. Conversely, Russia is moving away from Internet freedom.

Russia

Russia has a complicated history with human rights and democracy. Spanning two continents but finding its identity firmly planted in neither, it has been moving away from the promise of democracy begun in the era of glasnost and perestroika toward increased authoritarianism. In the period since this study began, Russia's scores for *Freedom on the Net* have deteriorated, moving it from Partly Free to Not Free as of October 2015. In 2009, the state scored an overall score of 49, with Obstacles to Access totaling 11 out of those 49 points and Limits on Content totaling 16 and Violations of Users rights totaling 22. By the 2015 report the score had jumped to 62, with limitations on content and violations of users' rights increasing while the score for Obstacles to Access, 10, remaining static from 2014. This change in their rank serves as an illustration of the development of the F2C. States have approached Internet diffusion as part of the greater regime of Internet freedom or tried to maintain firm state control over users and content. Russia has taken the latter approach as a consequence of the change in its political identity and regime type. As an anocracy that is marching towards authoritarianism, its scores predictably decline. Steps to test the viability of shutting off parts of the Internet, whether realistic or not, is only likely to further devolve Russia's score on both the Freedom House index and Polity's data set.

Background

Demographics

Russia is among the largest and most powerful states in the world. Its status as a superpower is questionable today after the fall of the Soviet Union, the "shock therapy" of the 1990s, and the current economic crisis it faces. Its fall from power is being countermanded by the efforts of the Putin regime since the late 1990s. As reported by the CIA's World Factbook, it has a population of 142,423,773 (ranking 10th in the world) and land mass that spans 17.1 million km^2 (1st in the world). Seventy-four

percent of its population lives in an urban area, with 6 major metropolises with populations of approximately 1.2 million or more[40]. It has the 7th largest economy in the world with a GDP of $3.5 trillion. This equates to $23,700 per capita, which means that despite the size of its economy, GDP/capita ranks 79th in the world. The country's GDP fell between 2014 and 2015, and the GDP per capita slipped by nearly $1,000, raising its ranking from 69th to its current position. There is a notable disparity between the masses and the elite in the state, and government is often characterized as an oligarchy. There have been some reports that the sanctions applied to Russia have been effective. Instituted in response to Putin's actions in the Crimea, the indirect pressures of sanctions against Russia have inconvenienced many of the elites upon which Putin's rule depends.

Looking at its ICT technologies[41], Russia has 39.4 million landlines, ranking 7th in the world. The figure escalates for cellular phones, with 221 million in the country, placing it 7th in the world. Freedom House (2015) reports that the cell phone penetration rate is 155 percent, 50 percent of which are smartphones. In total, there are 84.4 million Internet users in Russia which ranks the state 7th in the world and totals approximately 59.3 percent of the population.

Russia has a complicated history with traditional liberal civil and political rights. Its history as an empire and later as the Soviet Union necessitated the repeated violation of civil and political rights, and was followed by the democratization of the state during the 1990s. The dominance of the Putin regime since 2000 has coincided with the increasing limitations on expression and association.

The Human Rights Watch reported that in 2013 the Russian government had cracked down on civil rights that year more than any other in all of Russia's post-Soviet history:

> The authorities have introduced a series of restrictive laws, harassed, intimidated, and in several cases imprisoned political activists, interfered in the work of nongovernmental organizations (NGOs) and sought to cast government critics as clandestine enemies, thereby threatening the viability of Russia's civil society," it said (Human Rights Watch 2013).

Demonstrations are technically allowed by the Kremlin but must not interfere with government business and must be explicitly sanctioned. Internet controls were highlighted in the report, saying that the government's justification of censorship came from the desire to limit access to dangerous sites related to

[40] Moscow (capital) 12.166 million; Saint Petersburg 4.993 million; Novosibirsk 1.497 million; Yekaterinburg 1.379 million; Nizhniy Novgorod 1.212 million; Samara 1.164 million (2015)

[41] CIA Factbook 2015

assisted suicide and child pornography. Another example of Russia's contemporary attempts to curb dissent was its very public example of the detention of the three members of the feminist punk rock band *Pussy Riot*, who were accused of hooliganism after staging protests at Orthodox cathedrals that directly challenged the increasingly resurgent Russian Orthodox identity. Anti-propaganda bills were signed that same year banning speech that could be used to disseminate homosexual lifestyles to minors and "the other bill…targets religious offenders and promises to punish actions 'demonstrating disrespect to society and done with the goal of offending the believers' religious feelings' (AFP)."

Despite having a long history of ties to the West and a historical desire to be considered part of it, Russia's relationship with civil rights little resembles its counterparts. Tracing back its relationship with serfs, the condemnation of peasants and bourgeoisie alike in the Soviet era, and recent developments over LGBT rights, Russia's relationship with civil rights is highly circumscribed. Although Putin makes the argument that citizens should be free to express their opinions, even against unpopular ideas, any criticism or dissent must be lawful. Laws restricting rights are not limited to the potential actual harm it might cause others, as it might be in the US under "likely and imminent" standards. Since *Pussy Riot* chose the wrong place for their protests, Putin argued that their actions are legitimately curtailed by the government (AFP). But such justifications belie other possible motivations presented by media critics, as there is a significant resurgence of Russian nationalism, evidenced in Adi Ignatius' biographical article[42] on Putin and the regime's justification for actions in the Crimea to protect "Russian citizens and compatriots." Ignatius's portrait of Putin as a religious, patriotic leader may be a reflection of many of the leaders of the Russian Federation and a sentiment shared by its citizens. Just as many US citizens are willing to compromise freedom for security, contemporary Russian ideology appears to be willing to sacrifice some of the substantive values of democracy for economic prosperity, security, and national pride.

In terms of the F2C, the analysis is somewhat mixed. The importance of access for economic growth is undeniable, but like some other cases in the Partly Free and Not Free categories, Russia weighs the benefits of openness with the risks. Unlike Not Free states, Russia has not banned major Internet search engines or social media outlets, but piecemeal censorship and other restrictions to the

[42] *Time's* Person of the Year cover story, "A Tsar is Born (2007)."

freedom of expression on the Internet are commonplace. This is not unlike its history with others such norms, and calls into question the meaningfulness of access when it is provided.

The Internet in Russia

Background. As with the United States, Russia's history with networked computing begins with military applications. Projects in the 1950s set out to automate Soviet missile systems across the expanse of Soviet territory. In 1961, Gerovitch (2008) reports that the Cybernetics Council of the Soviet Academy of Sciences presented a paper regarding the potential of computing, networking, and automation for the Soviet economy at the 21st Congress of the Communist Party. The proposals made at the Congress were initially well-received, and "[t]he popular press began to call computers 'machines of communism (335).'" Similar proposals made over the course of the following decades never achieved networking at a national level, and the "machines of communism" never manifested. Gerovitch's purpose in "InterNyet" was to discount common accounts given for this failure, such as the obstacles like poor infrastructure and a lack of innovation in the ICT sector.

After Stalin's death, the party under Khrushchev attempted to decentralize much of the Soviet economy based on belief that innovation and competiveness were stifled in the past by the state. In pursuing this course one of the major advantages of centralized planning—efficiency—was lost. Supply chains became muddled, bureaucracy swelled, and output decreased. Like many Internet utopians today, cybernetics (akin to ICTs in contemporary jargon) appeared to be a panacea. Some cyberneticists argued that military systems that coordinated weapon deployment should be connected to the larger Soviet infrastructure and institutions. Engineer Colonel Anatolii Kitov suggested "to link them together to form 'large complexes,' or networks, and ultimately to create a 'unified automated management system' for the national economy (339)."

The problem became political. Reluctance stemmed from two important sectors of Soviet politics: on the one hand, industrial managers and the government, and on the other those would have liked to liberalize the Soviet economy further. The former feared that computerized automation would expose inefficiencies, show managers to be redundant, and remove a fundamental basis of the government's power. The latter feared that increased automation would be successful at increasing efficiency, and the re-centralization of the economy would make their argument for decreased state-control toothless.

Nonetheless, there was pressure to continue to develop the technology in response to the parallel developments in the US, particularly of ARPANET. The compromise did not the completely abandon the technology, but used it in piecemeal attempts in order to make its impact less far-reaching and profound.

> Ministry officials realized that there were many ways to skin the cybernetic cat without necessarily losing their grip on power. Each ministry built its own computer centers and developed management information systems for their internal needs. In 1971–75, the number of such systems grew almost sevenfold, but they often used incompatible hardware and software and did not form any cross-agency network…By accelerating the development of branch-based incompatible systems, the ministries effectively blocked the idea of a national computer network (Gerovitch 346).

Even early in the development of computer networks in the Soviet Union, politics and the concerns of officials to maintain their hold on power trumped considerations of the benefits technology would bring. Politicians and bureaucrats had as much to say on the use of technology as ICT professionals. Gerovitch concludes that the pace and the spread of the Internet in the US were related to its political economy as much as to its technological innovators. While the US government sponsored the creation of packet-switching, which enabled large amounts of information to be transmitted across the country, it was private industry, free to operate beyond the scope of the government that created new uses and markets for internetworking. Since innovation and development were shaped by Soviet politics, an equivalent technology never developed.

Larry Press of the Information Sciences Institute of the University of South Carolina, published an account of the role of ICT in the coup against the Soviet state in 1991. He reports with pride how a message enabled by American technology spread the news about the deployment of Soviet tanks that threatened that nascent movement, ending with the missive “Communists cannot rape the Mother Russia once again!” The sentiment spread from the Demos Cooperative in Moscow to over 70 computers across Russia in a matter of hours. This was possible because the computers were connected through RELECOM, based in Finland. Soviet authorities attempted to stem the tide of information, the involvement of tanks, and possible violence, but Press maintains that such attempts were abated by the Internet, and the entire world would soon learn about the coup as it unfolded in real time. Despite pleas from RELECOM to abate the sudden spike in traffic, messages ranging from conflict reports to missives to loved ones peaked during these crucial hours. Press recounts that beyond the hard facts, the

emotional support and the knowledge that the actions of the Soviet Union were being broadcast globally were of real comfort to those living through it.

Why the Soviets did not simply unplug RELECOM is a pertinent question. "When a friend asked why they didn't, Polina [a friend of Press in Moscow] replied "Thank Heaven, these cretins don't consider us mass media!" In assessing the impact of the network, Press comments upon the poor communication infrastructure in less-developed states (something that Russia certainly qualifies as during the period), and how email/digital messages were cheap alternatives available for young professionals. Further:

> As such, RELCOM may be a good model for other countries with poor telephone and postal systems, little capital, and well educated, motivated young professionals. Networks like RELCOM, probably using satellite technology, may change the face of the earth in peace time as well as helping to keep the peace.

The analysis in 1991 is typical of what Morozov characterizes as Internet utopianism as such enthusiasm is typical for that time period. Relatively new technologies that are popularly available invites hopeful analysis of the potential of them to bring about change in ways that were unfathomable before its availability. Yet analyses of the impact of "revolutionary" technologies like the telegraph, radio, television, etc. reveal that governments have a learning curve. It may take time for states to realize the threats posed by new technologies to the status quo, but will adapt as they see fit. "The cretins" may not have seen the impact of RELECOM in 1991, but authoritarian and semi-authoritarian governments have a way of catching up.

It took the implosion of the USSR to bring the Internet as we know it today to Russia. The gradual replacement of the incompatible UUCP with TCP/IP allowed computers in Russia to be able to network with the greater World Wide Web. The Internet gradually became available during the 1990s in major Russian cities.

One of the most important lessons of this look into Soviet/Russian history with networked computing is its fierce relationship with the state. Gerovitch writes:

> Recent scholarship on the "co-construction" of users and technology emphasizes the role of users in defining, modifying, redesigning, and resisting new technologies, and also explores the effects of technology on the definition and transformation of the user (347).

The introduction of technology is not linear, but operates in a feedback loop. Like the cyberneticists of the Soviet Union, the users of technology in Russia today are met by those who would desire to transform the

technology to their own ends. This is especially evident in Russia's actions in violations of users' rights and limitations on content, but also in regard to access.

These sentiments are echoed in an article from 2005 analyzing how the Russian state interacted with the development of popular Internet usage in the country. Alexander sets out to answer the question of how states like Russia as an anocracy—avoiding the extremes of actual democracy and its former authoritarian status under the Soviet Union—makes use of the potential liberalizing effects of media like the Internet. The expectation shared by many Internet utopians was that transitioning states like Russia would benefit from the increase in the availability of information which would weaken state control of the media in the short-term and increase demands for civil and political rights. In actuality, Freedom House reported that between 1995 and 2003, increased popular use of the Internet coincided with decreased freedoms for Russian citizens.

Alexander outlines two methods the Russian Federation has used to "control" the Internet. Initial response was Soviet-esque: reactionary attempts to regulate the medium through the lens of national security and evading foreign influence.

> …the laws set up a precedent of the government's justification for active control of the Internet by the process of registration, the creation of government bodies to monitor and guide development of the industry, and the delineation and qualification of rights (even constitutional) when applied to the Internet (615).

ISPs that could not meet the Federal Security Service's demands to install expensive "spying hardware" were made ineligible for licenses that allow them to provide services to citizens. Some 90 percent of the 360 ISP subproviders were made ineligible in 1999. By limiting the number of providers, the state made Internet penetration slower and ultimately left the development of the Russian economy in the lurch.

Since Putin took office, the Russian Federation has taken a more proactive approach to controlling its citizens' relationship with the Internet. Trying then to join the WTO, Russia's Internet regulation was necessary in order to achieve the levels of penetration that would lead to economic growth, but such expansion required government involvement. Examples include anyone seeking a domain name with .ru would require to have it registered through Rospatent which also handles things like trademark and patent applications. The Kremlin also adopted the E-Russia plan in 2001 that would use $2.1 billion to promote the growth the Internet in key areas like security, e-commerce, and equal access to ICTs in the classroom (Nefedov and Boreiko). Alexander reports that few Russians surveyed in

2003 either cared or even knew about the plan, while Nefedov and Boreiko report that the sector of Russian society most excited by the plans was the business community. "'It is excellent that the program has finally been adopted. It sets out how the country should use IT to increase the effectiveness of the economy,' said Olga Dergunova, head of Microsoft's local representative office (Nefedov and Boreiko)." The survey respondents in 2003 indicated that users were relatively uninterested in whether the state could provide further at home computer or Internet access, but were primarily concerned with going online in schools and hospitals.

In 2000, the Kremlin developed Internet Security Doctrine. The state should not just become one half of a PPP as the UN describes, but should instead be the engineer of Internet development in the state and this principle is used in Russian attempts to expand broadband penetration to this day. Second, there were to be clear limits of Russian citizens' rights on the Internet; the possibility of liberalization of the media or freedom of expression on the web was limited. Alexander concludes that Russia does not have to use tactics like overt censorship (although it certainly does), but represents a new type of relationship between the state and the apparent nebulous medium: "The development of Russian Internet policy shows that transition regimes have a third option: to promote Internet access and ISP proliferation, and then use the Internet for direct and indirect propaganda (624)."

Speed and cost. Today, access in Russia is expanding but its meaningfulness is hampered by speed. Twenty-seven percent of the Russian Federation's population had access in 2008 versus 61 percent by 2013. Over half of the population accesses the Internet on a daily basis, but this number is significantly below the number of US households that have access (72 percent). Costs are relatively low with speeds of 51 Mbps costing users $14 per month. Numbeo confirms this figure; 10 Mbps costs approximately $5.71, or 1.08 percent of a monthly salary. In all, Akamai reports that in the fourth quarter of 2015, average speeds across the country were 11.6 Mbps, placing Russia 33rd in the world and increasing its speed 30 percent from the previous year. A new law enacted in March 2014 required telecommunication access in every Russian settlement with a population of over 250 people. Such moves appear to be in accordance with the norm of the F2C, but is realistically a consequence of the realities of the global economy. Despite the law, Freedom House reports that 1,343 settlements have no

Internet in 2015. While this statistic is likely to decrease, it is a contributor to the Russia's score for Obstacles to Access.

Broadband is widely available in major Russian metropolises. Some of the results of testmy.net as of April 2016 are laid out below.

Table 6 Reported Internet speeds in Russian cities
(Testmy.net 12 April 2016)

City (Region)	Downstream	Upstream
Moscow	13.7 Mbps	6.5 Mbps
Omsk	6.5 Mbps	6.4 Mbps
Novosibirsk (Siberia)	4.7 Mbps	2.8 Mbps
Vladivostok (Primorsky Krai, Far Eastern Russia)	2.8 Mbps	1.9 Mbps
Yakutsk (Sakha (Yakutia) Republic, Far Eastern Russia)	2.2 Mbps	775 Kbps
Norilsk (Krasnoyarsk Krai, Arctic Circle)	373 Kbps	404 Kbps

As with other cases, the father from cities one travels in Russia, the slower the speeds.

As reported by the Internet and Democracy Project (see Epstein et al 2009), the Public Opinion Foundation (FOM group, Фонд Общественное Мнение) has collected statistics on Internet penetration in Russia since 2003. In its most recent report (Spring 2015), the digital divide between major metropolises and Russia's vastness still dominates the statistics.

Table 7 Dynamics of Internet penetration by Russian federal districts
FOM report, "Internet in Russia" (2015)

Dynamics of Internet penetration by Federal Districts in%	Type of settlement						
	Central	Northwest	South and North Caucasus	Volga	Uralian	Siberian	Far Eastern
Spring 2003	11	14	5	5	9	5	7
Winter 2014-2015	65	69	63	58	66	62	63
Spring 2015	67	71	65	61	67	63	66

Table 8 Dynamics of Internet penetration by Russian settlement type
Reproduced from FOM report, "Internet in Russia" (2015)

Dynamics of Internet penetration by type of settlement, in %	Type of settlement						
	Moscow	St. Petersburg	Cities >1 million+	Cities 500,000-1 million	Cities 100,000-500,000	Cities >100,000	Villages
Winter 2014-2015	76	75	69	66	69	63	51
Spring 2015	77	80	70	71	70	64	54

FOM is the only source of up-to-date statistics of the Internet's penetration inside the Federation. While access has increased since the first report, two problems are evident. First, nowhere in the report does the FOM qualify the type of Internet access; whether citizens rely on broadband, mobile, or dial-up access determines the meaningfulness of access, and such concerns would acknowledge the recognition of the problem of meaningfulness of access. Second, the FOM group itself is a subsidiary of Russian Public Opinion Research Center, a government-owned and run institution. Statistics may be inflated or there may be other inconsistences for which no account can be made.

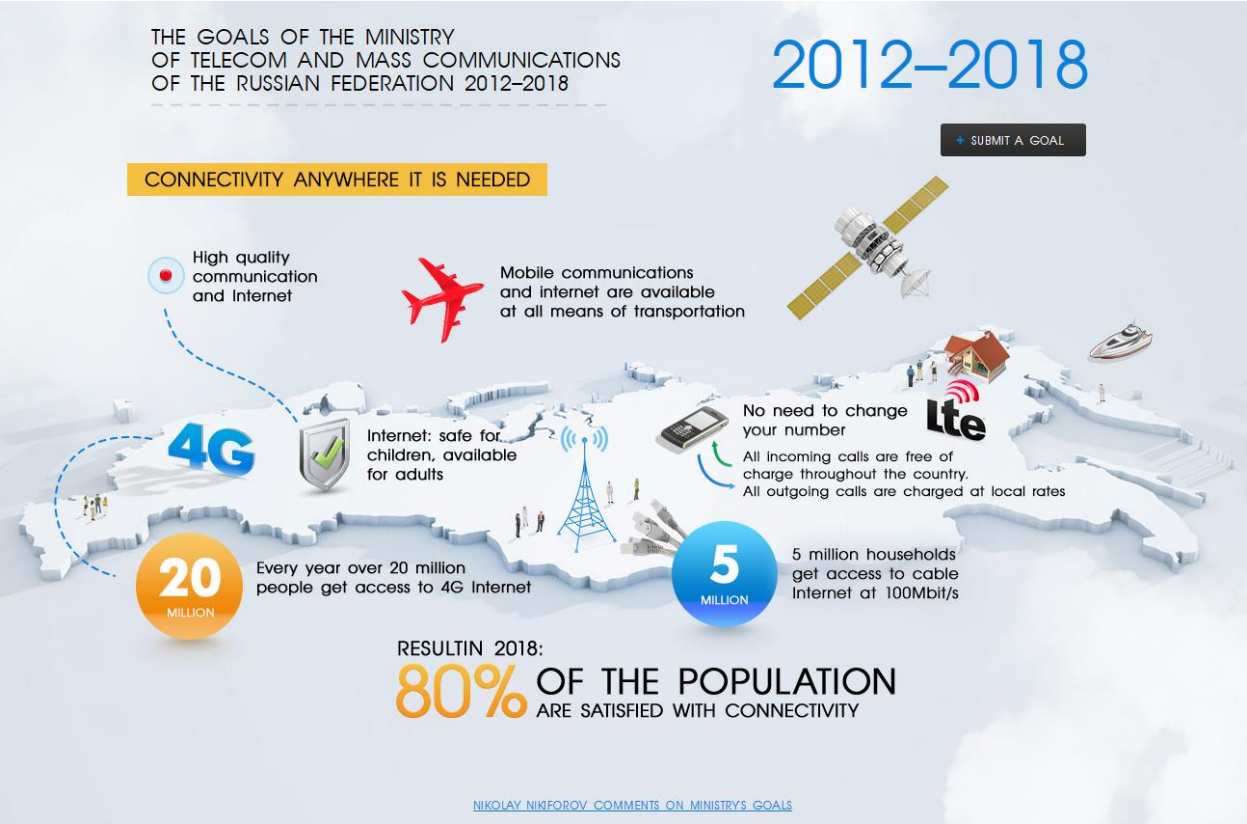
Another piece of the puzzle to be examined is smartphones. Google's Our Mobile Planet reported that in 2013, 36.2 percent of the total Russian population owned a smartphone, up from previous years at 19.4 percent in 2012 and 25.1 percent in 2011. The percentage in 2015 was 50 percent according to Freedom House. From a respondent base of 1,000, the report indicates that 86 percent of users with smartphones use them to access the web daily. The report indicates that while 66 percent use Wi-Fi to connect in their homes, 57 percent of those users use their mobile data service plan. While the study is enlightening, 96 percent of the 1,000 respondents were from urban areas. Most were well-educated with university degrees, employed, and middle class. Additionally, the World Bank reports that smartphone penetration is not a good indicator of Internet penetration, as it might be in the US. "…the ratio between mobile telephony subscriptions and mobile broadband subscriptions indicates that not more than 40 percent of total mobile telephony subscribers are signed up for mobile broadband services in Russia (Rossotto et al. 20)." While the reports continue to say that there is potential in this market to

expand broadband and Internet adoption among the high rate mobile telephone users in Russia, so far ownership is not a good indicator of access.

Information on the cost of broadband in different parts of Russia is difficult to ascertain, and what is available is somewhat outdated. Alexey Sidorenko produced a 2010 study on the cost of broadband in Russia's provinces and territories and found that cost varied widely. Unlike in the US, where ISPs generally charge the same amount of money for equivalent connection speeds due in part to the FCC's initiatives in 2005, there is no such government direction to do so in Russia. Central and western parts of Russia enjoy Internet speeds of 1 Mbps at considerably lower rates than provinces that are far removed from major cities or transit lines. Cities with cheap broadband had greater competition and multiple ISPs. In 2010, the city of Norilsk in Russia's Far East had the highest cost of broadband at $180 per month and had only four ISPs. Some of his cases were instead using 256 Kbps connections (dial-up speeds), but the report does not indicate what percentage. Since the US case has shown that dial-up persists in remote areas, it is safe to presume that the percentage mirrors or exceeds the American case of 2 percent. Sidorenko also measured costs of access in relativity to average citizens' salaries. The most populous areas have the most meaningful access at the best prices. ICT infrastructure is often built alongside preexisting infrastructure, especially rail lines. If a village is traditionally underserved by infrastructure, and there is no financial incentive for private enterprise to invest in a particular locale, it will be relatively ignored.

Unnamed broadband plan. Russian policy aimed towards increasing broadband availability began in 2012 with a plan enacted for the proceeding five years. Based largely on the work of Russia's largest ISP, Rostelecom, the plan relies on the extension of existing fiber-optic infrastructure, stating they would lay out 200,000 kilometers of new fiber lines. Satellite and mobile technologies would be put in place for rural and remote regions that would enable mobile broadband. Nikolay Nikiforov, the Minister of Telecom and Mass Communications, presented Russia's plans to expand connections at a speech at Moscow University, and plans were made into an infographic reproduced below:

Figure 1 Infographic of unnamed Russian broadband plan
(Ministry of Telecom and Mass Communication)



The highlights of the plan are the assertions that by 2018, 5 million households would have access to state-of-the-art speeds of 100Mbps, and that 80 percent of the population would be ‘”satisfied with connectivity.” The latter is vague; one might assume this satisfaction would be in response to protests over the digital divide that erupted in the 2000s (see Asmolov). The plan calls for a simplification of regulation of the ICT industry (further centralization?), allowing radio frequencies to be adapted for mobile technologies like 4G, and 97 percent of localities with at least 250 people would have broadband by 2019. Five new ICT-oriented development complexes or “technoparks,” would be built that would increase Russian programmers employment from today’s 350,000 to at least one million.

Nikiforov’s remarks about the importance of the increase in availability is largely economic in nature. He paid lip-service to the importance of access to information, social networks, and

entertainment, but these were largely eclipsed by the main thrust of his argument[43]. He remarked that a 10 percent increase in Internet availability would equate to a 1.5 percent increase in the state's GDP which is at the heart of many broadband projects in liberal and illiberal states. He said that "due to the fast development of information technologies the youth has huge prospects for personal development and self-fulfillment and it's important not to miss these opportunities." Such sentiments echo the pragmatic necessity of the Internet to make global competiveness feasible in the 21st century, but the rights component of the F2C is largely absent.

In a May 2015, Nikiforov updated the Federal Agency of Communications (Rossvyaz) on the deployment of broadband and satellites to deal with digital inequality. The intended audience was bureaucrats, but the speech centered around two ideas regarding the effort: cost and technological nationalism. Part of the allocated budget for universal telecom reform for the buildout of cable had been redirected to other purposes but the Minister promised those funds would be replaced. Further, the dependency on foreign-constructed satellites has been due to the uncompetitive pricing made by Russian-made ones; "Our country posses [sic] significant power in sphere of space communications and it should assume better position on the global stage."

Internet Service Providers

The characteristics of Russia's ISPs are indicative of the quality and meaningfulness of access for Russian citizens. Russia's ISP market share is highly skewed, with only handful of companies with a lion's share of the marketplace:

> According to the most current data available, the six largest providers occupy 77.1 percent of the market: the state-owned provider Rostelecom controls 38.6 percent of the market, while the rest is divided among ER-Telecom, VimpleCom, MTS, Trantelecom and AKADO. The mobile communications market is even less diverse, with the four biggest operators—MTS, Megafon, VimpleCom and Tele2—together controlling 92 percent of the market (Freedom House 2014 644)

Additionally, a 2013 concept paper from the Ministry of Communication would require ISPs to purchase foreign Internet traffic directly from state-controlled service providers. The centralization of transboundary traffic would further ensure state control of content, and would indirectly limit the number of ISPs due to

[43] "'The Internet provides not just an access to information, social networks and entertainment. It's also an opportunity to get public services in electronic form, to organize business and interact with business partners, sell your production throughout the world and increase the quality of education,' said the Minister."

the burdensome financial requirements. By the time of the Freedom House's report 2014, only Rostelecom could meet these standards.

Rostelecom is a state-owned ISP that provides not only Internet, but telephone and cable services across Russia and other European states. It has the greatest market share of all ISPs in Russia (36 percent) and is owned by the Russian state despite being a publicly-traded company. Much of the spread of connectivity in the next few years is dependent upon the infrastructure that Rostelecom owns. Their website reports on several "strategic projects" whose interests are more in line with those of the government than their customers. Among these include a "Digital Government" project that attempts to streamline citizens' access to government services, running the information systems of many of Russia's public institutions, the Sochi 2014 Olympics, and web monitoring of polling stations. Unmentioned on its website (which is curiously outdated), Rostelecom also takes part in blacklisting websites ordered by the central government, as the discussion below will detail.

ISP and ICT sector regulation is carried out by executive decree that gives regulators extensive authority. The Ministry of Communication and Mass Media, which is headed by Nikolay Nikiforov, controls the Federal Service for Supervision in the Sphere of Telecom, Information Technologies, and Mass Communications (Roskomnadzor). Freedom House states that "The regulatory body has the authority to determine if a website should be blocked based on whether or not the site contains material that is restricted by the law; these decisions do not require prior court approval (645)." The head of the agency (currently Alexander Zharzov) is appointed by executive decree, and generally the appointee follows the dictates of the Kremlin.

State Restrictions of the Internet

Von Twickel remarked in 2009 that the web was one of the final bastions of free speech in an environment in which other telecommunications media like television and newspapers were becoming increasingly brought under the control of the Kremlin. As in China and Iran, ISPs in Russia are regularly used as tools by the government to regulate content. *The Moscow Times*, an English-language newspaper started for foreigners living in Russia, reported in 2009 that the central government had already been regularly blocking sites that it defined as extremist. While not strictly related to the F2C, the control of content providers resembles historical actions to restrict the press. "In November, we got an

order from prosecutors recommending that we close access to extremist sites," [WiMax chief executive Denis Sverdlov] said in e-mailed comments. "Since we are a law-abiding firm, we put the order into practice." Blocked sites include advocates of the Bolshevik Party and Chechen rebel website Kavkazcenter.com.

Licensing regulations further illustrate how the government uses its authority to limit the meaningfulness of access. Freedom House (2015) reports that:

> Under current legislation, in order to receive an operating license, ISPs are required to install equipment that allows security services to monitor internet traffic. ISPs that do not comply with SORM system requirements are promptly fined, and may have their license revoked if problems persist. Russian authorities are technically required to obtain a court order before accessing an individual's electronic communications data; however, the authorities are not required to show the warrant to ISPs or telecom providers, and FSB officers have direct access to operators' servers through local control centers. At the same time, experts note that there is no information about government efforts to bring to account security officers who abuse tracking methods. ISPs and mobile operators are required to provide network access to law enforcement agencies in conducting search operations, as well as provide other information requested by the prosecutor's office, the Interior Ministry, the FSB and the Investigative Committee (660).

Unlike the US case, where the PRISM program is enabled with the voluntary cooperation of ISPs and search engines, the monitoring equipment is a requirement for providers under the mandate of FSB. *The Guardian* reports in "Inside the Red Web" that SORM further differs from the PRISM program in that it dates back to the days of the KGB. Before Putin came to power, journalists and Internet media activists attempted to contact FASPI workers for further information. In 1998, cryptologist Vika Egorova obtained a draft document that was marked "approved" that described SORM and through her private contacts had it published online by a Russian libertarian Anatoly Levenchuk. It was discovered that SORM was really SORM-2, successor to the KGB program that tapped telephone lines.

> "Big, old-fashioned tape recorders turned on at the beginning of a conversation and started recording," [SORM expert Boris Goldstein] recalled. "All of this was done in secret… In other words, the methods of Sorm directly descended from when no one thought of court-approved warrants — from the Soviet system of phone wiretapping.

ISPs have put up little resistance to the SORM project, and mostly complained of the financial burdens of the required equipment rather than the violations of their consumers' rights or the autonomy of their business. Levenchuk gave up the crusade against SORM when none of the ISPs resisted, tacitly accepting the limitation of democratic freedoms on the web.

Monitoring practices continue. “The lack of precise guidelines sometimes leads telecom operators, which are responsible for complying with blocking orders, to carry out the widest blocking possible so as to avoid fines and threats to their licenses (Freedom House 2015, 654).” Operated by a search engine owned by the Russian state, *Sputnik News* reported in 2013 that three smaller ISPs were brought to Supreme Arbitration Court and fined 30,000 rubles (US$1,000) for “violating the terms of a license for entrepreneurial activity.” They had violated a 2012 law that blacklisted websites that threatened the safety of citizens, including those related to drugs, suicide, and child pornography. Rostelecom controls the blacklist, but Novosti notes that it is only half-heartedly enforced and these small ISPs may have been made examples of to serve as a warning. The concerns over these websites and the downloading of copyrighted content is not the responsibility of the user; instead ISPs and search engines must control how the content they provide is used.

These policies are indicative of larger patterns among the government, ISPs, search engines, content providers, and the public. Moskvitch reports in 2013 on the backlash against such anti-piracy efforts mirrored the debate surrounding the US’s now defunct Stop Online Piracy Act. US lawmakers were pressuring Russian law enforcement to crack down on piracy where sharing entertainment files for free is as prevalent as Netflix is in the US. Torrent Freak, founded by an independent activist who identifies himself as Ernesto Van Der Sar, comments that the law was really a new means of censorship. The Russian Pirate Party stated "Access to online content should be free and global, because it is people's right to freely receive and distribute information, as well as it is their right to consume art (Moskvitch).” The Russian-based Pirate Party a bottom-up normative venture to fight the censorship and fight over artistic intellectual property including movies, music, and the like—has affiliates in many other states. Yandex comments that the censorship measures are "directed not at fighting pirates, but at the internet itself - and it's almost like permanently closing down a highway where one accident occurred (Moskvitch)."

The Guardian also reports policy proposals circulating about a Russian intranet[44] that would unplug Russia from the greater World Wide Web. The rhetoric justifying the moves is anti-American and

[44] An intranet is “[a] private network that uses Internet software and Internet standards. In essence, an Intranet is a private Internet reserved for use by people who have been given the authority and passwords necessary

techno-nationalist, asserting a need to ensure that an integral part of Russian infrastructure remains under state control. Cyber sovereignty, a norm emerging from authoritarian states that can be seen as a reaction to the F2C, was not stated by the Russian state but is evident in this scheme. Despite being reminiscent of the Cold War, it was uncovered that the US's PRISM program had spied on world leaders (Germany, Brazil, and several others), and as such fears of American actions on the web are not unfounded. Nevertheless, it can be seen as a window of opportunity to again increase state control over the Internet regardless of the scope of the threat. Combined with the fact that many of the state's ISPs are state-owned or highly tied to the state, like Rostelecom, and that Russia has relatively few IXPs, it would be fairly easily to greatly restrict the Internet in Russia. However, as many smaller ISPs have purchased access from the outside it could not do so entirely. It would also take over direct control of national domains from .ru, .su, and Cyrillic .рф; today domains must be registered through the Russian bureaucracy for approval.

Freedom House (2015) reports that in the summer of 2014, the Ministry of Communication, along with the Ministries of Defense, the Interior, and the FSB conducted a joint experiment to test if they could disconnect Russia from the global Internet. Domains ending in .ru and .рф were shut off at their server locations in Moscow, Novosibirsk, NY, Amsterdam, and Hong Kong. Officially the tests were to develop policy in the case the Internet was cut off from the outside, citing fears over US control of the Internet, but journalists uncovered that the experiment was also meant to test the feasibility of turning off the Internet from the inside. According to Harding, the impetus for such tests is concerns over possible civil unrest stemming from oligarchic abuses and a floundering economy. The influence of the Arab Spring—and the resultant chaos—is impossible to ignore.

Domestic Attitudes towards Access and Policy

The global surveys reviewed in this study all address the opinions of Russians dating back to 2008. Kull et al. (2008) show that 64 percent of Russians believe that it is important that the news can publish what they want without governmental control, 57 percent believe that they should be able to read whatever they want on the web without restriction, and that 56 percent argue that the government should

---

to use that network. Those people are typically employees and often customers of a company (Newton 612)."

not be able to restrict these rights arbitrarily. GlobeScan (2010) showed that Russian Internet users are technology-dependent, 71 percent reported they could not live without being connected and that 58 percent of them believe that the most important use for the medium is to find information. Fifty-two percent believe that the Internet should not be subject to any regulation. Internet Society's 2012 survey revealed yet again that public had great expectations for the government and the provision of access, with 83 percent remarking that it should provide cheaper computers, 82 percent arguing that should encourage competition among providers, and 81 percent saying that the government had an obligation to provide access.

Eighty-seven percent of the survey respondents argued that Internet access should be considered a right, 88 percent argued that freedom of expression should be guaranteed, and 81 percent said that freedoms of association and assembly were enhanced by access. Only 49 percent would accept increased controls in exchange for safety, and 62 percent argued for the right of government to set whatever Internet policies it wished. In Pew's 2015 survey on the freedom of expression on the Internet, 79 percent of Russians agreed that it was either somewhat or very important to maintain the principle. It is apparent from these surveys that government policy and citizens' beliefs about the role of Internet in their lives and the government are divergent.

***

The move of Russia from Partly Free to Not Free was predictable, and is tied more to its efforts to censor ideas and control discourse on the web than its efforts directly related to the F2C. Its assertion of cyber sovereignty and its testing of shutting of parts of its Internet infrastructure are symbolic of the greater moves away from democracy and towards authoritarianism. Yet, unlike cases in the Not Free category, the state utilizes some of the language associated with the F2C, which includes not only equality of opportunity but also the freedom of expression, even if only half-heartedly.

Mexico

Mexico's experience with the Internet resembles Brazil, Indonesia and other states that have attempted to increase overall levels of access and to bridge the digital divide between urban and rural, young and old, and the wealthy and impoverished. The state has taken measures including amending its constitution in 2013 to recognize Internet access as a civil right. Yet the telecommunications market is dominated by six ISPs, one of which is owned by the second richest man in the world and enjoys *de facto* monopoly status. Another major problem concerning Internet freedom are digital journalists who cover drug cartels that often become targets of retribution. While the government signed a law to protect them in 2012, it is not strictly enforced, which lowers Mexico's Freedom House score. The desire to become a technological "hub" in Latin American is overshadowed by the concentration of power and the plague of violence that threatens the lives of activists, journalists, and politicians.

Background

Mexico is a moderately large and powerful state. It has a population of 121,736,809 (12th in the world), and takes up an area of 1,964,375 km^2 (14h in the world). It has a large urban population, encompassing 79.2 percent of its population, with six major metropolises with about two million people or more[45], including Mexico City, one of the largest city proper and metropolitan areas in the world. The state is characterized by socioeconomic divisions among its 32 states/districts, with the richest including the Federal District and those located along the US border and the poorest concentrated in the south. Mexico's annual GDP is $2.149 trillion, ranking it 12th in the world, with a GDP per capita is $18,000, ranking the state 90th in the world.

Mexico has 21.1 million landlines, ranking it 14th in the world; one phone is plugged in for approximately every 18 people in the country. The figure escalates for cellular phones, with 102.2 million in the country, placing it 14th in the world. In total, there are 49.5 million Internet users in Mexico which ranks the state 12th in absolute numbers, and totals 41.1 percent of the population. Users are concentrated in major cities where infrastructure is widely available.

[45] Mexico City (capital) 20.999 million; Guadalajara 4.843 million; Monterrey 4.513 million; Puebla 2.984 million; Toluca de Lerdo 2.164 million; Tijuana 1.987 million (2015)

Mexico had a tumultuous history with democracy in its early years and had been dominated by a single, sometimes corrupt, political party for the majority of the 20th century. Liberal norms have nonetheless developed, first having been used instrumentally since independence in 1821 and developed and matured as evidenced by its various constitutions. Since the 1917 revolution, protected rights have been largely socioeconomic in nature, including environmental protections, rights to health and education, and indigenous rights. Johnston admits that protecting cultural rights against globalization is more difficult in the concrete than the abstract, but nonetheless Mexico should be considered, at least legally, as a bastion for "lovers of liberty." More difficult is implementation: "Even though every Mexican has at reach procedural tools such as the amparo, recourse before the Human Rights Commission, claims for patrimonial responsibility of the State, etc., the reality proves that there is a big gap between the letter of the law and its implementation (Johnston)." Instead, poverty and underdevelopment hinder the meaningful application of human rights standards. The "will and opportunity" for people to implement human rights is largely missing in an undereducated, underemployed populace. The political climate of Mexico has been a challenge to the application of human rights throughout its history. The near total dominance of the PRI, and the current overwhelming corruption of the political and police systems due to the influence of drug cartels, creates a vast divide between what human rights have been articulated and what can actually be achieved.

The Internet in Mexico

Background. Mexico's history with the Internet begins in academia. The National Autonomous University of Mexico (UNAM) had the first computer in Latin America in 1958, and its purpose was to support computation for intensive fields like applied mathematics, physics, and engineering. The geographic advantage of proximity to the US allowed the institution to rent the computer for 25 pesos per month from the University of California, the same institution that would be instrumental in the creation of ARPANET. Unlike other cases explored, such as Indonesia, UNAM institutionalized the use of computers not only for academic computations but also administrative purposes, bypassing the tradition of networking being a pastime for academic ICT experts and enthusiasts.

In 1982 UNAM connected to ARPANET. By 1986, UNAM had networked computers across academic facilities that is generally the precursor to further international connections. In 1987, the

University of Monterrey was connected to BITNET, and by 1990 UNAM established a 56 Kbps satellite link to the Internet with the University of Colorado, Boulder. By the early 1990s, academic institutions came together to promote the Internet and establish some of the necessary infrastructure; MEXNET, AC established the first national backbone and began to shape the idea of the popular use the Internet outside academia. By 1994 the Internet was legalized for commercial use, and the Centro de Información de Redes de México (NIC) was given the task of assigning domain names, .mx, starting with 150 addresses in academia and later expanding to businesses.

Mexico's expansion of the Internet into residential and commercial markets included the consolidation of what became hundreds of ISPs into Telmex, which at the time was the government-run monopoly of telecommunications industry. Today, it is a subsidiary of América Móvil, owned by magnate Carlos Slim who incidentally studied civil engineering at UNAM when computers and networks were getting their start.

Speed and cost. Access is limited in Mexico according to several criteria: geography, education, and age. The CIA reports the total penetration rate of 41.1 percent of the population, while the ITU (based on the statistics provided by the Instituto Nacional de Estadística y Geografía (INEGI)) reported 44.39 percent in 2014. Speeds in Mexico appear to be slow but not crippling, with an average download speed of 5.9 Mbps in Q4 2015 and an average peak speed of 29.9 Mbps, with each statistic improving about improving between 20 and 30 percent over the same quarter in 2014 (Akamai). Speeds vary greatly according to one's location in Mexico. Below are reported cities across the country:

Table 9 Reported Internet speeds by Mexican city
(testmy.net 12 April 2016)

City (State)	Downstream	Upstream
Mexico City (Distrito Federo)	18.1 Mbps	5.1 Mbps
Hermosillo (Sonora)	7.2 Mbps	1.5 Mbps
Tijuana (Baja California)	6.4 Mbps	1.1 Mbps
Veracruz (Veracruz)	6.2 Mbps	1.9 Mbps
Chilpancingo (Guerrero)	4.4 Mbps	498 Kbps
Tuxtla Guiterrez (Chipas)	3.5 Mbps	293 Kbps
Oaxaca (Oaxaca)	1.6 Mbps	345 Kbps

Numbeo estimates costs to be $21.89 per month for 10 Mbps, or about 3.79% of net monthly income, within range of the UN target.

Penetration and geographic divide. Mobile penetration in Mexico is relatively good for a developing state but is far less than most developed states; 83 percent of Mexicans have cell phones, while 40 percent have access to mobile broadband, usually 3G or better. Smartphone use is increasing because of lower costs and the gradual introduction of competition like Nextel and AT&T. A subsidiary of América Móvil Telcel introduced 4G-LTE capability in late 2012 in partnership with Ericsson in nine major cities. Today, more than fifty cities use 4G service from Telcel, but rural areas of Mexico remain underserved (Sensorly). AT&T announced coverage plans in five cities in 2015. In its announcement, the AT&T CEO in Mexico framed the extension of service as positive for economic growth. Nonetheless, mobile penetration remains concentrated in major cities with industrial capacities; outside, it appears that 2G coverage or above is difficult to come by (Sensorly).

The INEGI published a raw data set on Internet use that was the result of a survey of Internet use across Mexico in early 2013. Los microdatos del Módulo sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (MODUTIH)[46] survey was published in 2014 and contained data on almost 130,000 respondents, including questions relating to both computer and Internet use, frequency, location, and reasons for use. To begin, of the total number of respondents, 50.24 percent answered they had used the Internet within the last 12 months, while 49.76 percent had not. Of those that did, nearly half (49.66 percent) used it on a daily basis, meaning they likely had a direct connection in their home or used a smartphone. Forty-three percent used it a least once a week, while 6.68 percent had accessed the Internet once per month. Less than 1 percent reported using the Internet infrequently when they had reported using it at all, with 0.83 percent reporting use at least once every six months and 0.22 percent at least once a year. The report also outlined where they accessed the Internet:

[46] Availability and Use of Information Technologies in the Household.

Table 10 Location of Internet access in Mexico
(INENGI)

Location	First Choice	Second Choice*	Third Choice*
Home	56.84%	13.00%	3.94%
Work	10.91%	30.99%	2.19%
School	5.90%	24.76%	11.42%
Public site (for a fee)	22.52%	19.96%	24.51%
Public site (free)	0.92%	4.16%	26.92%
In the house of another person	2.58%	5.96%	23.17%
Other	0.32%	1.18%	7.85%

*Only 37.12% of survey respondents had a second choice for where they access the Internet and only 4.13% had a third avenue of access.

Public sites, free or otherwise, are common avenues of access for those of lower socioeconomic status. They are supplied both by NGOs and government initiatives.

As has been explored in other cases, Mexico faces a geographic divide among its states. There is a reported 26 percent difference between people who have accessed the Internet in 12 months among the 31 states and the federal district in Mexico—a considerable range—summarized below:

Table 11 Survey participants reporting on Internet use in the last 12 months, by Mexican state
(INENGI)

State	Yes	No
Sonora	62.54%	37.35%
Distrito Federal	61.64%	38.36%
Baja California	61.28%	38.57%
Colima	59.39%	40.49%
Baja California Sur	57.57%	42.26%
Nuevo Léon	57.16%	42.84%
~~		
Oaxaca	43.36%	56.49%
San Luis Potosí	41.90%	57.19%
Veracruz de Ignacio de Llave	41.04%	58.89%
Tlaxcala	40.74%	59.19%
Guerrero	39.95%	60.03%
Chiapas	36.47%	63.51%

States that reported high rates of Internet use tend to be among the richer ones in Mexico that specialize in industrial production and the service industry over agriculture. Sonora and Baja California's proximity to the US mean that maquiladoras[47], a contentious albeit popular area of employment are rather

[47] "…a factory that enjoys special tax breaks. When Mexico set up the first maquiladoras half a century ago, they were sweatshops that simply bolted or stitched together imported parts, then exported the assembled product north across the border to the United States. America got cheap goods; Mexico got jobs and export

common, and could explain both the availability of the Internet and the high rates of use. The Distrito Federal is made up of Mexico City proper and its metropolitan area, and is known to be Mexico's "economic and cultural hub (History 2010)," enjoying a GDP per capita that is the highest of any city in Latin America. The states reporting the lowest use of the Internet—Tlaxcala, Guerrero, and Chiapas—share two important features. First, they are economically driven by agriculture, a feature that many under-connected regions share amongst all the cases examined in this study. They also have minor manufactures (textiles) and are supported by tourism. Second, they are populated by indigenous, traditionally marginalized groups which is another feature of poor Internet access that is shared across the cases in this study. Indeed, Guerrero and Chiapas are continually plagued by violence perpetrated by both drug cartels in pursuit of profit and guerilla Zapatistas in pursuit of autonomy.

The survey also included a question addressing why people do not use the Internet. As has been explored in much of the literature on the digital divide, access is not simply about the physical existence of infrastructure, but includes concerns over speed, cost, and ability for users to understand computers and software.

Table 12 Mexican survey participants reporting why they do not use the Internet (INENGI)

State	Do not know how to use	No need/ Usefulness unknown	No access	Other
Sonora	50.30%	40.88%	8.01%	0.67%
Baja California	57.63%	35.41%	6.43%	0.52%
Distrito Federal	50.04%	39.53%	9.51%	0.92%
Colima	46.58%	63.84%	9.71%	1.37%
Baja California Sur	45.82%	41.39%	11.56%	1.07%
Nuevo Léon	57.00%	28.83%	12.94%	1.22%
~~				
Oaxaca	48.79%	45.62%	5.192%	0.40%
San Luis Potosí	49.53%	41.77%	8.35%	0.34%
Veracruz	56.39%	36.34%	6.81%	0.39%
Tlaxcala	43.25%	46.19%	9.74%	0.87%
Guerrero	64.14%	29.26%	6.43%	0.16%
Chiapas	60.08%	33.01%	6.78%	0.10%

Unfortunately, the survey did not address the issue of prohibitive cost. The lack of direct access is not a primary cause of why people do not use the Internet; it presumes that the other two reasons most often

revenues. [Today,] the maquiladoras are having to up their game, moving into more sophisticated types of manufacturing and doing more product design (*The Economist* 2013b)

reported—digital illiteracy and lack of interest—were overcome. There are slightly more people that reported digital illiteracy in states that reported low access frequency, but the number of people who had little interest or need in the Internet remained remarkably similar across the states. There is a correlation in the US among age, socioeconomic status, and the desire to use the Internet; in 2015 Pew reported 39 percent of adults did not go online were 65 or older compared to just 3 percent between ages 18-29 (Whitney). Presumably this relationship between age and desire for access exists in Mexico as well. Additionally, with the increase in availability, more people will find uses for the Internet in ways than are currently unimagined. The lack of knowledge is one of the most important barriers to be overcome, or as Sujarwoto and Gindo Tampubolon (2013) suggest, proliferation of the Internet will exacerbate, rather than reduce socioeconomic inequities thereby putting those with deficiencies in education, language, or skills further behind their counterparts.

Humberto Merritt studied the digital divide in Mexico (2011), discussing the factors that primarily and secondarily affect Internet diffusion and the hits and misses of the Mexican government's efforts to reduce it. Reviewing the literature, Merritt recounts much of what this study has already discussed: affluence, urbanization, and education levels all have great predictive power about people's access and use of the Internet. The more symmetrical the marketplace and the lack of burdensome regulation, along with factors like age and ethnicity, also have roles to play in determining Internet diffusion. The important barriers in Mexico in particular are the following:

> 1) Lack of any digital experience caused by individual (or collective) apathy, computer fear and unattractiveness of the new technology.
> 2) No possession of computers and network connections.
> 3) Lack of digital skills caused by insufficient user-friendliness and inadequate education or social support.
> 4) Lack of significant usage opportunities (127).

The temptation to paint the first barrier as temporary and isolated is compelling, particularly to think that disinterest lies with the elderly, housewives, the illiterate, or the unemployed. But such estimations are largely due to biases from a developed state's perspective. Nonetheless, the e-Mexico program was undertaken during a time when few people desired or could realize the benefits of access to the Internet. The usefulness of access was questioned by Merritt and Bill Gates (2005), and the applicability of "Knowledge Centers" for the illiterate, or the use of satellite mapping of schools of fish for fisherman who

do not the possess the equipment to take advantage of the information. "Far better, it would appear, to spend scarce resources on combating AIDS, say, or on better sanitation facilities (Merritt)."

Such concerns, despite being put forth over a decade ago, remain relevant for Mexico. Nevertheless, there is a growing recognition that development without taking into account the importance of technology do citizens a disservice, because economies will only become more reliant on technology in the coming decades. As the MODITUH revealed, a great number of people report unfamiliarity with using the Internet, either know-how or its possible applications to everyday use. The programs below have had different approaches to bridging these gaps.

National Digital Strategy

In 2013, the government of Mexico adopted a national digital strategy as part of the common practice encouraged by the WSIS to establish short, medium, and long-term targets for Internet penetration and use. States have framed their vision regarding access in these policy documents often relating to the tenets of the F2C. While Mexico's plan does not establish specific targets, it envisions the increase in Internet penetration as essential to the economic and social development of the country.

The plan contains five objectives:

1. Government Transformation: Build a new relationship between society and government, focusing on the experience of the citizen as a user of public services through the adoption of ICTs in the government.
2. Digital Economy. Develop a digital economy ecosystem that will contribute to achieving a prosperous Mexico, through the assimilation of ICTs in economic processes, to stimulate increased productivity, economic growth and formal job creation.
3. Quality Education: Integrate ICTs into the educational process, in both educational management and teaching and learning processes, as well as teacher training and the dissemination and preservation of culture and art, to allow people to be successfully inserted into the Information and Knowledge Society.
4. Effective Universal Health: Create a comprehensive digital health policy to harness the opportunities offered by ICTs with two priorities: on the one hand increase coverage, effective access and health service quality and on the other, make more efficient use of installed infrastructure and the resources allocated for health.
5. Public Safety: Use ICTs to prevent social violence, by coordinating the efforts of citizens and authorities around common objectives to promote safety and prevent and mitigate the damage caused by natural disaster (16).

None of these objectives are framed in terms of rights, and instead contain a largely utilitarian vision of what an increase in use and knowledge about ICTs can bring to users in Mexico.

Nevertheless, the plan acknowledges that human rights will be bolstered by the increase in ICT availability. First, because some elements of governance will brought online, people will be better able to

obtain services and second, that the use of ICTs is a human right in itself (32). Each of this goals are listed under "inclusivity" heading, indicating that the plan must come to terms with the digital divide in Mexico. Elsewhere, digital literacy is emphasized in order to make equitable use of ICTs.

Public-Private Partnerships and NGOs

To combat the low levels of access and bridge the various digital divides that exist in the state, NGOs and government initiatives work alongside each other to increase both physical and meaningful access. One of the state's methods for bridging the digital divide has been to remove barriers from the marketplace and increase public spaces rather than get directly involved with infrastructure development. It may be that this is case as a consequence of a strong belief in the liberal market system, and also the concentration of power that allows América Móvil to keep profits ahead of efficiency. While Carlos Slim sits as one of the co-chairs of the International Broadband Commission, the sincerity of his commitment to the Commission's goals is questionable. Perhaps like illiberal states that sign onto human rights instruments to improve their perception, a bit of corporate goodwill could deflect some of the criticism his company receives.

Public access. Government efforts date back to 2002. Like its successor, the e-Mexico program focused on the construction and the running of community access centers. Then-President Vicente Fox pledged $68 million to install 3,200 community Internet access centers in schools, libraries, and town squares, and had promised 10,000 such places by the end of 2004 (Anderson). These pledges proved successful, as Mexico Conectado reports that by 2015, 70,000 public spaces provide free Internet access. Run by the Ministry of Communication and Transportation, Mexico Conectado's mission was bolstered by the recent amendments to the Mexican constitution that guarantees access as right. In order to achieve it, the website claims that through economies of scale and preexisting infrastructure, 250,000 public spaces can be ready to provide free Internet to the public by the end of 2018. The program frames access as both a right and an enabler of other rights like work, education, and even participation in the public policy process.

Mexico Conectado won the "WSIS Project Prize" in 2015, which is meant to showcase programs that have shown success in increasing access that could be replicated by other developing states. While not a PPP, the cooperation among the state, NGOs, and ICTs is representative of the model that WSIS

espouses. Hughes Communications provided satellite equipment and service in conjunction with the Mexican Ministry of Communications and Transport, which runs the Mexico Concectado program and operated by a decentralized government office Telecomm Telegrafos. The program was going to include 11,000 broadband terminals, and even used solar power to support the equipment.

Huerta and Sandoval-Almazán study the problems of these telecenters in 2007. While outdated, the study surveyed users in the state of Mexico largely from lower income villages. The authors reviewed the skillsets necessary that allows users to make use of computers and the Internet, and users in this study new to computing could overcome some of the limitations by user-friendly interfaces that were easy to navigate. They determined a plethora of problems facing digital immigrants in Mexico: lack of English proficiency, the inability to expand searches for related information (the "branching" skillset), they did not critically assess information that was provided (information skillset), and that they saw no use for the technology beyond recreation or chatting. The primary telecenter users were students, who regularly copied and pasted information from encyclopedia entries, and did not learn to synthesize the information they found in any new way. Users in the telecenter saw the use of the Internet with only a limited functionality, and either did not know or did not bother to develop other skills that would be important in the global marketplace. Even more telling was the study's observation that operators of these telecenters suffered from many of the same limitations as users; partial digital literacy would grossly underserve those who use these facilities, and simply training someone on how to turn machines on would not be enough to make the telecenters have an impact beyond rudimentary access.

An NGO attempting to bridge the digital divide in Mexico, Fundación ProAcceso takes into consideration some of the weaknesses of the older models of community centers to heart. It was founded by Aleph Molinari in 2008, an entrepreneur who having experienced Mexico's inequality firsthand, who having "studied economics and critical theory abroad and returned home with the idea of doing something to narrow the country's socioeconomic divisions (Villagran)." The group frames their mission of increasing Internet access—both physical and meaningful access—to the larger issue of the equal education. This mirrors the Kansas City NGO Connect for Good sentiment that connects economic opportunity with access. By democratizing access, it would have a positive impact on disadvantaged groups. In collaboration with the government, ProAcceso began with 10 training centers that specialized

in teaching computer skills to increase educational opportunities and employment, and initially expected to attract 50,000 users. It exceeded that figure by 25 percent, and gained the support of foreign partners: "Microsoft donated $1.7 million in software licenses; Google donated its Labs, AdWords and educational programs; Dell donated the equipment to outfit two learning centers (Villagran)." They work with local NGOs, MNCs like Google, Nokia, and, the international organizations like the World Bank and UN Information Center.

These Red de Innovación Aprendizaje (REIs)[48] now total more than 70 with 420,000 users and 127,000 graduates in the State of Mexico. The foundation also funds digital libraries and microenterprise centers. While the majority of these centers are located in dense, urban locales—which already ignores one of the fundamental digital divides—it teamed with Dell to open its first rural location in San Felipe del Progreso in the state (territory) of Mexico. It partnered with Nokia to create a REI with something they called a "Makers Lab" that included three-dimensional printers, laser cutters, and sophisticated metal routers (Canal AR). These partnerships among public, NGO, and the private sector is emblematic of the types of relationships touted by the UN community.

Internet Para Todos[49] is the result of a hyperlinked network of NGOs working on Internet, whose purpose is using its resources to enable free, unhindered access to the Internet. It was used in 2013 to gather signatures for a petition to lobby for the inclusion of Internet access as a civil right to be articulated in the Constitution. Its blog highlights other efforts to increase penetration, including online courses to familiarize learners with Internet use, wireless charging technology, statistics on the usage habits of the young, and touting 5G as the "network that will connect all." They link the cause of telecommunications reform to the norms of the F2C:

> Those involved in the project share the diagnosis of centralization and monopoly of traditional media (particularly television) as well as the *violation of human rights* that this situation causes, so we decided to build a project that seeks to force, to through constitutional and legal reform, the State to use the existing infrastructure to create a network of free Internet in virtually the entire country [emphasis added].

[48] Learning Innovation Networks
[49] Internet for all

Internet Service Providers

The shape of Mexico's telecommunications market has dramatically shifted in the past few years due to government intervention, forbidding any company from controlling more than 50 percent. This stems from the recognition that the state must enable conducive conditions for the private sector to function properly. First, President Enrique Peña Nieto issued a decree to amend the constitution to recognize the following as human rights: "(i) information and communications technology, and (ii) broadcasting and telecommunications services, including broadband and the Internet (Arroyo)." The law forbids the government from limiting access or censorship in any way, and reimagines telecommunications and broadcasting as public services, rather than simply valued-added services.

The Mexican Senate in 2013 approved a bill to de-monopolize the telecommunications market that was made up of 6 companies but was dominated by América Móvil. The legislation passed by an overwhelming margin, 103 to 3, and was accomplished in coordination with the PRI's traditional rivals that stemmed from a series of social reform laws in the areas of labor and education that was dubbed "Pact for Mexico (Al Jazeera)." Providers cannot refuse to provide certain services and requires the installation of infrastructure that would increase mobile access.

> The Law provides a new kind of public/private network structure, called "public telecommunication networks with public participation." The concessions for commercial use to public bodies under a public-private partnership scheme have the character of "shared network of wholesaler telecommunications services." Such networks cannot provide services to final users (Arroyo)

Carlos Slim's company at the time controlled 80 percent of the landlines under Telmex (which had been privatized in the 1990s) and 70 percent of the mobile market under Telcel. Freedom House reports that Axtel, the next largest supplier, had only six percent of the landline market and Movistar claimed 20 percent of the mobile market. In anticipation of government mandates, Slim sold enough of the company's assets in order change América Móvil's status as a "preponderant economic agent (Estevez 2014)." The effect has been harmful to the company, contributing to the fall of its stock price and Slim's personal wealth (Estevez 2015). "The legislation aims to increase foreign investment, allowing non-Mexican companies to own 100 percent of the capital of a telephone firm - compared to 49 percent today - and almost half of radio and television broadcasters - compared to zero today (Al Jazerra)." These

efforts seems to have paid off; AT&T bought the mobile provider Iusacell in late 2014 and Nextel in early 2015.

The new law also created Federal Institute of Communication (IFT), whose mission was to guide competition in the restructuring of the ICT market and was given constitutional autonomy. In recent months, the IFT has taken up cause to force Telmex to open up its "last mile" portion of network to competitors (Keane, Sarmiento and Barrera), meaning the portion of Telmex's ICT infrastructure that connects to customers. It was ordered to make it available after 60 days in June 2015, but got a 20 day extension in October. As of April 2016, it is unclear what degree Telmex has turned over control to other suppliers.

An article in *PC Magazine* provides the only other discussion of ISPs in Mexico besides the ongoing efforts to unmake Slim's empire. Critical of the constitutional reforms, the article repeats the dubious claim that the amendment gives the government sweeping control over the Internet, users, and an "ON/OFF switch." Nevertheless, it profiles the competitors to Telmex and what they have contributed to the increase in Internet penetration and meaningful access. Axtel was the one of the earliest competitors to Telmex, and provides the best service in Mexico with average downstream speeds of 44.5 Mbps. In order to compete, Telmex offers packages that include 200 Mbps and 20Mbps at $44 per month, but because service is unreliable, the magazine does not see the Telmex offerings as worthwhile. Unfortunately,

> Once you move past third place [in the rankings], things drop precipitously again; none of the bottom six make it past a PCMag Index Score of 10.0. These ISPs represent the past, the older services that grew out of the privatized government utility companies and grew rich by offering pitiful and overpriced Internet service to a country that had no other options (Sosa).

It is apparent that despite government efforts to curb the monopoly of Telmex, Mexican users, like their American counterparts, face limited choices. Yet considering the attempts to wrest control from Telmex, encouraging foreign investment with the likes of AT&T, articulating access as a civil right, and opening last-mile services to competitors, the government has taken steps in the right direction to reshape the telecommunications market.

The IFT also provides reporting mechanisms for customers about poor quality or speeds, using language that is remarkably similar to net neutrality norms. "Your operator must respect the

characteristics of the service you hired regardless of content, origin, destination, terminal or application that you want to access, as well as services that are provided over the Internet!" If the ISP fails to comply with the promised speeds, the IFT can impose sanctions upon them. Such a policy mirrors the efforts taken by Brazil in 2014.

The IFT announced that it would be investing into infrastructure along with the Federal Electricity Commission. Since the switch to digital television, the 700 MHz band had been freed for mobile phone use, with goal of increasing the size of the market and lowering the price for consumers. The National Digital Strategy articulates the desire of the state to enable the market to provide access by eliminating "prevailing extraordinary agents" that hold the industry back, especially for "sectors of the historically disadvantaged population."

Domestic and International Rhetoric

Mexico City was host to the Ministerial Conference on the Information Society in Latin America (eLAC) in August 2015, a bid to continue its pursuit of being a "hub" for digital technologies in Latin America. Mexico Conectado boasted that:

> The signatories pledged to continue to strengthen regional cooperation in digital matters with regional projects, activities aimed at promoting innovation, the formation of digital capabilities, the spread of new technologies and promotion of best practices, especially in an environment of inclusion and sustainability (Mexico Conectado 2015b).

The declaration stemming from Mexico City tied the efforts of eLAC to the wider Internet freedom community, including WSIS and the UN General Assembly and recognized the right to privacy in the digital era. The Digital Agenda for eLAC (2018) contains 23 objectives within five general areas, and includes first a commitment to increasing access and bolstering infrastructure, which includes the creation of community networks, IXPs, next-generation broadband networks, keeping in mind "vulnerable groups" and even the "gender perspective."

There are several survey reports on Mexico available, dating back to 2008. Kull et al. report that Mexico had the highest percentage of respondents that argued for the media to publish information without government control, while only 17 percent argued that the government should be able to restrict access and content in the name of stability. GlobeScan (2010) reported that only 14 percent of Mexican Internet users would be able to cope without it, the lowest percentage in the world. Ninety-four percent argue that it should be considered a human right. Pew (2014b) reports that in 2013, 79 percent of

Mexicans argued for uncensored Internet, and the percentage climbed according to youth, with 85 percent reporting such an opinion between the ages of 18 and 29. Forty percent reported freedom being a very important issue surrounding Internet use, 39 percent stated it was somewhat important, 13 percent said not too important, while only six percent argued that it was not at all important. By 2015, Pew (2015b) reports that 83 percent of Mexicans believed it was important to use the Internet without censorship.

***

Mexico's barriers to access include burdensome geography, a monopolistic telecommunications market, and entrenched inequality that has an unfortunate tendency to perpetuate itself in the digital realm. The state has taken great strides to become a "hub" of Latin America and has been influenced by the metanorms of the IS, WSIS, and other entrepreneurs involved in the construction of the Internet freedom regime. Its measures to increase public access spaces, to dismantle the Slim empire, and add Internet access as a right to its constitution all signal the strong impact of the F2C.

Indonesia

As with the Philippines, Indonesia's Internet penetration is hampered by a populations spread across many islands that enhances the socioeconomic causes of the digital divide. The state and private sector have worked to bridge the digital divide—sometimes together, sometimes, separately. There is evidence that the state is moving toward norms relating to the F2C, but such moves are hampered by the cronyism that is endemic to Indonesian politics.

Background

Indonesia has the world's largest Muslim population, making up 87 percent of its total of 256 million people (July 2015 estimate), ranking the country 5th in the world in overall population. Iran has a larger percentage of Muslim citizens, but a discussion of how Indonesia accommodates the presence of the Internet in the face of religious beliefs is enlightening. It is a large state, comprising 1,904,569 km^2 (15th in the world), and is the world's largest archipelago-state with 6,000 inhabited islands. Access is greater surrounding large cities on Borneo, Java, and Sumatra rather than those on less populated islands. Fifty-four percent of its population lives in an urban area, with 6 major metropolises with populations of 1.4 million or more[50]. It has the 10th largest economy in the world with a GDP of $2.84 trillion, yet this equates to $11,300 GDP/capita, which means that despite the size of its economy, it only ranks 131st in the world.

Looking at its ICT technologies[51], Indonesia has 29.67 million landlines, ranking 11th in the world; one phone is plugged in for approximately every 8 people in the country. There are 319 million cell phones in the country, placing it 4th in the world; like China, mobile phones are often seen as a viable alternative to wired Internet connections. In total, there are 42.4 million Internet users in Indonesia which ranks the state 14th in the world in total numbers, but amounts to approximately 16.7 percent of the population. While the CIA and the ITU report Internet use at 16 percent of the population, the Association of Indonesian Internet Service Providers (APJII) reports the same figure to be 28 percent. In all likelihood, the former figure is closer to the truth; it is unsurprising that a domestic organization would inflate statistics in order to offer a positive reflection of the association's members' activities.

[50] Jakarta (capital) 10.323 million; Surabaya 2.853 million; Bandung 2.544 million; Medan 2.204 million; Semarang 1.63 million; Makassar 1.489 million (2015)

[51] CIA Factbook 2015

It is difficult to disentangle the impact of cultural norms of former colonies from their colonial masters' legacies, and Indonesia had been ruled indirectly or directly by the Dutch for almost 350 years. It is necessary to frame their contemporary relationship with human rights with this backdrop of Indonesia's relationship with modernity. While Indonesia is the world's largest Muslim-majority democracy today— perhaps providing a model of democratic norms within Islam—its relationship with democracy is less than two decades old. It is within these rather uncharted waters that the applicability of Internet freedom and the F2C must be analyzed.

Carnegie describes the vast patrimonial networks that persist in Indonesia. "A major post-colonial legacy of the Dutch was…patrimonial networks of political elites who had acquired conditional power as colonial proxies (46)." Both the Guided Democracy and New Order periods were characterized by these patrimonial systems that relied on favors and pay-offs to get things accomplished. Under Suharto, "[p]olitical competition among the elite did not involve policy, but power and the distribution of spoils (55)." The situation persists today as the government's policy implementation is characterized as being at best inept and at worst corrupt. Local elites misappropriate money intended for local-level village projects, and it is not difficult to see what impact that would have on Internet infrastructure projects, especially those undertaken by the state.

Earlier in its history, the influence of human rights did not appear to have strong predictive power. Instead human rights were instrumentally used to challenge the state without directly doing so, mainly by radical student groups during the Suharto era. The belief in the content of the human rights discourse may be strong, but seeing them carried out in practice is not easy.

> One thing is for sure: the politics of pragmatic change is anything but smooth. At the village level, formal political rights are one thing, exercising them is another. Corruption is still rife especially among local elites, with money appropriated from village projects, land certificates overcharged, public land privatized and public social safety nets misused (Carnegie 130).

Citizen Lab reports on more recent developments with human rights, recounting how the constitution was amended several times between 1999 and 2002, changing the language of the document from asserting the 'the existence of the principles' of human rights to legitimate implementation. In a decree (XVII/MPR/1998), the state now affirms rights to expression, association, and even communication. The latter includes guaranteed and protected rights to communicate using all available

channels for “his/her personal development and social environment.” A law adopted in 1999 (Law No. 39 on Human Rights) affirmed that as a member of the UN, Indonesia had an obligation to apply the rights of the UNDHR to its policy and law. However, while these protections are now firmly rooted in place in Indonesian law, it is often curtailed in practice. Partly due to pressures from conservative groups, content in Indonesia is circumscribed, with pornography and gambling sites being regularly blocked. A law that would grant the state power to control content on the Internet was challenged in 2014 by the Press Council because of its vagueness and unconstitutional nature (Freedom House 2014 407). These developments show the government’s practical inclination towards controlling Internet content despite orations about freedoms like expression and association, and the recognition that communication technologies are critical for development in the 21st century. This is a consequence of the mix of influences with which the Indonesia must deal, specifically a multi-ethnic society that at times threatens to ignite in conflict and promote separatism rather than unity, and the forces of both moderate and conservative Islam.

The Internet in Indonesia

Background. The Internet in Indonesia began in an academic setting with amateur radio in the Institut Teknologi Bandung (ITB). Onno Purbo of the ITB describes early Internet pioneers at the institution that experimented with radio packet switching in 1986 and 1987. Early Internet in Indonesia made use of a different protocol, UUCP rather than TCP/IP, for email and access to the rest of the Web and used a sort of intranet, UNINET, among major universities in the country. Describing these early days, Purbo is not immune to the ICT professionals’ narratives that are dominant in his field:

> At that time in the early 1990s the Internet network in Indonesia is better known as a community network. The spirit of cooperation, kinship and mutual cooperation is very warm and felt among the perpetrators. Somewhat different from the atmosphere of Indonesian Internet these days that feels more commercial and individual in most of their activities primarily involving Internet commerce (Purbo).

Indonesians living abroad sparked interest beyond these relatively isolated connections. The list serve indonesian@janus.berkeley.edu allowed for discussion about the sophisticated Internet users enjoyed in California between those living abroad and those in the ITB. Indonet was the first ISP that set up business in Jakarta in 1994, but the state intervened into its service. Purbo recalls that like earlier ICT companies in the 1960s, ISPs in Indonesia would be required to get licensed by the Department of Post

and Telecommunication Services. Speeds were at a respectable 1024Kbps, or 1 Mbps, but required the utilization of undersea cables owned by Sprint and Singapore's SingTel making costs prohibitive for users outside of universities.

The combination of the potential profitable marketplace, the high costs, and relatively slow speeds encouraged 27 licensed ISPs jointed together to create the APJII in 1996. This private-sector association is still highly influential in Internet access and policy in Indonesia. Its stated objectives are to:

1. Assist members in providing quality Internet services for the people of Indonesia.
2. Popularizing Internet to support human resource development in Indonesia.
3. Support the creation of business opportunities Indonesian businessmen by providing global information and communication facilities.
4. Assist the government in an effort to economic equality in this country through the opportunity of access to information and communication evenly throughout Indonesia.
5. Assist members in providing sources of information about Indonesia.
6. Indonesia to increase community participation in international cooperation. (APJII)

The APJII was responsible for the first Indonesian IXP. "Without funding from the government the [Indonesian Internet Exchange] IIX was promoted by the APJII, a non-profit organization which seek sponshorship [sic] with international vendors to build the much needed internet exchange (Alam 2)." Utilizing partnerships with the likes of Cisco, Hewlett Packard, and Microsoft, among others, the Indonesian Internet Exchange (IIX) was built so private and government-owned ISPs like Telkom and IndoNet would not be dependent on foreign-owned infrastructure. Alam estimates that the project saved ISPs on average $70,000 per month in fees that would have went to Sprint or SingTel.

The IIX along with another Internet exchange OpenIXP, do not directly hook into the greater Internet. Instead, Indonesian governments require ISPs use network access providers (NAPs) for global upstream, and moreover local IXPs serve only domestic functions for networks located in Indonesia (Citizen Lab). Is this an attempt that like China, the Indonesian government has established a means to crackdown on users' rights by controlling one of the most important avenues to meaningful access? Such a comparison seems ill-conceived as is evidenced by, a) the licensing scheme that ISPs must adhere to, b) the tariffs on end-users that the APJII is required to collect at the state's behest, and c) the culture of bribery and corruption that is endemic to Indonesian political culture; this final requirement is more likely an attempt by the state to extort fees and create dependency on the government for the purpose of extrapolating wealth, not control. If the Minister of Telecommunication and Technology Rudiantara can

be taken at face value, the government fails to understand the technical aspects of ICT infrastructure and it is best left in the hand of the ICT professionals: "'The Internet [space] in this country is very dynamic – the Government will not pretend that we understand the technical details,' he said. For me, the best regulation is actually less regulation[52].'"

Contrary to the narrative above, John Savageau constructs his own optimistic assessment of how far the Indonesian Internet has come. He recounts that by 2010 Indonesian Internet had transformed itself from his experience in the country in the mid-1990s when he had worked for Sprint in Jakarta setting up X.25 networks[53] that used the Sprint-owned Internet backbone. Savageau exclaims that "Jakarta is wired," while ignoring the depth of the digital divide throughout the country and within the city as well. He claims that its competitive ISP market has enabled progress in infrastructure investment, like the Palapa Rings and the IXPs like the IIE.

Today, the issue of the increase in Internet access looms largest for those with stakes in Internet policy in Indonesia. What follows is a discussion about the limits of Internet penetration and attempts to rectify the disparities within the country and particularly how geography poses serious limitations to access Indonesia. This is coupled with divides perpetuated by SES and literacy.

Internet penetration. There are various figures for the number of citizens who have Internet access in Indonesia. The CIA and the ITU cite similar figures of 16.7 percent (2014) and 17.14 percent (2013) respectively, but the domestic ICT ministry, Kementerian Komunikasi Dan Informatika, or the Ministry of Communication and Informatics (MCI) sites 73 million users, making Internet penetration nearly 30 percent of the population (Freedom House 2015 414). At nearly double the institutionally reported statistics, the MCI's report is suspect.

Wired broadband, as in other cases, is becoming the less popular mode of access in favor of smartphones. While mobile phone penetration is 127 percent, only 21 percent of the population owns a smartphone (Freedom House 2015). As recommend by the ITU, the Indonesia Bureau of Statistics began collecting extensive data on Internet penetration in 2010. They report the number of households

[52] Such claims of ignorance calls to mind Machiavelli's exhortation "That on occasion it is wise to feign Folly (*Discourses on Livy*, Bk III, Chp II)."

[53] X.25 protocols, set up by the ITU-T, is a packet-switching network that commonly used throughout the 1980s and 90s that was eventually standardized into TCP/IP (Newton 1246).

with mobile phones has increased over a four-year period, from 72 percent in 2010 to 86.09 percent by 2013.

In March 2015, the *Wall Street Journal* reported a discrepancy in Internet access in Southeast Asia. A study revealed three clusters of Internet penetration in the region:

> Cluster 1 covers countries where more than 60% of the population has access to the Internet – Singapore (73%), Malaysia (67%) and Brunei (65%). In Cluster 2, Internet penetration is between 25% and 50% – Vietnam (44%), the Philippines (37%) and Thailand (29%); and Cluster 3 accounts for penetration rates below 25% – Indonesia (16%), Laos (13%), Cambodia (6%) and Myanmar (1%) (Larano)

Most indicators of access are correlated to GDP, except for Indonesia and Thailand. Jakarta was reported to have promised to use significant funds for infrastructure projects like the Palapa Ring projects and others to little avail. The study claims the continuance of the digital divide is a consequence of governmental malfeasance and interference in the private sphere. Yet it ignores some other independent variables. For instance, Malaysia and Brunei are comparatively much smaller than Indonesia, with concentrated rather than disperse populations. The reality of Indonesia's geography—an archipelago spanning some 6,000 inhabited islands—hampers efforts to expand access by both the public and private sectors.

Indonesian penetration rates vary greatly between urban and rural areas. Access in concentrated on the most populous islands like Jakarta and Sumatra. Freedom House reports that of 41 Internet backbones in the state, 60% are located in Jakarta alone, while less than 2% where located on Bali and Nusa Tenggara (415). The latter's populations are relatively small, having less than 10 million people in both provinces and also comprised of minorities, Hindus and Sasaks, which are traditionally underserved populations.

Freedom House claims that the gap is exacerbated by private Internet providers, particularly 3G providers. Base transceiver stations (BTS)[54] are concentrated on populated islands with extensive urban centers. "The highest concentration is in West Java, where there are nearly 10,000 stations, followed by Jakarta with 6,800. There are less than 1,000 3G BTS in Papua, Kalimantan, and the Mollucan Islands

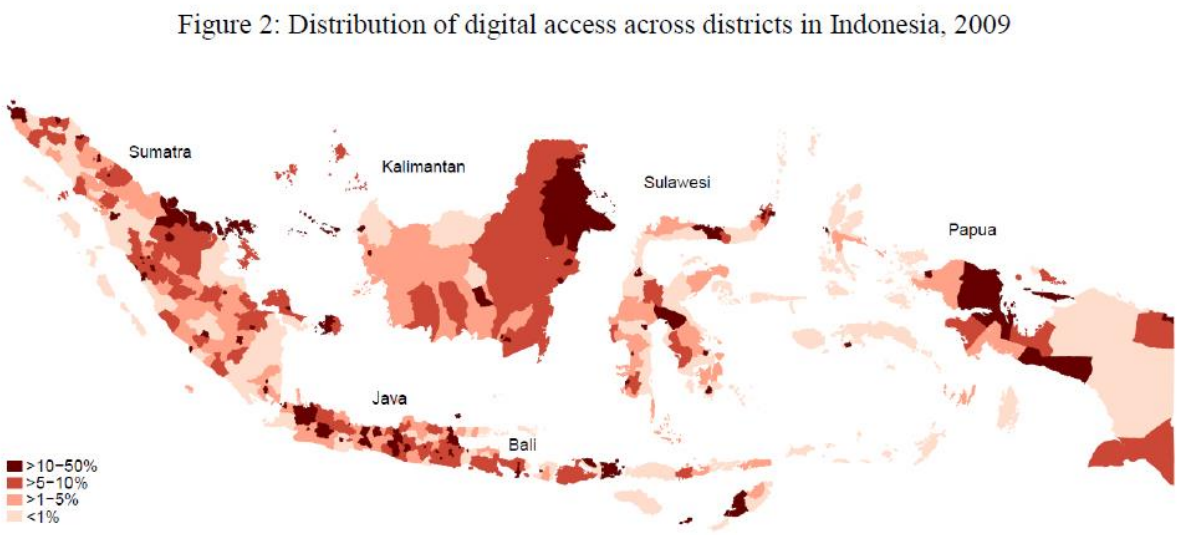
[54] "The electronic equipment housed in cabinets that together with antennas comprises a PCS facility or 'site' (Newton 173)."

combined (Freedom House 2015 415)." While total mobile penetration is 128 percent, less than 40 percent of Papua residents owned a cell phone compared to 97 percent of Jakarta residents.

In accordance with the recommendation of the ITU, the Bureau of Indonesian Statistics has been compiling extensive statistics on Internet penetration rates using different indicators province, age, use, etc. Despite the dangers of inflation from official ICT Indonesian statistics, there is a wide variance in Internet use in Indonesia according to province. Highest among these is Jakarta, reporting 63.4 percent in 2013 and the lowest being the province of Papua at a mere 11.0 percent. The average reported percentage for all of Indonesia was 32.2 percent.

This map, although dated, is correlated to socioeconomic status. Districts with important urban centers have greater amounts of access, and these disparities persist today.

Figure 2 Distribution of digital access across districts in Indonesia
(Sujarwoto and Tamubolo 8)



Sujarwoto and Tampublolo conclude that the diffusion thesis has far better explanatory power in Indonesia than the normalization thesis about the diffusion of Internet, and that the digital divides along socioeconomic status, gender, and education will persist unless there are adequate ICT strategies put in place. The authors see the government, rather than the private sector, taking on this role.

Other divides. Other forms of the digital divide are apparent in Indonesia. Freedom House (2015) reports that the Internet use has shifted from older, urban residents—who presumably had the money and a purpose for Internet—to younger demographics. Today, 70 percent of Internet users are under 35. Most people get to use the Internet as a result of ubiquitous cheap hardware in major cities.

There is a gender gap in Indonesia in terms of both access and use. The Indonesian Bureau of Statistics reports in 2013 that 55.67 percent of Internet users were male while only 44.33 percent were female, similar to levels one might find in China. Moreover, D'Urso reports that the way in which the Internet gets used by women is different than men as it is mainly used for social media and staying in touch with friends and family. "They are 25 percent less likely than men to use it for job hunting, and 52 percent less likely to express controversial views online." Gender equality is one of the SDGs and seeks to have women use technology in a more meaningful way, like economic independence and political participation.

Such opportunities are reported by Bold and Davidson (2012) that chronicle the use of extant SMS and 3G technology to enable micro-franchise. The technology is made available by Village Phone Operators, a micro-franchise in itself run by women who sell airtime, and commercially available mobile technologies. The results appear promising:

> As of January 2012, over 10,000 entrepreneurs have served more than 1 million unique customers. An estimated 47 percent of the entrepreneurs who stay in the portfolio for more than four months have moved above the poverty line, which the World Bank defines as US$2.50 per day. Currently, more than 83 percent of the businesses are owned by women and 100 percent are profitable (74).

These micro-enterprises are carried out in collaboration with NGOs, in this case the Grameen Foundation. This foundation became a darling in the international community because of their development of microfinance and its impact on developing countries. Geared towards women, microloans increase entrepreneurship and had low rates of default. The movement to integrate microfinance with cheap Internet makes sense but has to overcome issues of availability and literacy.

Average speeds in Indonesia are low compared to the rest of the region at 0.8 Mbps downstream in 2013 (Pribadi), or 1.7 Mbps (Chandra). Akamai claims that by Q4 2015, Indonesia's average speed was 3.9 Mbps, ranking the state 92nd in the world, but with admirable peaks speeds of 79.8 Mbps, marking a 495 percent increase from the previous year.

Table 13 Recorded Internet Speeds by Indonesian cities
(testmy.net 12 April 2016)

City (Province)	Downstream	Upstream
Pontianak (West Kalimantan)	10.1 Mbps	1.2 Mbps
Jakarta (Jakarta)	7.6 Mbps	8 Mbps
Bandung (West Java)	5.4 Mbps	4.1 Mbps
Surabaya (East Java)	3.8 Mbps	1.3 Mbps
Jambi (Sumatra)	1.4 Mbps	304 Kbps
Ambon (North Maluku)	790 Kbps	215 Kbps
Banjarbaru (South Kalimantan)	463 Kbps	118 Kbps
Parepare (South Sulawesi)	151 Kbps	53 Kbps

Jakarta, Bandung and other cities in Java had the best tested speeds. The farther from the economic and cultural hubs of Jakarta and Bandung, the poorer the Internet. Parepare, a city of moderate size (130,000) is located on Sulawesi and has the worst reported speeds at the equivalent of 0.15 Mbps. The city's economy is based primarily on agriculture and fishing and has little industry, and is made up of numerous ethnic minorities. Costs are relatively high in Indonesia as well. Numbeo records that a 10 Mbps wired connection would cost $26.37 per month, or 8.58 percent of a net monthly salary.

Palapa Ring Projects

> *As long as I have not united the archipelago, I will not enjoy the palapa [spice]. Until I conquer the island Desert Island Seram, Tanjongpura, Haru Island, Island Pahang, Dompo Island, Island of Bali, Sunda, Palembang, Tumasik, I will not taste the palapa.*
> Palapa Oath - Patih Gajah Mada

The Palapa oath, purportedly spoken by 14th century military leader, politician, and national hero of Indonesia, symbolizes the desire for unity among the inhabitants of the Indonesia archipelago. Invoked by early nationalists like Sukarno, it served an important role in shaping the identity of Indonesia in the early 20th century in the wake of colonialism and ethnic tension. It is fitting that the submarine cables meant to link major and minor cities in Indonesia would be named after this symbol in the hopes that such projects would lessen the digital divide that creates such disparities in access across Indonesia.

Eueung Mulyana, a professor at ITB recalled on his personal blog[55] in 2008 that the Palapa Ring project has deep roots going to Nusantara-21 (N21), a broadband network proposed by Jakarta in 1988

[55] This form of social media appears to be highly popular among Indonesians, and includes many academics and scholars.

inspired by similar Singaporean and Malay initiatives at the time. Despite the recognition of such needs nearly 30 years ago, the state failed to accomplish much. In an official statement from 2008, the Indonesian government claimed that "The combination of a much higher demand for telecommunication services, ICT applications and reduced costs due to the further development of technology has improved the financial feasibility" of carrying out the project. But the facile acceptance of the governmental statement may be unwarranted.

Divakar Gowami of LIRNEasia, a regional ICT think tank paints a less rosy picture. While Mulyana's recollections are accurate, the dream of national-scale infrastructure was to be fulfilled with government funds. When those funds dried up as a result of the 1997 Asian financial crisis, such large-scale projects floundered. It took until 2007 for the government to take up the project again, but this time pressured the private sector to front the cash. The consortium of the willing was initially made up of seven telecom operators including some state-run ISPs: Telekom Indosat, Excelcomindo, and Bakrie Telecom. The goal was to create a network of submarine cables that would connect 33 provinces across Indonesia, partially bypassing the market and directly addressing the problem of the diffusion of the Internet. By 2013, MCI reported that four of the seven original members of the consortium dropped out of the project because of the worldwide financial crisis. The three members remaining were Telkom, Indosat, and Bakrie Telecom, of which only the latter was privately owned. By 2015, Telekom makes the somewhat questionable claim that among the three remaining consortium members, only *it* has made the serious commitment to constructing the Indonesian Digital Network. Its press release pays homage to the norms of the F2C, saying infrastructure projects are "…expected to the have a positive impact for equitable access to broadband information and communication…" The press release also shows that such broad and expensive projects are profitable, seeing that the company will be able to make its Triple Play IndiHome package available in Eastern Indonesia, encouraging investors to be optimistic about future growth. However, to date, it appears that the entirety of the Palapa Ring submarine cables has not been completed, but progress has been made according to Telegeography's Submarine cable maps. All of these cables are owned by Indonesia Telekom.

Palapa Ring II was proposed by the Indonesian government in 2015. It would also operate as a consortium that would pool resources and funds to construct submarine cables to connect the existing

infrastructure to the eastern part of Indonesia. The government included a bidding process for this project and would select the option that promised to conduct the project at the lowest cost. Estimated costs are $222 million and it is hoped the project will be completed by 2018. Presumably, Papua would be served by these connections in addition to the SMPCS cable that Telekom is apparently in the stages of constructing.

The presence of submarine cables is a necessary but not a sufficient condition for broadband access. The presence of the submarine cables does not guarantee how the technology will be deployed by ISPs that will determine who eventually gets access or if users can afford connections or necessary hardware. The Digital Divide Institute was founded in 1999 to explore financial options to solve the problem of the digital divide. With various stakeholders—states, MNCs, local ISPs, and others, they work at bringing "ethics," rather than rights, to bridging the digital divide in Southeast Asia. They report in 2013 that in consultation with the World Bank, they adopted a "bottoms-up" approach within the nation's 500 "kabupaten" (local districts). The report that the Palapa Ring is "underutilized," and that despite its presence, it would necessitate outside intervention to make full use of the cables' potential. Despite Telekom's investment in these cables, without the market to sustain further investments in local infrastructure, the only ones who might benefit from their presence are the investors.

Internet Service Providers

The ISPs that serve Indonesia are indicative of the types of policies one can find about access. Citizen Lab reports on a law enacted in 1999, Law No. 36 on Telecommunications that changed the face of the sector in Indonesia. It simultaneously privatized or semi-privatized the industry, promoting competition and infrastructure development, and deregulating the telecommunications sector as a whole. These were undertaken as obligations under the WTO Agreement on Basic Telecommunications. As a result, there are about 300 ISPs that operate in Indonesia, but like other cases, several large important companies dominate. Three have the largest market shares of the mobile industry, Telkomsel (a subsidiary of Telecom Indonesia) with 60 percent of the market, Indosat (21 percent,) and Axiata (19 percent). Telkom and Indosat are semi-private entities with the state owning the majority shares. Axiata is a Malaysian company that seeks to serve underserved areas across Southeast Asia. (Freedom House 2015 415-416).

As mobile access makes up the vast majority of Internet use in the Indonesia, the semi-autonomous Telekom is the primary provider of the Internet for all of the state, despite attempts by the state to increase competition for efficiency's sake and to abide by the rules of the WTO. While the APJII has hundreds of members to date, these ISPs serve a fraction of Indonesia's population. For example, a random selection from the Association's website—BitsNet—offers an array of ICT services, including infrastructure construction and IT consulting alongside Internet service. But their service area is limited to two neighborhoods in Java. Five Mbps will cost a business—not a household—approximately IDR 1,500,000 or $110 per month. The company also appears to be peering with Telekom, thus the service is dependent upon the quasi-state owned infrastructure. Hundreds of these small providers may mean better customer service, but their dependency on extant infrastructure means that no better Internet speeds are in the realm of possibility in the foreseeable future.

Gou Eu reports on Indonesia's plan to change a licensing model for mobile operators in order to simplify the process of becoming a provider. Rudiantara, the minster of the MCI claimed that in the past the state prized providers who installed more infrastructure, but since then the emphasis has shifted to the prioritization of consumer experience. An unnamed analyst stated that "At the end of the day, the Government can only push as far as the telcos agree. It may not be as easy as it seems to push this through." Details of the plan were not revealed in the article, but the importance the government places on user experience rather than prioritizing ISPs in an important signal for the F2C.

While the state is attempting to implement policies that remove some of the red tape that must be overcome by new ISPs, both the state and the APJII are part of the Indonesian culture of patrimony. Licensing fees collected by the state and membership dues to the Association ensure that private ISP startups are already burdened with the task of paying these institutions their due. This translates to limited innovation and the poor performance of ISPs, especially outside of Jakarta and Sumatra. However, policies are in place in attempt to rectify this.

State Policy Regarding Internet Penetration and Use

Internet freedom and F2C entrepreneurs have a direct impact on state policy on Internet penetration. Dr. Illham A. Habibie along with Craig Smith founded a chapter of the Digital Divide Institute

(DDI-I) in Indonesia. "[Warren and Habibie's] collaboration resulted in the aggregation of Indonesian ICT stakeholders in support of broadband development."

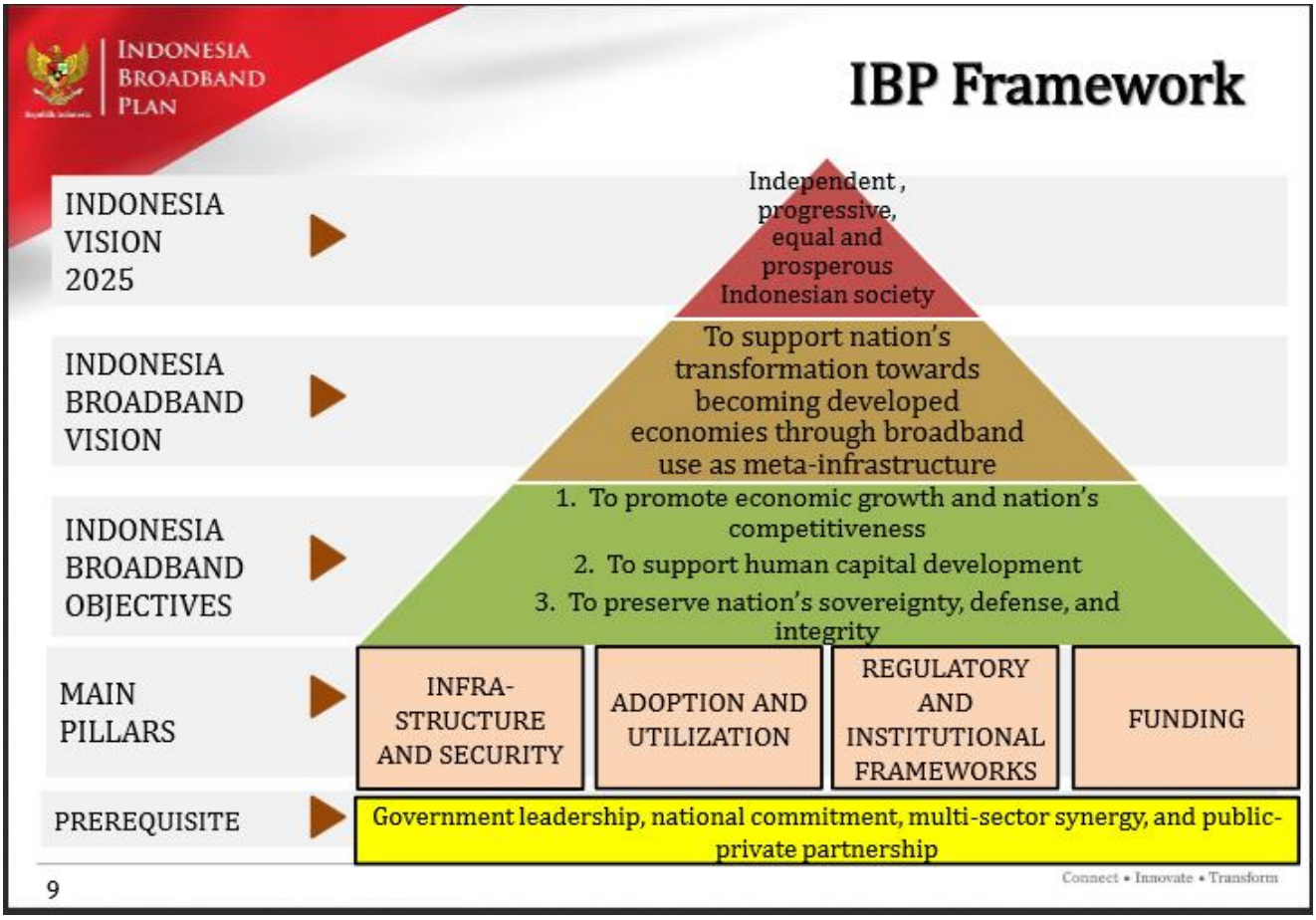
This resulted in the "Jakarta Declaration on Meaningful Broadband," which was adopted by Habibie, local NGOs, the Chamber of Commerce, and the director of the MCI. The declaration is framed within the Masterplan for Acceleration and Expansion of Indonesia's Economic Development through the Meaningful Broadband Indonesia (MBI) group, which seeks to bring Indonesia's economy to greater levels of growth and competitiveness. Inherent in this vision is the need for sophisticated Internet access which requires a "big push" of broadband deployment services guided by holistic policy. To achieve this, the plan lays out five policies:

- New Wireless Network Technologies which, for the first time, could bring provide an affordable "last mile" broadband solution, to middle-to-low-income citizens and enterprises currently excluded from Indonesia's growth economy.
- Cell phone upgrades: local manufacturing industry capable of developing mobile phones, tablets, and mobile internet devices at price points suitable to lower income citizens, able to provide access to broadband;
- Completion of Backbone Infrastructure: the impending completion of the massive fibre optic infrastructure -- a vital national asset with capacity to support increased broadband demand,
- Public Private Partnership: Plans are underway for a subsidized broadband network which could induce market forces to serve and empower millions of users whose income lies below the threshold of commercial markets.
- Broadband as "Meta-Infrastructure": International models that show how broadband could be a "meta-infrastructure" – driving, boosting, integrating and enhancing social impacts of all other infrastructures.

The push for bridging the gaps among the poor and isolated citizens and PPPs loudly rings of the F2C norm as envisioned by WSIS. The MBI held a consortium in late 2015 about the process of "leapfrogging" broadband among the 500+ government units in Indonesia to bring broadband to 25 million people.

In recognition of the numerous challenges facing Indonesia to increase Internet penetration, broadband, and meaningful access, the state developed another and more extensive policy guideline, the Indonesian Broadband Plan in 2013. The presenter Lukita Tuwo, Vice Minister of National Development Planning invokes the MDGs as a backdrop for the need for meaningful broadband and the challenges including unequal penetration rates and the burdensome tariffs places on ISPs. Parroting the ITU's WSIS vision, he states: "It becomes mandatory for the Government together with private sectors to unlock the potential of broadband."

Figure 3 Framework of the Indonesia Broadband Plan
(Tuwo 2013)



Unlike the Russian and Chinese visions about the expansion of broadband and Internet access in their countries, Indonesian ministry officials like Tuwo invoke some of the language and framing from the F2C norm entrepreneurs like the WSIS's outcome document recommendations and individuals like Craig Warren of the Digital Divide Institute. These recommendations are specific to Indonesia's economic context, such as problems with burdensome regulations and the desire to find a balance between private companies' work alongside government intervention. Eu reports on targets that the Broadband Plan, along with the "Master Plan" for Indonesian growth:

Table 14 Indonesia Broadband Plan Targets for 2019
(Eu)

	Target achievement
Household penetration rate of fixed broadband in urban areas	71% at 20 Mbps
Buildings connected to fixed broadband in urban areas	100% at 1 Gbps
Penetration rate of mobile broadband in urban areas	100% at 1 Mbps
Households connected to the fixed broadband in rural area	10% at 20 Mbps
Penetration rate of fixed broadband in rural area	6%
Penetration rate of mobile broadband in rural areas	52% at 1 Mbps

While there is sufficient evidence that the F2C influences policy-making and its norm entrepreneurs that operate in Indonesia, there is also some evidence of Internet policies being pulled in other, more techno-nationalist and cyber-sovereignty directions. Kontan (2015) reports that the government is incentivizing the use of domestic domain names by promising to invest 50 billion Rd, or $3.7 million, for the creation of one million domestic domains. The purpose is to reduce the amount of traffic that goes overseas, which is approximately 80 percent of total Internet use. The motivation for this development was not explicitly stated in the article. It is not likely that it is the result of a desire to control content, but instead to heighten domestic prestige and encourage domestic consumption.

There are some more concerning developments that straddle the problems of access and content. It is well-documented that Indonesia tries to limit content like "…radicalism, hate speech, fraud, gambling, child violence & pornography, internet security, intellectual property rights, violence and miscellaneous (Freedom House 2015 418)." Yet, the filtering or blocking of sources of political critique or dissent is mostly absent. An anecdote reported by *Ars Technica* presented a bemused American perspective on a poorly executed example of site blocking by an Indonesian ISP. Moratel had attempted to block Google's services in Indonesia (no reason was given), but due to a technical glitch, managed to redirect all searches for Google to a fake route. Because Moratel was connected through Singapore and Hong Kong, the incorrect configuration change had a ripple effect on the rest of the web. "The error was possible because most routing of traffic on the Internet is dependent on trust between network providers. When networks set up "peering" relationships, they agree to trust each other's' routing advertisements and to propagate them (Gallagher)." Because Indonesia's Internet infrastructure is not domestic, but

depends on transnational connections, such mistakes are possible and reveal that Indonesia is far away from controlling more extensive content.

Citizen Lab reported on the potential dangers of the Palapa Ring project. In particular, Snowden's disclosures revealed the British Government Communications Headquarters (equivalent the US's NSA), had been using a cable that Telekom partly owns, SeaMeWe-3, to spy on data in the UK and Northern Europe. While not immediately relevant to the question of the F2C in Indonesia, complicity—or ignorance—of these programs may signal future troubles for Indonesian Internet users upon the completion of the Palapa Ring projects. The possibility of the Indonesian state collecting metadata on its citizens does not seem out of the realm of possibility, especially in the light of Free states undertaking similar projects in the name of national security.

Domestic Attitudes towards Access and Policy

The global surveys reviewed in this study dating back to 2008 all address the opinions of Indonesians, even if Indonesians themselves do not appear to regularly conduct such studies on their own. Kull et al. (2008) reveal that the majority of respondents, 56 percent, saw political stability as a justification for the restriction of access, but 73 percent argued that the news should be able to publish want it wants without government control and that 65 percent thought they should be able to read whatever they want on the Internet.

As was the case in the Philippines, GlobeScan's 2010 survey revealed that 46 percent of the respondents felt that social connections were the most important value of the Internet. At the time, 51 percent argued that government should never restrict content, and 67 percent saw Internet as a fundamental right. Internet Society's 2012 survey revealed that Indonesians saw the need for the government to step in to helping to assure access, with 96 percent arguing that the government should find a way to provide cheaper computers, 93 percent arguing that it should encourage competition among providers, and 94 percent arguing that the government should ensure access to its citizens. Such statistics are remarkably similar to the Philippines. Ninety percent argued in 2012 that the Internet should be considered a human right, 88 percent argued that expression should be protected on the Web, and 91 percent argued that social media enhanced rights to assembly and association. Fifty-seven percent would accept increased controls or monitoring if it meant enhanced security, and a vast majority, 91

percent, said the government had the right to govern the Internet according to the way it sees fit. Pew reports that the percentage of those that argue that Internet should not be censored is relatively low, 55 percent in 2014 and 53 percent in the 2015 survey[56].

***

It is not altogether clear what to make of the survey data that simultaneously demonstrates a desire for stronger state control but also for Internet freedom. It could be a consequence of the same phenomenon reported by the 2011 WEF in that "users want it all." People do not see access and control as contradictory demands and most Indonesians feel strongly about the centrality of access and the state's role in the provision of that technology. There is evidence in Indonesia that the state, despite stops and starts, has adopted the principles of the F2C in their pursuit of regulating the ISP market and the construction of the Palapa Ring projects. In so doing, they are addressing the issues related to physical infrastructure and meaningful access.

[56] Pew 2014b and 2015b.

Chapter 6: Not Free Cases

The states contained with Freedom House's final category are remarkably different from each other in terms of size, political culture, Internet use, and capabilities. Despite these differences, each state's regime-type is some version of authoritarianism, and as such governments are highly concerned with maintaining order and security above the promotion of rights and equality.

China

> *The party has achieved something few had thought possible: the construction of a distinct national internet. The Chinese internet resembles a fenced-off playground with paternalistic guards.*
> –The Economist*, April 2013*

As with the US and Russia, China is among the largest and most powerful states in the international system which makes it appropriate for the final choice as the archetype case for those in the Not Free category. It has achieved notoriety among IR and comparative scholars due to its extensive capacity to surveil its users and filter content and in doing so has violated the spirit of liberal human rights. Yet like other states, China faces uneven geographic distribution of the Internet and use is concentrated among urban, middle-class youth. Efforts to bridge the digital divide in China are done in the hopes of bringing economic prosperity while maintaining social harmony have been overlooked in favor of the steps it takes to control its users. The Chinese government has taken a variety of steps to increase Internet penetration and all the while has managed to maintain its firm control.

As reported by the CIA's World Factbook, China has a population of approximately 1.37 billion (ranking 1st in the world) and a land mass that spans 9.6 million km^2 (4th in the world). Fifty-six percent of its population lives in an urban area, lower than the other two archetype cases, with 6 major metropolises each with a population of 10 million or more[57], with Shanghai as the largest city-proper in the world. It has the largest economy in the world with a GDP of $19.51 trillion. This equates to $14,300 GDP per capita, ranking China 112th in the world; much of the rural population suffers from underdevelopment.

China has 249.4 million landlines, ranking first in the world. The figure escalates for cellular phones, with 1.3 billion in the country, placing it again as first in the world. In total, there are 667.69

[57] Shanghai 23.741 million; BEIJING (capital) 20.384 million; Chongqing 13.332 million; Guangdong 12.458 million; Tianjin 11.21 million; Shenzhen 10.749 million (2015)

million Internet users in China which ranks the state first in the world, but totals only 48.8 percent of the population (China Internet Watch).

Its history with human rights is antagonistic. While the state is party to six human rights instruments and a signatory to the ICCPR, it derogates from those rights in the name of order and social harmony. Throughout the 19th century, China was indirectly controlled by the West but was never a colony, and as a result it is both distrustful of the West and its elites did not absorb a liberal tradition in the way India and African countries had done. In a telling bit of history, nationalist Chinese scholar John C. H. Wu attempted to synthesize the liberal tradition with Chinese political culture into a national constitution. The rights enumerated in the proposed constitution included rights to property, speech, religion, association/assembly, residency, privacy of correspondence, to vote, to call for referendum, to recall politicians, to petition government, and *habeas corpus*. Yet these rights were highly circumscribed by other elements of the Chinese Nationalist Constitution, which allowed the legislature or the executive to abridge or revoke these rights when it was deemed necessary. Wu summarizes the new relationship between rights and duties in the document he drafted:

> ... Rights are entrusted to the individual by society; the society is the fountain which produces rights. It can be said that if an individual leaves society he is without rights. Since society can confer rights in times of necessity, can also strip away rights; at least it can limit the scope of rights. Therefore, *minquan zhuyi* advocates that all rights are relative; they are decidedly not absolute (Grieff 461).

The Western tradition argues that rights are given either by natural law (social contract), or through rational consensus (Kant), both of which are meant to protect citizens from arbitrary government action. Within a Chinese framework, these liberal values are made subservient to the state because rights stemmed from society in the first place. The failure to separate individual rights from the state and society continues today.

China is widely cited as a violator of human rights and especially those associated with the F2C and Internet freedom: expression, assembly, association, and press. In its Universal Periodic Review, China has one of the few dialogues with the UN regarding its practices on the web and its connections to its human rights obligations. It proclaims it continued to invest in information facilities and the growing number of Internet users among its citizens, a common boast for China in order to claim that it is technologically progressive. It maintains that at many stages of the law and policy-making processes the

public is encouraged to consult with national and local lawmakers. The public's views are solicited during the drafting process but it is unclear whether such views have direct impact on the policy-making process and hence could be considered crowdsourcing. The only recognition to the limitations on content or other violations of users rights comes in the form of the admittance that it has taken measures to "strengthen the management" of the Web. Content that incites violence, pornographic content harmful to children, and Internet fraud are all areas in which the state admits to "cracking down," with no admission that it does so to encourage social harmony and unity. Instead, these actions are framed as necessary exceptions to an otherwise free Web.

The Internet in China

Background. Most official accounts of China's first venture on the Web focus on an email heard around the world—"Across the Great Wall we can reach every corner in the world"—sent in September 1987. Its source is a joint team of Chinese and German academics in Beijing's Institute of Computer Applications in communication with the University of Karlsruhe in Germany. Other reports state that another academic partnership led to the first connection of the Internet in China was in fact a year earlier. In August 1986, Wu Weimin from the Institute of High Energy Physics of Chinese Academy of Sciences in Beijing remotely logged into the account of Wang Shuqin on a machine located in CERN of Geneva via the satellite link, and sent an email (CNNIC 2012). Despite the debate, as with almost all other cases in this study, it was academia that took charge of the introduction and later the spread of the Internet.

In subsequent years, Chinese academics worked to build the infrastructure that spread access throughout the country's universities. They developed the X.25 protocol to enable email communications between academics in China and their counterparts in Germany, which meant access to the World Wide Web was not yet possible. In 1989 after a loan from the World Bank, the National Computing and Networking Facility of China was created to develop China's Internet backbone and other necessary infrastructure. In 1990 they gained the top-level domain of .cn, thus creating a Chinese intranet. Connecting it to the greater Internet was the next hurdle, but was not without its barriers.

> At the INET'92 annual conference [Internet Society, an NGO; see Frames Chapter] held in Kobe, Japan in June 1992, Researcher Qian Hualin from Chinese Academy of Sciences met with the person in charge of International Network Department of National Science Foundation of the U.S., and for the first time officially discussed the issue of China's access to the Internet. However, he was told that there was political barrier for

> China's access to the Internet because there were many American government organs online (CNNIC 2012)

Tsinghua University adopted the first network that used TCP/IP in December 1992, but it took until April 1994 for China's "Golden Bridge Project" to successfully connect China to the World Wide Web. It had taken several years for the Internet backbone, servers, and other infrastructure to be completed. The development of this infrastructure was assisted by Sprint through a special 64 Kbps connection (a state-of-the-art speed at the time). Little information is available that details the deal between the Ministry of Posts and Telecommunications (MPT) and Sprint; *Reuters* published a brief on the project, stating nothing other than the "Financial terms of the memorandum of understanding were not disclosed." Until 1995, the Internet was relegated to universities and academic centers in China's major cities of Beijing, Shanghai, Guangzhou, Nanjing, and Xi'an. Public access was enabled through the national X.25 protocols in January 1995. CHINANET was the nationwide backbone that was put into service by January 1996, and the bureaucracy that surrounds Internet penetration and usage today began to emerge.

By 2000, Goldkorn reports that anonymity on the Internet became a norm in China as it had been across the Web before the rise of social media. Yet as these practices became widespread, they did not remain unnoticed by the authoritarian government. Goldkorn states "The government uses increasingly sophisticated technologies to block and filter certain foreign websites, and starts regulating Chinese websites more strictly as Internet use grow." One famous incident was the arrest of journalist Jiang Lijun in 2003 with the assistance of Yahoo. "On Nov. 18, 2003, Lijun was found guilty of 'subversion' and ordered to serve four years in prison for allegedly planning to use 'violent means' to push democracy (CIO)." Yahoo had provided the government with the information that traced his email account back to him. The push against anonymity is discussed by La Rue (2013), who argues that it is fundamental to the security of citizens on the web because it protects their privacy and freedom of expression. China's moves against anonymity discussed below are inimical to this sentiment.

Becky P.Y. Yoo explores the dynamics of Internet development in her 1994 article "Telecommunications reforms in China," developing an analytical framework of the forces at work. She claims that at different stages, there were three forces that shaped the Internet's development in China which are presumably in place today:

> (1) government concerns (including the state's desire to provide universal coverage, to control the telecommunications industry and, more recently, to improve the efficiency of state-owned enterprises)
> (2) the call from foreigners (sometimes made through their governments) to open China's telecommunications industry and
> (3) the overwhelming market demand of the Chinese population and the business sector (including foreign firms operating in China) to have freer and more rapid movement of information (especially on the Internet). (698)

Early stages meant a large amount of state direction and control. China desired inclusion in the WTO, and faced pressure to reform state-controlled industries between 1994 and 1997, and by 1998-1999 domestic competition was being encouraged simultaneously by state policy and market forces. "There were repeated calls from respondents of CNNIC surveys for lower charges, better services and more choice (Yoo 706)." By 2000, she reports that the state took on a number of significant roles, including balancing three problems: encouraging domestic competition, dealing with the inefficiencies of state-run enterprises, and dealing with threats that would alter the state's ability to control the Internet. The state developed a series of licensing laws to counteract political and pornographic content, and owners of Internet cafés would be required to monitor and report their customers' illegal activities. Use of public venues for Internet access has declined today, but the latter regulation is emblematic of authoritarian and semi-authoritarian governments in general. Middlemen, like Internet cafés and ISPs, are put in the service of the state to police their users or face the loss of their businesses.

China faces the dichotomous challenge of growing Internet penetration for use among its *wangmin*, or netizens, to enable growth in the global economy while simultaneously monitoring this access to assure stability and order. It is not an easy challenge, and some saw these as incompatible goals whose pursuit would ultimately weaken the regime (see Taub 1998). Instead, the state has earned a reputation for being adept at this balancing act by enlisting domestic and foreign ICTs to help expand and monitor the web simultaneously. The possibility of voices that challenge the state using the Internet is inherently difficult as the infrastructure is controlled by the state. As Herold and *The Economist* report, Beijing controls the gateways to the greater World Wide Web. "…the Chinese government owns and controls the access routes to the Internet, and only allows private enterprises and individuals the rental of bandwidth from state-owned entities (Herold 2)." This built-in limited access to private ISPs means that few alternatives to the state-owned Internet are available to users.

Freedom House (2014) reports the state's desire to control the medium is growing; "The Internet has become the main battlefield for public opinion struggle," (General Secretary Xi Jinping) said in the speech, which provided the ideological underpinning for the internet freedom decline." There was controversy over the August 2013 speech by the Communist Party official, but from some commentators noted that it harkened back to the party's darker days:

> This editorial implied that there were some who were avoiding the "public opinion struggle," but after the editorial came out there was a rebuttal from Cao Lin in the August 27 edition of *China Youth Daily*. Cao's piece was headlined: "The Term 'Public Opinion Struggle' Makes People Uneasy" "Using the term 'public opinion struggle' to characterize the current ideological conflict ushers us back into the past," Cao wrote, referencing China's tumultuous Cultural Revolution (Gang).

Gang argues that the party was no longer seeking only to manipulate public opinion as it had done in traditional media, but also make sure the party's voice was front and center. "'Public opinion channeling' focused on the need not just to control, but also to grasp discourse power. It wasn't enough to muzzle the voices of others — the Party's voice had to be heard and accepted as well (Gang)."

Despite the Internet's birth in China as an academic venture whose purpose was the development of science and technology, its spread is characterized by the intense interest of the Chinese state. Though developed in partnership with private sector MNCs, it was the design of the Chinese state from the outset to develop the Internet's infrastructure in ways that would allow it to control access and content as soon as the tool stretched beyond universities.

Internet penetration and digital divides. A whitepaper by China Internet Watch (CIW) provides statistics on Internet penetration since June 2015, and regularly reports on these in six month increments (2015a). It is part of a private Singapore-based firm Incitez Pte, Ltd. whose purpose is provide data for "digital strategy consulting and digital development." It is curious if not uncommon phenomenon that the private sector is driven to provide up-to-date data for infrastructure development that is pertinent for both the private and public sectors[58]. The China Internet Network Information Center (CNNIC) is the government agency of the Ministry of Information Industry that deals with the Internet. Its annual reports also provide such information, but the former was chosen for being the most current.

[58] The ICT sector is not alone in this phenomenon. The International Maritime Bureau, for example, is a privately run institution from the International Chamber of Commerce which provides the most accurate and up-to-date statistics on maritime piracy, primarily for those who own ships or pilot them.

CIW reviews changes over a four-year period, from June 2011 to June 2015. Total Internet usage in China rose by 12.6 percent to 667.69 million users. This means that 48.7 percent of the Chinese population was online in 2015, below both the US and Russia. As elsewhere in East Asia, Internet usage is highly skewed towards mobile technologies; 88.9 percent of users used smart phones to access the web in 2015 which represents more than a 20 percent jump from four years prior. These percentages are in themselves evidence of the poor performance of Chinese Internet access; the large state, while growing rapidly, scores such a low score on Freedom House's scale because less than half of their population is connected. 3G technology that enables mobile access in major Chinese metropolises is no longer the state-of-the-art today, and in part this is a consequence of techno-nationalism discussed below.

The digital divide manifests itself within these statistics shown in areas like urban rates, age, and socioeconomic status. The urban-rural divide, which affects much of China's development, is pronounce in ICTs and Internet usage. There was little change between 2011 and 2015: 72.5 percent of Internet users lived in cities in 2011, and 72.1 percent by 2015 (recall that the entire urban population is 55.6 percent). Age is another good predictor of Internet use. For the young, ages 10-29, urban use of the Internet 85 percent while rural use is 69 percent. For the elderly, the gap is the most extreme; in cities, 13.3 percent use the Internet while in the countryside a mere 2.5 percent use the web. Education is a predictor as well, with only 12.4 percent of users of having primary education or less having Internet access; such numbers are partly a reflection of literacy. Socioeconomic status, which at least in the US is highly correlated to education level, is also a predictor of Internet access, with middle-income earners making up the majority of Internet users.

The question of where netizens access the Internet is covered by the CIW survey. Ninety percent of users can access the Internet at home, comparable to levels found in the US. Thirty-four percent access at work, 18.6 percent at cybercafés, while 14 percent get access through school and 18 percent through other public means.

CIW (2015b) (2015c) reports on smartphone trends, which are also on the rise in China. As elsewhere, mobile phone usage is common among young people and those who have no other means of access. They report by the third quarter of 2015, there were 1.25 billion active smartphone users in

China (smartphones are therefore the majority of all mobile phones); a number that is rising, albeit more slowly now than in recent years. People 25 and under account for 36.6 percent of the total. Nearly 530 million people have smartphones in China or a penetration rate of 38.6 percent. In cities with the most sophisticated infrastructure, penetration among ages 16-59 is a whopping 94 percent, while in rural areas it is 32 percent.

Internet penetration rates within Chinese provinces are unavailable, but Freedom House reports that while access has been expanding for years, it is now slowing. Urban markets are reaching near-saturation levels; most people who can afford access to the Internet either through broadband or mobile technologies already do so.

Like the CIW, the CNNIC publishes regular statistics on Internet penetration. The report acknowledges that there is a considerable gap between urban and rural populations. While the authors are pleased to report that gaps within provinces have improved since 1997, the gaps between mainly urban and rural provinces remains substantial. Beijing and Shanghai each have usage rates above 70 percent, while ten provinces have rates below 40 percent. "…unbalanced economic development among regions was the root cause [of the penetration gap]. How to narrow such a digital gap needs further research and exploration (2)." Bildner reports in 2013 that Jiangxi's Internet penetration was actually less than 30 percent, so while overall penetration continues to grow in China, inequality remains a significant problem. Why this divides persists is a more pertinent question. Both of the other archetype cases face similar problems of how some regions, especially rural or indigenous are under connected or disconnected from the Internet. Guizhou and Jiangxi are both rural, landlocked, and dominated by agriculture, but the former especially is characterized as having significant ethnic minority populations. Political ideology that emphasizes the centrality of Beijing and ethnic Han Chinese may be one of the roots of this gap.

Another piece of the puzzle is economic. Bildner reports that ICT infrastructure development is tied to a province's main economic base. The impetus to rapidly improve ICTs is absent in Guizhou and Jiangxi because their economies are primarily agricultural. By contrast, while Inner Mongolia has a relatively sparse population, its relatively higher rate of Internet penetration is due to its richness in coal and rare metals. Unlike Russia and the US, China does not make rhetorical pronouncements that

Internet access is important for all of its citizens. While it does acknowledge the importance access to government services and the promotion of e-commerce, this rhetoric remains centered on urban populations with the means to make use of them. There is little acknowledgment of a rights-based approach to the Internet for those who have little meaningful access. The narrative is couched in economic necessity and global competitiveness, and even the rudimentary courtesies that Russia pays to how the Internet enables human rights are absent. As a result, Bildern suggests that there are two Chinas, the Connected China where the relatively wealthy have potential access to outside information, and the Disconnected China that more fully resembles the state-controlled media of decades past. The latter suffer more acutely from the paltry availability of information not directly provided by the state.

Speed and cost. Speed is limited in China. Freedom House reports the average download speeds in China are 3.2 Mbps, while Akamai reports 4.1 Mbps in Q4 2015, an increase of 20 percent from the previous year. For comparison's sake, the following are what testmy.net reports for some major and minor cities in China:

Table 15 Reported Internet speeds in Chinese cities
(testmy.net 12 April 2016)

City (Province)	Download	Upload
Beijing (Beijing)	7 Mbps	2 Mbps
Shanghai (Shanghai)	6.7 Mbps	3.9 Kbps
Guangzhou (Guangdong)	4.9 Mbps	1.6 Mbps
Chongqing (Sichaun)	4.6 Mbps	1.1 Mbps
Guiyang (Guizhou)	3.9 Mbps	1.3 Mbps
Nanchang (Jiangxi)	3.7 Mbps	1.9 Mbps
No city available (Xinjiang Uyghur Autonomous Region)	2.5 Mbps	601 Kbps
Xi'an (Shaanxi)	2.2 Mbps	493 Kbps
Hothot (Inner Mongolia) (few results)	1.1 Mbps	N/A

At such speeds that the average citizen in Beijing, for example, falls far below developed countries' standards for Internet access. Recall that the FCC now requires 25/3 Mbps as a minimum criterion for broadband since 2015. Figures for Guiyang and Nanchang, cities that fall into the underserved provinces discussed above, are lower than the central cities that lie within the outer provinces in China. Inner Mongolia and the Uyghur Autonomous region experience the worst speeds observed.

Costs are relatively expensive, with 1 Mbps wired broadband on average costing 469 times more on mainland China as compared to Hong Kong (Freedom House 2014 195). Yet in Beijing, China Unicom's 10010 monthly 4G mobile service package costs a user ¥50, or about $7.88 per month. Such prices are in line one might find in Moscow and is a relative bargain compared to American counterparts. Numbeo records that a 10 Mbps fixed connection would cost $17.37, high for Asia, but still only 1.83 percent of the average citizen's salary.

Internet Service Providers

Internet service in China is provided exclusively by the state in one of two manners. First, "private" ISPs that serve businesses with telecommunications service must rent bandwidth from state-owned infrastructure like IXPs. Such arrangements are not uncommon—most American ISPs likewise share infrastructure by utilizing peering—but the infrastructure is privately-owned by large corporations. Second, the three largest ISPs in China, the China United Network Communications Group Co., Ltd. (China Unicom), the China Telecom Corporation Limited (China Telecom), and the China Mobile Communications Corporation (China Mobile), are all state-owned enterprises.

The viability of these ISPs is manipulated by the state. A virtual monopoly by China Telecom was challenged in a 2008 anti-trust suit[59], and the rearrangement of the entire telecommunications industry was the result. Since 2008, these three providers of broadband and/or mobile Internet service have been orchestrated to compete against one another to increase innovation and efficiency. While provincial branches of these ISPs operate semi-autonomously, they are still engines of the state and are responsible for carrying out state policy about availability, regulation, and censorship.

Despite the encouragement of domestic competition the domination of these ISPs stems from techno-nationalism. Hong, Bar, and An (2012) review the development of ICT industries in China and how the country is attempting to reverse a long-standing trend of foreign-direct investment that enabled the development of Chinese ICT infrastructure. Three decades of dependency upon this model of growth for this sector meant that China was reliant on foreign-developed technology to modernize their economy,

[59] The Tenth People's Congress passed in 2007 and began enforcing in 2008 vast anti-trust legislation throughout various sectors of its economy. The purpose as stated in Article 1 is as follows: "In order to prevent and combat monopolistic behavior, to protect fair market competition, improve economic efficiency, to safeguard consumer interests and public interests, and promote the healthy development of the socialist market economy, the development of this Law (NPC)."

and simultaneously meant that there was little technological accumulation and innovation. "There has been an outburst of techno-nationalist discourse," the authors note, "expressing the shared concept of 'Chinese national, as opposed to foreign, control' over rapidly changing information network infrastructure (914)."

Such concerns over the foreign origin and control of technology are common. Recall that the *Guardian* reported Russian policy of looking into ways to "unplug" the Internet, which has since been tested in 2015 and justified as a response to the perceived threat of American control of the Web. Such a sentiment was echoed after another "email heard around the world." Morozov reports on an incident that took place during Iran's Green Revolution that involved an email from a member of the US State Department to Twitter executives to postpone scheduled maintenance. The maintenance would have interrupted the ability of the protestors to stay connected, and the official published the email in solidarity with the pro-democracy advocates in the country. On the other hand, Iranian officials—and the Chinese—saw the email as evidence of American meddling in domestic affairs utilizing the medium they indirectly control, and soon cracked down on social media users in their own countries.

Accordingly, China has formed its own standards for mobile technologies. TD-SCDMA air interface[60] is a 3G technology that is designed for exclusive use in China (Hong, Bar, and An 915). As mobile ISP providers are required to get licensed in order to be able to provide services, Chinese mobile netizens are forced to use state-developed technologies incompatible with the rest of the world's standards. Simultaneously, this new standard has been marketed abroad to encourage innovation and profit-motivations for all three of China's top ISPs. "As Ji Zhengkun, Director of the Standardization Administration, pointed out, technical standard-setting constitutes a key national strategy (Hong, Bar, and An 919)." By establishing national proprietary standards—and ones they could sell to markets overseas—China's ICT development policy attempted to consolidate control on the most commonly used device for Internet access and attempted to provide an alternative to the Western-originated standards like GSM and CDMA.

[60] "Air interface is a cellular industry term. It refers to the system that ensures compatibility between equipment (cell phones) and the base stations (Newton 113)." Essentially, it the particular type of technology which allow cell phones to access the Internet and other types of data.

Continuing along the lines of attempting to bring efficiency, innovation, and state control in line, Hart discusses developments in China's mobile technology markets in 2013. First, all three major ISPs were awarded licenses to sell 4G service[61]. The prices of broadband reflected above from China Unicom are monthly 4G plans. Such technology is the next step in a country that is largely reliant on wireless technology for access. Hart remarks that similar to 3G technologies, China is licensing this home-grown, proprietary technology before the internationally-licensed competition: the Frequency Division Duplex-LTE (FDD-LTE). Additionally, China Mobile is trying to encourage domestic consumption (and presumably foreign sales) by pushing for phones that would cost less than 1,000¥ ($158). Finally, a new element of competition was being introduced in 2013, Mobile Virtual Network Operators (MVNOs) which enter into agreements with established mobile or ICT companies to buy network services wholesale and subsequently sell plans to consumers[62]. Hart and Xiang report that by the end of 2013, eleven different companies received licenses to provide these services, some of which are mobile phone distributers, but others that are Internet infrastructure and/or solution providers and retailers. Xiang points out that "Five of them will work with both China Unicom and China Telecom," and doubtless the rest will work with one of the main ISPs or telecom companies. While China is trying to encourage domestic competition to enliven innovation and efficiency (something which Hong, Bar, and An report has had mixed success in past), all licensees are dependent on state-controlled infrastructure in addition to the direct requirements of the government to control content and limit users' rights.

Internet gateways (IXPs) are directly controlled by the state. "Despite these signs of liberalization," the Freedom House report notes, "six state-run operators maintain China's gateways to the international internet, giving authorities the ability to cut off cross-border information requests. All service providers must subscribe via the gateway operators under MIIT oversight (Freedom House 2014 196)." Thus, a cut-off from the rest of the world—for a legitimate Chinese intranet—is a real possibility. The scenario would endanger China's economy which is dependent on foreign trade, so its likelihood increases only with the rising threat to Chinese national security.

[61] Time-Division Long-Term Evolution [TD-LTE]
[62] Examples in the US include Boost Mobile (Sprint) and Consumer Cellular (AT&T, T-Mobile).

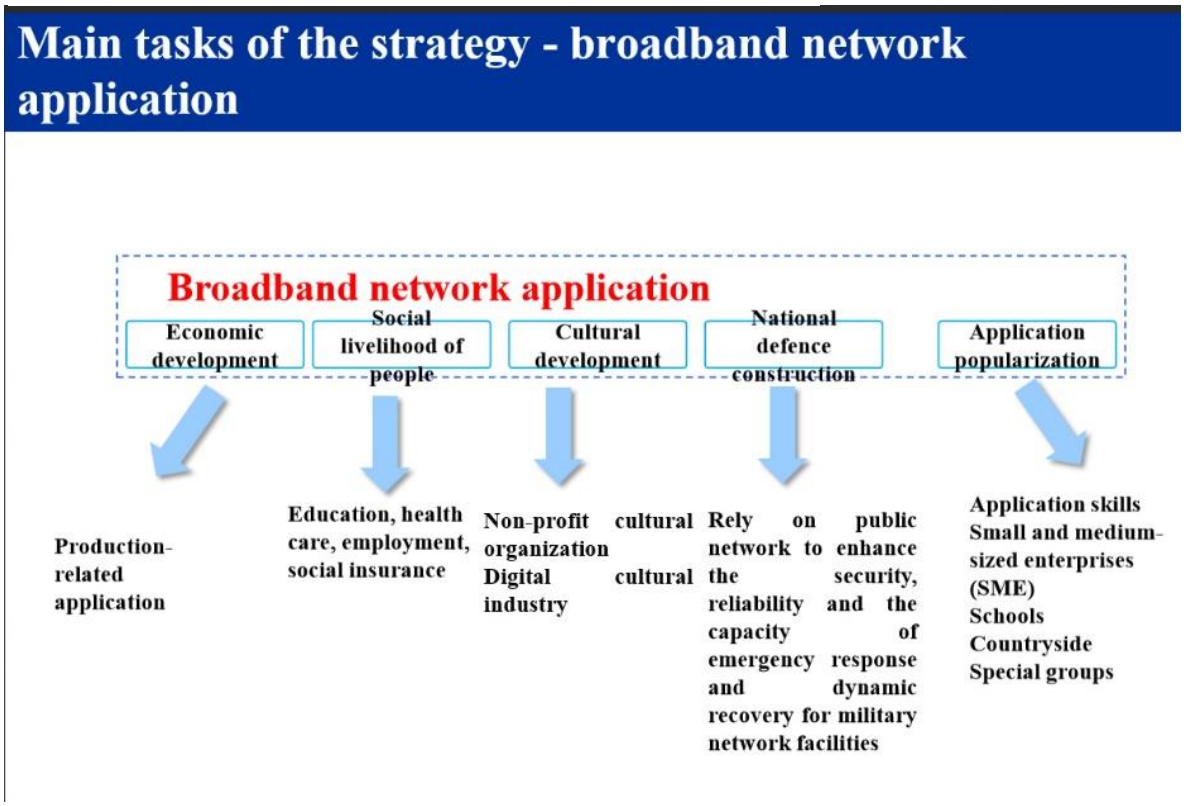
As a preliminary analysis, comparing Russia and China's attempts to control the Internet through their ISPs is of interest. From the beginning of popular use of the Internet in China, the state has been ever-present. Partly, this is a consequence of the illiberal nature of its economy in particular. For instance, China Mobile took over fixed-line operator China Tietong in 2008 after the shakeup of anti-trust legislation. Yet China Tietong was formally China Railcom, which had been part of the now defunct Ministry of Railways PRC. Railcom was primarily developed for the country's railway communications industry, and later expanded to residential and other users (China Daily). In short, the competition that the state seeks to introduce is still very much controlled and is in a way artificial. What exists today as the Chinese ISP and mobile technology markets are directly linked to its past. While the Internet began in an academic setting, it has always had a distinctive Chinese quality, with state ventures cooperating with foreign companies to expand the Internet beyond academia to businesses and the general public. In comparison, Russia's ability to control the Internet today is hindered by its quasi-liberal economy and how the Internet got initially dispersed through private enterprise. While the state-owned Rostelecom is the largest ISP in Russia, it controls only 35 percent of the market and the state still has to deal with the reality of nominal democratic values. The roots of China's intranet were built into the system from the beginning, which can be seen as an advantage of long-standing authoritarianism over quasi-democratic authoritarianism.

State Policy Regarding Internet Penetration and Use

Broadband Targets. The 12th Five-Year Plan was adopted in 2011 and promised the construction of a greater degree of broadband for the "safe and ubiquitous" use for its Internet users, and subsequently the "Broadband China Strategy and Implementation Scheme" was published in August 2013 (Hart). *Forbes* magazine and Hart reported that the Chinese government had announced an infrastructure upgrade to increase urban centers' speed to up to 20 Mbps and rural speeds to 4 Mbps by 2015. Such speeds have yet to be achieved. By 2020, the State Council's "Broadband China" strategy would have 50 Mbps in urban centers and 12 Mbps in rural areas. Rapoza poses two interpretations of the meaning of further broadband penetration: "To build out its internet infrastructure, Beijing will be toying with opening its society to the rest of the world…or cracking down and censoring a highly populated internet even further." Chinese officials are adept at opening technology while simultaneously

strengthening state control, so Rapoza's glimpse of openness may be merely a specter. Rapoza's pessimism, on the other hand, might be warranted. The image below is from a presentation from the China Academy of Telecommunication Research of MIIT (the government ICT branch).

Figure 4 Main tasks of the Chinese national broadband strategy
(Yu 13)



The rhetoric that surrounds the F2C is absent of any advocacy of increase meaningful access in China. While the MIIT acknowledges that increasing broadband to the countryside would improve the "social livelihood of people" it is simply a furtherance of what the state has claimed to provide since 1949. The state will play key roles in increasing broadband availability, encouraging domestic competition, and establishing new national technological standards for the purposes outlined above, all while controlling content and excluding users from potential threats to national security and harmony. It is apparent that China is moving to create a more sophisticated "fenced-off playground;" faster, more widely available, but still fundamentally limited.

Shut downs. In both Xinjiang and Sichuan, the state has shut down all Internet access or mobile phone services in the wake of conflicts with ethnic minorities, usually in connection with violent clashes with police. It is in these cases that the normative content of the F2C is most directly challenged.

In July 2009, Internet access in Xinjiang province was shut down for 10 months. The Uyghurs living in the province, who are of Turkish decent and mostly Muslim, are facing growing tensions with ethnic Han Chinese. Andrew Jacobs of the *NY Times* reports that tensions had flared due to the internal migration to the resource-rich region of Han Chinese in search of employment. There had been growing restrictions on freedom of religion, including campaigns against religious mandates on modes of dress (headscarves for women and beards for men). Required political education classes and raids on unauthorized schools illustrated the state's desire to achieve "social harmony." By the time Internet was restored, only two official news websites were available; anyone wanting access to the rest of the Web had to travel to a neighboring province. The announcement of the Internet's restoration also came with a warning "…that anyone using the internet to spread harmful information would be punished severely (Hogg)."

In the summer of 2013, nearly 50 Uyghurs died in clashes with police. Official reports, when such incidents are reported nationally, paint the protesters as separatists and terrorists, but Jacobs argues that those who killed were not heavily armed. When the reporter arrived in Hotan, an isolated city in the Uyghur-dominated southwest Xinjiang, these clashes had resulted in the cut-off from mobile Internet access. There are other ways in which the state limits the meaningfulness of access for Uyghurs, including using the Arabic script for the few websites that exist (6,000 versus some 400,000 in Beijing alone) when most Uyghurs are familiar with the Latin script. It is possible to bypass the restrictions and censorship through virtual private networks[63] (VPNs), but Olesen reports that most are unwilling to use such a method.

> In March, Xinjiang's top Communist Party official, Zhang Chunxian, told reporters at the annual meeting of the National People's Congress, China's legislature, that 90 percent of "violent terrorists" use virtual private networks, which obscure a computer's location, to circumvent China's web controls and watch extremist videos.

[63] "A VPN has the look and feel of a private network to a user. But it's really part of the Internet with heavy security—so no one on the Internet can see what's going on in the VPN…it exhibits at least some of the characteristics of private network even though it uses the resources of public switched network (Newton 1210)."

Like the rest of the China, Uyghur webmasters are pressured to report the activities of their users, especially anything associated with separation or independence.

These tactics are not solely found in Xinjiang. Olesen reports that censorship and monitoring—and cut offs—occur most frequently in areas that exhibit ethnic hostilities and poverty. In Sichuan Province, the state cut off mobile phone and Internet access in areas of unrest that were tied to the Tibetan ethnic minority. Three were killed by police after what Branigan reports as peaceful riots, and access was cut off in a 30-mile radius of the events in Ganzi, Sichuan. Like in Xinjiang, officials often blame outside influence for the unrest to justify the cut off from the Web, saying that Uyghur and Tibetan diaspora and Western supporters were instigating protest from the outside.

Censorship and surveillance. Censorship and violation of users' rights by the Chinese state are well-documented by Freedom House, Amnesty International, the HRC, and many other international institutions. Like Russia, China's ICT corporations including ISPs and content providers are responsible for carrying out state policies. And like Russia, providers of content are expected to monitor and otherwise comply with state policy for achieving social harmony. Baidu, the nationally-owned search engine, Sina Corp, owner of Weibo (a Facebook/Twitter hybrid), and Youku, (You-Tube equivalent) all meet with government officials to harmonize new censorship efforts as a consequence of current events. For example, Reporters without Borders recounted in 2011 that there was a coordinated effort to block any searches or tags with a combination of "Occupy [city]" as a result of the fear of the influence of the Occupy movement from elsewhere.

Other measures. In addition to being veritably all controlled by the state, and used to cut off entire populations' access, ISPs have been recruited into directly reporting on the actions of its netizens. Xinhuanet and Grant Brunner report on the legislation approved in December 2012 about new requirements for ISPs. Users must register with their ISPs and other telecommunication companies using their real names and contact information, "even a copy of their passports or IDs (Brunner)." The purpose, as explained by Xinhua, is the protection of public interest and users who had been increasingly the victims of Internet scams, fraud, identity theft, and libel. As the policy is meant to protect the public from thieves, ISPs are barred from using that information for any other purposes; real identities would be held "backstage" while users could still post comments anonymously. Yet, as Brunner highlights, the

responsibility for ISPs to delete illegal or subversive content and record the users that participate is indeed “scary” for users that would wish to remain truly anonymous. Frank La Rue, in his 2013 report to the HRC, comments on the trend of states using technology to violate users’ privacy. While the US, the British, and Russian data-collection programs (PRISM, Tempora, SORM) are carried out behind closed doors, albeit with the acquiescence of ISPs and other ICTs, the more blatant mandate of collecting real data on users takes the violation of privacy to whole new, and perhaps more honest, level.

Deep-packet inspection allows ISPs to detect the use of VPNs, so even one of the most commonly used methods for circumventing censorship and detection is not a viable option. As Olesen recounts, the use of such tools to shield users from the eyes of the government can quickly become evidence of guilt. As a consequence of the government’s ability to identify users, and the harsh sentences some users have received for their actions, Freedom House reports that self-censorship in the broader public is now largely common.

Domestic ICTs are not alone in these tasks. Recently, Baidu, China’s most popular search engine partnered with a San Francisco-based company CloudFlare to bring cloud services to Chinese businesses. Named Yunjiasu, or “fast cloud,” the service would create a “unified content delivery network that makes foreign sites more easily accessible in China, and for Chinese sites to load faster in destinations outside the country (Hamilton).” Cached sites would download faster for Chinese netizens and for foreigners trying to load Chinese business websites also cached by CloudFlare. The fact that Baidu, a Chinese content provider that is required by Chinese law to report illegal behavior to authorities, would have access to potentially harmful information stored in the American-owned cloud is a cause for concern for Hamilton. Yet, CloudFlare states such concerns are unwarranted: “customer identifiable information such as email addresses, password hashes, and billing information are never stored in the China network or shared with Baidu (Hamilton).” Bejtlich is dubious, claiming that the joint venture that is touted by some as a model that can be duplicated by other Western firms is exactly what the Chinese state wants. Motivated by China’s techno-nationalism, this sharing of technology would allow the Chinese state to learn how to copy and circumvent the protections afforded to users by companies like CloudFlare.

> With technical IP [intellectual property] in Chinese possession, domestic companies can build national champions to rival, and eventually replace, Western firms. China can also

> better understand, and eventually defeat, CloudFlare's security services, having first-hand access to IP and operational details.

For instance, CloudFlare has helped political movements keep websites operative during distributed denial of service[64] (DDoS) attacks. Bejtlich argues that by collaborating with Baidu, the company's IP can be used against others. Already, China's censorship is leaking through from domestic to international DDoS attacks; the "Great Cannon" was fired against a private website reporting on censorship in China, GreatFire, and against an open source code platform, Github. Each website could be seen as a threat to Chinese national security, but the attacks on sites hosted outside of China were unprecedented. Yunjiasu could also be used to censor content for netizens; the government could tell Baidu to censor some of the pages hosted by the cloud service in China. There is a growing tension when foreign companies do business with China; Google famously stopped doing business with the state in 2008 because of pressures to carry out censorship policies and hacks to its source code. But such decisions by MNCs to cut themselves off from one seventh of the world's population are bad business. It is likely that the CloudFlare and Baidu deal is a prototype that will be emulated, with the assurances from American companies that they will not be party to policies that are aimed at dismantling human rights. If Bejtlich is right, such beliefs are at best naïve.

Public Opinion on the Role of the Internet

There is a Western predilection, well-recorded in Morozov's account of the outsiders' perspectives on the Green Revolution, to look for the transformative capacity of the Internet in social and political life. The narrative in the United States is that the Internet grew to be the integral, global technology it is today because of the absence of the state and the freedom of anonymity, allowing for open discourse about a plethora of topics. Often, Western media focus on the violations of users' rights as seen through the lens of universalism; for example, the Chinese artist Ai Weiwei was featured in *Time* in 2011. He was painted as a sort of local hero who had the courage (and the Twitter followers) to

[64] Newton's definition of a Distributed Denial-of-Service attack: "You're a horrid person with mean intentions. You ping a website 400 or 500 times a second. Or, even worse, you create a virus and use email attachment to infect a lot of networked computers, which become Zombies under your control. You command them all to go to that website, which is then overwhelmed and no longer able to serve legitimate customers. Hence the term Denial of Service attack. Such an attack is very hard to prevent, since sometimes it's done from computers all over the country or the world. This is called a Distributed Denial of Service Attack, or (DDoS)… (Newton 357)."

discuss controversial and potentially embarrassing government actions, like collapsing schools and the murder of Shanghai police by an abused former inmate.

While routine crackdown on dissidents offer important accounts of how China abuses human rights, the cultural relativist notions of varying expectations is largely absent. How *do* the netizens of the "fenced-off playground" see the Internet?

The CNNIC reported in June 2015 that

> According to a survey conducted in December 2014, the proportion of Chinese netizens who believed the country's network environment was safe or very safe, who trusted Internet information, who took a positive attitude toward Internet sharing, who liked posting comments on the Internet, or who depended or heavily depended on the Internet was respectively 48.6%, 54.5%, 60.0%, 43.8% and 53.1%.

Such numbers are fairly typical, but do show a higher than expected percentage of netizens trusting the information (and perhaps the source of that information) on the Web, up from 35 percent in 2007. The official report categorizes trust as a sort of post-modern problem; as urbanization rates climb, traditional sources of trust are abandoned in a "society of strangers." Trust in cyberspace not only improves peoples' interaction on the Web but also in real life. Yet, the report also states: "Although network security incidents occur frequently, netizens' overall level of online trust and inclusiveness is improving." The authors do no clarify what they mean by the "network security incidents."

Moreover, the CNNIC reports that the Internet functions as a "relief valve" in which users can post comments and suggestions for the state that in turn promotes socialist democracy. The fondness of its users, especially digital natives ages 10-29 for posting comments about state policy "…mitigate[s]…social conflicts, and therefore promote[s]…social harmony (40)." Over fifty percent of the survey respondents in that age group reported liking to post online comments, while the rate drops to the nevertheless respectable 35.4 percent for respondents aged 60 or over. The authors also remark while the Internet can help develop young peoples' personalities, it is also a vulnerable time in which reality and virtuality become distorted, and "…where polarization of speech may produce some negative effects on young people's social cognition (40)." The extrapolation from "posting comments online" to political discourse may be an exaggerated one. At least in the US, youth interest in online political discourse in the last ten years has been low, with the possible exception of the Bernie Sanders campaign. It is an indicator of

some rhetorical recognition by the state of a positive political role for the Internet, albeit shaped by distinctly Chinese values.

Other global surveys confirm some of the optimism reported by the CNNIC, but not all. Kull et al. (2008) report that 42 percent of netizens thought the government should have the right to limit access to preserve stability, leaving the majority of respondents not in favor of such measures. Eighty-five percent wanted to read unfiltered or uncontrolled news, and 71 percent reported a desire to read whatever they wish on the Internet. GlobeScan (2010) reported a prevalent belief in access as a right, with 87 percent of respondents answering affirmatively. Forty percent argued that content should not be controlled by the government, while 55 percent said it was not a safe place to freely express oneself. The final available survey was conducted by Internet Society's Global Internet Survey 2012. Eighty-four percent of respondents said that access should come without data or content restrictions, 93 percent said that freedom of expression should be guaranteed on the Internet, and the same percentage argued that social media enhanced rights of assembly and association. Ninety-two percent argued that the Internet should be considered a human right. While many argued there were numerous roles for the government to play in access and availability (government should provide cheap computers 92 percent, government should encourage competition 93 percent), 88 percent argued that the state had the right to govern the Internet as it sees fit, one of the highest percentages of all states (though eclipsed by Indonesia in this study, at 91 percent). Netizens are often nationalistic in nature, and support for the cyber sovereignty here is unsurprising.

David Herold's 2012 article "Escaping the World" paints a stark portrait of young *wangmin*. Overall, Chinese users see Internet spaces outside of China as rather uninteresting; access to these sites from China is slow with many time-outs, and content is dominated by foreign languages. The nationalist streak that is present in state policy concerning infrastructure and access is present even in netizens' perspectives about the web.

Different from F2C frames and instead of seeing online spaces as real extensions of their social and political lives, some Chinese Internet users view it as an escape from the conformity and drudgery of the real world. The metaphor Herold uses is that of the 19th century carnival, in which the line between

performer and observer is blurred. The carnival was exaggerated reality where regular rules did not apply.

> "Chinese Internet users, whatever their background, are strongly influenced by their cultural context", as "the 'relational self' and *mianzi* (face), which are core elements of Chinese culture, are reinforced via ICTs (W. Chu)." In other words, Chinese Internet users like to connect to other netizens and place a great value on their online identity or presentation, which is, however, separate, different, and not easily connected to their offline identity as Farrall pointed out (2).

The disconnect between reality and virtuality is engrossing; netizens spent on average 19 hours a week online in 2012 [by 2014, this became 26.1 hours; 56.4 percent use the Internet for gaming, 66.7 percent watching video (CNNIC 2015b)]. "Online they can play games, watch movies, get married or divorced, take part in 'virtual' manhunts, engage in the harassment or bullying of 'evil' people, and be entertained by it all, before returning to their 'real' lives (12)." At times, the line between reality and virtuality can be blurred, as the CNNIC indicated; Herold recalls the case of the Kaiping Girl of Guangdong Province who was the victim of kidnapping and rape in 2008. Video of the crime was posted online, apparently without any consideration of the real life consequences it could have for the perpetrators. As Herold explains, the incident "provides a strong example of the reckless behavior of young Chinese who believe they can do anything *online*, but ignored that their 'real' misdeeds had occurred *offline* (8)."

What one should extrapolate from the carnivalesque quality of Chinese netizens' views of the Internet in their political lives is not immediately clear. On the on hand, increased Internet access would mean more accountability for the government. Particularly, that the inhibitions against posting criticism of the government could be reduced because what they do in the virtual world would have little consequence for the real *mianzi*, or face, of an individual or his family. On the other hand, the fantasy aspect of the netizen's virtuality could mean that any political discourse might not be serious or have consequences in the real world. The disconnect between real world actions and posting a video online of the Kaiping incident may not be the norm, but just the most extreme expression of this concept. Instead, if the Internet is seen as nothing of consequence beyond an escape from reality, one could conclude that looking for real political discourse or change in such places would be nothing but ephemeral farce. This, coupled with the state's strong monitoring of its netizens, further discourages how the Internet could viewed as a transformative tool in China.

The *Economist's Facebook* post from 23 March 2016 about the lack of meaningful respect for human rights by the Chinese government illuminates some of the tension that the Chinese diaspora and Taiwanese feel about the techno-nationalism, social media, and the role of the Chinese state. User SY Chan is located in Taiwan and claims that even Facebook itself should be considered a human right. Ian Meng and Hu Ru Zhu who claimed that Chinese social media was just as acceptable to use as an alternative to Facebook were located in the US at the time of their reactions but from originally from Beijing and Guangzhou, respectively.

Another line of inquiry for future research is revealed in this data: to what degree does the Chinese public represent the rhetoric of China about techno-nationalism and cyber sovereignty?

To play a devil's advocate, it is fair to say that you cannot know what the mass of users would think or do were they able to access the World Wide Web in a meaningful way. Since many Chinese users have never been connected without censorship or monitoring, nor do they exhibit signs that see it as an avenue for political discourse other than as a suggestion box, looking for signs of the viability of the Internet to challenge the government in a meaningful way may merely be a Western illusion.

International Rhetoric

The norm of the F2C is not evident in China. While there are policies in place to extend access and to establish state-of-the-art speeds, their aim is global economic competitiveness, not political participation. Instead, China's response to the F2C is nationalistic in tone and aims instead at the harmonization of interests among the state, the people, and the business community.

The first articulation of cyberspace sovereignty by the Chinese is found in a White Paper published by the *People's Daily* in 2010 (Liang). The document reveals an expansive vision for the Internet in China, viewing it as a cornerstone of economic growth, scientific and technological innovation, and "livelihood improvement." The government is required to create conditions conducive to its development and regulate it so that the Internet remains in line with the community's goals. The white paper promotes its successes mostly in terms of statistics, boasting about increases in network infrastructure, including optical and submarine cables, the number of netizens, and increases in speed. They acknowledge the digital divides that persist among its regions and between urban and rural centers,

but the importance of closing those gaps is framed within the pragmatic benefits of the Internet: economic, technological, and cultural progress.

A cursory glance at the contents of the white paper suggests that the government is sincerely grappling with civil rights, including "Guaranteeing Citizens' Freedom of Speech on the Internet" with cybersecurity threats (real and imagined). The rhetoric contained within the paper sidesteps traditional understandings about the freedom of expression, instead framing it in terms of the ability of users to stay abreast of news and interact with the government. "The Chinese government has actively created conditions for the people to supervise the government, and attaches great importance to the Internet's role in supervision." This "suggestion box" feature is a mechanism through which the Chinese state interacts with Internet users. Further, while privacy of correspondence is something protected by law, it cannot interfere with the overriding interests of the state, collective interests, or other users. Such conditions easily justify the intrusion of the state on its users' actions on the Internet. The state also faces threats from abroad, which means that the government must safeguard against any that would impinge upon the honor of the state, incite ethnic tension, jeopardize the state's religious policies, or spread rumors or slander. Finally, the white paper mentions that while China cooperates with the WTO and WSIS in order to protect foreign MNCs and to improve technological capacity, Internet policy is ultimately a domestic affair. "Though connected, the Internet of various countries belongs to different sovereignties."

This belief is articulated in a letter to the UN General Assembly dated in September 2011. Also signed by Russia, Tajikistan, and Uzbekistan, the letter confirms the need for cooperation among states for the development of the Internet, including overcoming the issue of digital divide and cybersecurity, but reaffirms the primacy of the state in this networked arena. The letter reaffirms "…that policy authority for Internet-related public issues is the sovereign right of States, which have rights and responsibilities for international Internet-related public policy issues." The General Assembly responded to this assertion in 2013, confirming that states have sovereignty authority to ICT-related activities and infrastructure within their borders, but also added that sovereignty must respect human rights. "State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments." The report from

General Experts in ICT also admonished states not to use proxies in cyberattacks, referring to the fact that states can act with relative impunity when hackers or state ICT experts can cover their tracks adeptly.

Shannon Tiezzi reports on the development of the cyber sovereignty norm, noting that Chinese officials are quick to point to, first, their compliance to WTO, WSIS, and efforts at technological cooperation, and second, the UN's affirmation that states have the right to develop ICT policy which gives credence to their global policies and crackdowns on netizens. In its justification, Chinese representatives ignore the admonitions of the UN that ties ICT policies to human rights. Instead, Chinese representatives tie ICT policy to security, and claim that their perspective on the relationship between state law and the Internet is meant to challenge the dominance of the United States, whose position as the leader of global Internet policy is a threat to everyone due to cyber-espionage and cyber-attacks. Tiezzi states that:

> China's goal for this dialogue would be to codify its own interpretation of "Internet sovereignty" into international law, much as Western countries have been able to codify their idea of "universal values." The *People's Daily* article sees cyberspace as a contested zone where the U.S. wields too much influence; it seeks to combat this by pushing for international consensus modeled on its own vision for the Internet.

MIIT Minister Miao Wei asserted the Chinese position on the Internet related to domestic and foreign policy. In an October 2015 press release titled "The Big Picture: Big Data as a competitive resource," Wei argues that technology, specifically big data[65] will be the most important aspect of power for the remainder of the 21st century. He compares it to other modern contests over resources among the great powers: coal, gas, gold, etc.

> Big data analysis through data integration and depth of excavation, find the law, create value, and thus establish a seamless link from the physical world to the digital world and the online world. Large data era, online and offline, virtual and reality, software and hardware overlapping staggered, cross-border integration, to reshape our understanding and practice mode, open a new industrial breakthrough and economic restructuring.

By 2020, Wei predicts that global data usage will be about 44 zettabytes (ZB), or 44 trillion gigabytes. Whoever has control of this capital resource will determine where economic growth takes place and at what rate. Wei insists that Chinese councils and the legislature intend to be ready to take advantage of this capital resource. "Internet +" and "Made in China 2025" plans are meant to build a development

[65] "The amount of data in our world has been exploding, and analyzing large data sets—so-called big data—will become a key basis of competition, underpinning new waves of productivity growth, innovation, and consumer surplus… The increasing volume and detail of information captured by enterprises, the rise of multimedia, social media, and the Internet of Things will fuel exponential growth in data for the foreseeable future (Manyika et al)."

strategy to strengthen China's domestic Internet and information infrastructure along with cultivating business leaders who will be sophisticated enough to use these technologies and be innovative in the field. Unlike the F2C and even the ITU's visions for the development of Internet access and technologies via entrepreneurs or public-private partnerships, China views the development as essential to foreign policy and economic growth and emphasizes its techno-nationalistic standpoint.

In line with these goals, Chinese officials are not shy about exporting the technology elsewhere. First, early in 2015 the Xiahua news network touted Internet infrastructure investment in West Africa. It loaned Benin $69.14 million for a broadband project, and the Chinese Ambassador who coordinated the project noted it would achieve two aims: strengthening ties between the countries and fostering economic and social development. The ties between African states and China are both longstanding and growing, with *The Economist* reporting in 2014b that China gave $62.7 billion in loans to African states between 2001 and 2010, totaling 20 percent more than the World Bank. The authors of the 2014 article comment that it is difficult to ascertain what China's intentions are in Africa: to mold its ideology in the fashion of the Chinese as Westerns have done in the past, or simply that entrepreneurial Chinese citizens see opportunity in these markets. The latter seems more likely as tensions are apparent, and racism and bitterness is shown on both sides.

> In Guinea, writes Mr. French [a *NY Times* journalist] , "there was mounting resentment over the way China was seen to be…despoiling the environment, dispossessing powerless landholders or flouting local laws, fueling corruption, and, most of all, empowering awful governments."

It is unlikely that the Chinese deal in Benin is motivated by an earnest desire to mold an African Internet in the fashion as a Chinese one. Instead, it is more likely that such deals are done with the desire to do business there more efficiently. Broadband is seen by China as vital to economic growth, and so deals in Benin would mirror the same impulse to enable broadband in the Inner Mongolia Autonomous Region. Just follow the resources.

In moves that might be guided more by the prospect of profit, growth, and innovation rather than ideology, China also sells its surveillance technology to other states. The majority of its DPI technology is powered by the American MNC Cisco's and its routers. China buys $2 billion worth of Cisco equipment per year despite the criticism that Cisco has received for supporting the illiberal tactics of the regime. Nevertheless, Huawei, a Shenzhen-based company also manufactures its own DPI suite, the SIG 9800.

Insider Surveillance reports that while the technology is marketed as a "network management system," it is also adept at surveillance tasks which include monitoring peer-to-peer networks (like file-sharing), voice over Internet protocols (Internet phones), instant messaging services, videos, as well as applications like Skype, Facebook, MSN, among others. The suite can monitor more than five million URLs in *multiple languages, "*including not just Chinese, but also English, Russian, Arabic, French and Spanish." Huawei, in addition to ZTE and Sempetian, sells this technology to others including "a number of states in Central and South-East Asia, eastern Europe and Africa, including Kazakhstan, Vietnam, Belarus, Ethiopia and Zambia (*Economist* 2013)." Stecklow reports that Huawei was brought before the State Department about whether it violated US sanctions against Iran by selling them equipment in 2011. Some of the articulation of the cyber sovereignty norm is indirect; nevertheless implicit in the marketing of these products is the full-fledged acceptance of the right that governments possess to control and monitor citizens' access.

Such deals signal the incompatibility of the Chinese view of the role of the Internet and the F2C. As noted elsewhere, Western states support ICANN and what they view as a more dispersed view of Internet governance. Russia and China would like the ITU to gain more power in the area, which would bring newcomers to the Internet equal players in a system that was by and large created by America.

***

As the archetype case in the Not Free category, China demonstrates the various ways that a state can circumscribe Internet freedom and the F2C. While increasing Internet penetration is important for economic purposes, it has done so while keeping the needs of unity and social harmony in balance. As such, it controls ISPs and the policies they have for users while artificially creating a competitive marketplace to improve costs, speed, and efficiency. It has shut off parts of the country from the Internet either as a punishment or as a preventative measure aimed at curbing nationalism and other challenges to the state. Additionally, it has helped develop cyber sovereignty as an exception to the F2C in both practice and rhetoric. But it has not directly challenged the goals of Internet openness as invalid or openly opposed human rights on the web, only framing state intervention as necessary for immediate state interests.

Cuba

…the wild colt of new technologies can and must be controlled.
Ramiro Valdés, (former) Communications Minister International Conference on Communication and Technologies in Havana, February 2007

Cuba is the extreme case in this study. While all of the states face rapid changes to their ICT sectors, as of late Cuba has been the focus of much scholarly and media attention since the thawing of the remnants of Cold War tensions with the US in December 2014. Well-known throughout the world as one of the least connected states, there are hopes that as restrictions are eased—or the embargo is lifted—political repression will be lessened. Yet these hopes ring of the cyber utopianism about the transformative capacity of technology. First, the Cuban government fears both the loss of sovereignty in the face of ICT MNCs and the loss of control over media and expression. Second, the Internet's immediate ability to affect change will be hampered by Cuba's ICT infrastructure that has not been updated since before the invention of the Internet. It is clear that Cuba's reason for technological backwardness can no longer be blamed solely on Havana's inability to purchase ICT infrastructure because of the embargo. The state will no doubt find new justifications to perpetuate its stranglehold on information and technology.

Background

Cuba has the smallest population of this study with approximately 11 million people, ranking the country 80th in the world. Cuba's geography is also a condition of its Internet access. While it consists of 110,860 km^2, ranking somewhere in the middle of all nation-states at 106th in the world, it is the proximity to the US—90 miles from the coast of Florida—has influenced its social, political, and economic development since independence and even before. Seventy-seven percent of its population lives in an urban area, but it has only one major metropolis, Havana (2.137 million), with other cities with populations of 425,000 or less. It has a mediocre economy, accruing $128.5 billion in 2014 placing it 76th in the world. While being a communist state in name, it has largely depended on foreign aid to supplement its economic model, which is highly dependent on agricultural exports like sugar. Cuba's GDP equates to $10,200 GDP per capita, 131st in the world, two rankings above Indonesia.

Statistics regarding ICT technologies (CIA Factbook 2014) are well below global averages. The country has 1.26 million landlines, ranking 67th in the world; one phone is plugged in for approximately every 11 people in the state. The figure escalates slightly for cellular phones, undoubtedly also hindered

by the embargo, with 2.5 million in the country, placing it 144th in the world in 2014. There are 3 million Internet users in Cuba which ranks the state 85th in the world in number of total users and totals 27.5 percent of the population. The statistics in part reflect a concerted effort by the government to hamper Internet access among the broader population apart from government officials and healthcare providers. Such a policy directly challenges the norm of the F2C. Unlike China and Iran, Havana has chosen a path that differs from the cyber sovereignty model in which a government choses to exert varying degrees of control over Internet access and use and instead, Cuba has purposefully kept its citizens off the Web, a method that comes with serious economic consequences.

Cuba had a relatively short-lived democratic experience, and its brief foray into the political arrangement was marked by citizens' dissatisfaction and political corruption. Like all of the other non-archetype states of this study, Cuba's history is marked by outside influences, first by Spanish colonialism and second by direct American intervention after 1898. Its lack of any adherence to the freedoms of expression and association, along with arbitrary arrest and inhumane prison conditions draws the ire of HR NGOs and the Cuban diaspora. With reference to HR norms related to the F2C, the 1976 Constitution (amended in 2002) pays lip service to these ideas:

> **Article 53:** Citizens have freedom of speech and of the press in keeping with the objectives of socialist society. Material conditions for the exercise of that right are provided by the fact that the press, radio, television, cinema, and other mass media are state or social property and can never be private property. This assures their use at exclusive service of the working people and in the interests of society. The law regulated the exercise of those freedoms.
> **Article 54:** The rights to assembly, demonstration and association are exercised by workers, both manual and intellectual, peasants, women, students and other sectors of the working people, and they have the necessary means for this. The social and mass organizations have all the facilities they need to carry out those activities in which the members have full freedom of speech and opinion based on the unlimited right of initiative and criticism.
> **Article 57:** Mail is inviolable. It can only be seized, opened and examined in cases prescribed by law. Secrecy is maintained on matters other than those which led to the examination. The same principle is to be applied in the case of cable, telegraph and telephone communications.

The term "social property," while making good use of socialist ideology, is another term for government-owned. The power of the state is evident in the entire document, claiming it to be the sole representative of "the power of the people and for the people," and the organizational vanguard of revolutionary leaders like nationalist hero José Martí along with Marx and Lenin.

The question that is pervasive among media outlets and interested parties is whether such a regime can survive the opening of diplomatic relations and trade. As argued by Larry Press of the Information Sciences Institute of the University of South Carolina (see Russia chapter) and others, one of the main justifications for the failure of Cuba to keep pace with technological advancements is the inability for the state to get the materials it needs to update its infrastructure. Once it is lifted, there is little reason to expect that the Castro brothers will loosen restrictions on expression or access. Instead, as Lillian Guerra explains, the Cuban government is seen domestically as *el Sistema*, and the norms that helped the Castros cement power during the Cold War live on today. "…the will to police oneself and others in a surveillance culture went hand in hand with deference to leaders' higher will and allegedly higher political consciousness (Guerra)." The fact that by 2011 Raúl Castro had opened up the Cuban economy for foreign investment has assured that those who are part of the *el Sistema* will continue to hold their power long after the brothers are dead.

> …without the right to organize politically, let alone lead a march down any Havana street or start a chess club without permission, they enjoy little or no influence over their government and their leaders enjoy little accountability.

In all likelihood, the members of the military or Castro's regime will make Cuba look like its past in that leaders (elected or not) will benefit from foreign direct investment without much opposition from the people.

The Internet in Cuba

Background. Cuba had some early history with sophisticated computer technology, getting its first computers from the US in the 1950s. This relationship dissolved after 1959, but together with the Soviet Union and Council for Economic Mutual Assistance (CMEA), Cuba trained technology experts and had a "modest" microcomputer industry through the 1960s and 70s that sold its hardware to other CMEA countries (Mesher et al 1992). It could not sell it domestically because there was no market. By 1992, Mesher et al. report that the industry was "in very deep trouble," because of the lack of funds that could keep the industry—and the rest of the Cuban economy—afloat. Cuban economic planners at the time realized the potential of a successful computer software industry and what it could bring: "hard currency income, employment for an oversupply of university graduates, technology transfer into Cuba, international visibility, applications to other sectors of the economy, and modest requirements for initial

capital investment (Mesher et al 1992)." The government planned to train a new labor pool alongside an educational program that would improve computer literacy throughout the island by the Communist Youth Union (UJC). But this nascent industry faced two basic problems: first, the lack of infrastructure meant it was difficult to have state-of-the art facilities in place that could develop software among the geographically separate facilities, and second, the state that was notionally ideologically opposed to the idea capitalism that would bring substantial profits, and perhaps power, to the quasi-independent companies that would produce the software. As a result, the "informatics" industry died out and produced little new hardware or software.

The reluctance to adopt the Internet largely grew out of a similar reluctance that characterized Brazil under the bureaucratic military regime: a fear of a foreign technology that the state could not control. Unlike Brazil, Cuba never attempted to substitute its own alternative. Instead, the first Internet connection was a UUCP exchange between the state-run Center for Automated Exchange of Information (CENIAI) and a Canadian affiliate, the Association for Progressive Communications (Press 1998). In 1996, UUCP networks were replaced with a TCP/IP 64 Kbps link from CENIAI to Sprint in the US (Press 2011). The director of CENIAI, Jesus Martinez, sent the first email to his fellow networking community, thanking the Forum of Latin American and Caribbean Networks whose assistance was vital for the know-how to establish the link, and said in closing "A new era has just begun for us." Press puts the director's enthusiasm in perspective: "Martinez was clearly proud of Cuba, but he also shared the values and enthusiasm of the international networking community, who believed, correctly, that the Internet would profoundly impact individuals, organizations and society." Despite all of the obstacles that stand in the way of the ICT professionals' narrative, its presence in Cuba is enough to give Press hope in 2011. Recent blog posts by Press follow the developments of Cuba's recent steps towards recent Internet penetration with a critical eye. Whereas Press seems to be optimistic about some the increased availability detailed below, the presence of American ISPs and telecoms to fill in the gaps may not lead to the equitable distribution or the new era for Cuba that Martinez hoped.

By 1998, Press et al report on the meaningfulness of Internet access in Cuba[66], and as expected, it scored rather low overall and comparatively to the region. In the intervening years between UUCP protocols and the switch to TCP/IP in 1996, only 100 users of the Internet were to be found in all of Cuba. Geographically, Internet access was limited to Havana, but on this measure Cuba scored better because of email access points scattered through other major cities. Cuba scored low on sectorial absorption because of the rare use of the Internet outside hospitals and government sectors and connectivity infrastructure. While they had the TCP/IP link, no other infrastructure existed alongside pre-revolutionary telephone cables. Health care users were able to use the Internet for both email and information retrieval, but little other use could be made of the connections that actually existed. In sum, the meaningfulness of Internet access averaged 1.5 on a scale of 0-4 by 1998. While this assessment of access in Cuba is nearly two decades old, it is nearly identical in terms of access today. This appears to be slowly changing during the last twelve months, but the process is painfully slow and its outcome is not guaranteed.

Internet penetration. According Freedom House (2015), roughly 30 percent of citizens in Cuba have access to the Internet, a percentage that has doubled since 2009. Of the developments, two positive trends emerge: websites registering the domain of .cu have tripled in the previous two years and new laws have permitted more of the private sector to use the Internet. Markedly though, of the 65 cases assessed, only two others scored lower on their ranking on Obstacles to Access, Ethiopia (23), the result of poor infrastructure and government-owned ISPs like Cuba, and Syria (24), whose state's infrastructure has been devastated by war and electricity cuts due to government attempts to control the way the war proceeds.

As in the past, Cuba's Internet remains geographically centered in Havana, a few other major cities, and for trusted elites. These include access for doctors, Cuban officials, trusted journalists, and intellectuals in their offices, albeit using the Cuban intranet for email and informative websites. It was not

[66] Press et al (1998) present six measures of the meaningfulness of access: pervasiveness (users per capita and the degree to which non-technicians are using the Internet), geographic dispersion (the concentration of the Internet within a nation to a particular cities or major cities), sectoral absorption (the degree of Internet utilization in the education, commercial, health care, and public sectors), connectivity infrastructure (IXPs, internet backbones, and last-mile access methods), organizational infrastructure (ISPs and the market share), and finally sophistication of use (whether the Internet is a substitution for other technology or it is being used innovatively).

until 2008 that home PC ownership became legal, but the average PC was $800 at a time when the average wage for all Cubans was $20 per month (Voss). Internet access at home is highly regulated and Resolution 92/2003 forbids access to unapproved persons; the penalty for disobeying the law is the revocation of access privileges.

Speed and cost. Testmy.net reveals results for three locations in Cuba. First is La Habana, referring either to the district or the city, at speeds of 1.7 Mbps download and 4.4 Mbps upload. Mantanzas, a resort town 56 miles from Havana, has 788/919 Kbps connection, while another tested site in Havana recorded 678/943 Kbps.

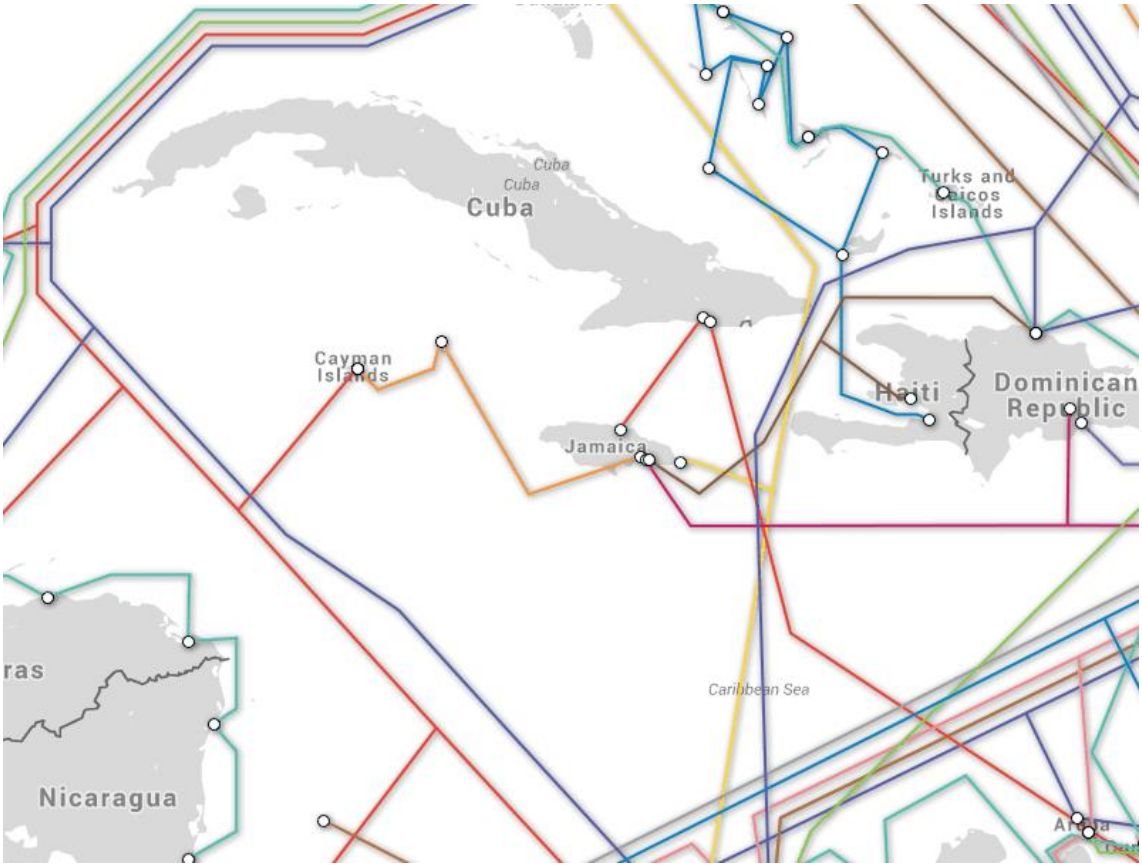
After the thawing of relations with the US after 2014, Havana is taking some steps towards increasing Internet penetration. By mid-2015, 261 "navigation halls" were made available around the island, mostly in major cities. Highly monitored by the state, these halls are prohibitively expensive. While the price has gone down—from $4.50 per hour to $2 for access to the Internet ($0.60/hour for access to Cuba's intranet)—costs are approximately 10 percent of the average Cuban citizen's monthly salary. Users can also purchase a Nauta card from ETASCA for 30 days of access or a permanent card (if they can afford it) that comes with the requirement of submitting to the authorities the users' names, email addresses, and passwords. Such accounts are extensively monitored. In order to get access, users rely on expatriates to provide the cash for the hourly rates or ETASCA cards. It may be a government policy aimed at profitability and hard currency rather than inhibiting penetration.

How well do new Internet access points accommodate demand? By October, Luis Paz reports that the feeling among users was not optimistic. Demand had far outpaced supply at newly minted Wi-Fi hotspots. They can accommodate only 50 to 100 users at a time, and the speed deteriorates according to the number of users using the service simultaneously. Users are critical, with problems of being kicked off the Internet alongside poor customer service. Even Cuban television segment on *Cuba Dice*, a show that is controlled by state, saw fit to criticize its poor rollout: "The report criticized the terrible planning evinced by [the Telecommunications Company of Cuba] ETECSA, which failed to provide comfort for its customers, despite the high demand for the service, as well as the superficial replies offered by some of its executives in this connection." Interviewees claimed that the poor performance was indicative of the

state using these hotspots and navigation halls as a distraction from the overall inadequacy of the government's provision of Internet services.

In 2007, an agreement between Cuba and Venezuela arranged for the construction and deployment of a submarine fiber optic cable that would decrease Cuba's dependency on satellites for Internet access. Voss (2008) reports that preceding the agreement, the Cuban government blamed the US embargo for its paltry infrastructure and inability to connect to any of the apparently plenty of undersea cables in the region. Press (2013) reports that from 2007, Cuba had been dependent on three satellite providers: Tata Communications (an Indian MNC), NewCom (a US satellite provider based in Miami) and Intelsat (a former IGO privatized in 2001). The cable's completion was planned for 2009, but numerous delays meant that the cable's connection was not made until early 2011. The cable is shown below in red, while the remaining numerous cables conspicuously appear to go around the island:

Figure 5 Cuban submarine cable map 6 November 2015
(Telegeography 2015)



Subsea News and Press (2013) both report that despite the cable's completion, it remained unused for nearly two years. When traffic began in January 2013, it did not serve the entirety of the Cuban intranet. Instead, ETECSA Cuba's *de facto* sole communications provider controls traffic asymmetrically (as Lebanon did in 2011), using the cable to improve speeds and reduce latency for incoming information, but directing outgoing traffic to the satellites. This improves web browsing for a few but makes it difficult for most to send information outside the island. Freedom House argues that the cable connection that directly links Cuba's intranet to the rest of the world did not improve speeds for users as much as hoped. This hampers the meaningfulness of access in 2015 in that any speed under 1 Mbps makes sites or content with multimedia all but impossible to use.

Mobile phones, the bastion for access when all other avenues fail, are also underused in Cuba. The ban on their ownership was lifted not long after the ban on PC ownership in 2008, and today there are 2.5 million mobile phones in the country, reaching a penetration rate of 22 percent. Recently, the state has cut monthly charges for mobile phone use, airtime, and SMS. Nevertheless, costs of both the hardware and the service plans, provided by Cubacel, are unaffordable for most Cubans. Like the Nauta cards and ETECSA hourly Internet charges, many of the fees are paid for by Cuban relatives living abroad in the US and Spain. ETECSA has even enabled an online service that allows for easy payment of fees of those living inside Cuba. Smartphones, again usually gifts from the diaspora, can send email using the Nauta cards but have no further connectivity, and users are charged $1 per Mbps of information transfer. GPS-enabled phones are forbidden. The state has restricted cell phone use in times of heightened political sensitivity (Freedom House 2015 239).

Internet Service Providers

As with all of the cases explored, the ISPs of Cuba are indicative of the meaningfulness of access for its citizens. There are two such providers: the Center for Automatic Interchange of Information (CENIAI) and ETECSA. The former appears to be relegated to academia and Cuba's informatics past. Cubacel, the mobile provider, is a subsidiary of ETECSA, so in fact most access is channeled through just one ISP. So few options are unprecedented in this study; in China, recall, that despite being state-owned, all three major ISPs are made to compete with each other to increase efficiency and innovation

through the industry. However contrived such a model might be, consumer choice forces considerations about customer satisfaction.

The fastest and most meaningful access most people can get in Cuba is in hotels, government institutions, and foreign embassies. There is a stipulation that this access is solely for tourists rather than for citizens, but people often subvert such rules in order to get access to unblocked social media and other “dangerous” websites.

Following in the footsteps of Venezuela’s Telefónica, several ICT companies have already come forward to work with ETECSA in developing its infrastructure. Orange Digital Horizons, a French ICT agreed in July 2014 to help develop the industry in Cuba by sharing phones, equipment, and expertise. There were concerns that the thawing of relations between the US and Cuba may endanger the agreement, but the CEO of Orange assured interested leaders it would not (Paquette). This PPP is a development that may signal how Cuba might proceed with increasing Internet penetration rates in the future.

The evidence is carried over with other agreements that have developed in 2015. Bustamante and Freedom House report that a Newark, NJ based long-distance company, IDT Corp, reached an accord with ETECSA to provide direct international long distance calls.

Google came calling on Cuban blogger and Western media darling Yonai Sánchez in June 2014. She gave the representatives, including Chairman Eric Schmidt, a glimpse into the realities of the Cuban Internet.

> It was a night without technology. No one pulled out a cell phone to check the web-not possible in Cuba...We were very fortunate to be in front of the magic mirror, but she did not want questions or answers, only to describe to him who Cubans are and where we are going (Sánchez 2014).

Other interested ICTs in recent months include Microsoft, Airbnb, and Netflix. The latter two companies’ interest appears to be premature: "’Our first reaction was: “Really?”’ said Northwestern Engineering's Fabián E. Bustamante. ‘As a business model, Netflix and Airbnb rely on most people having Internet access (Morris),’" which is not the case, at least not yet, in Cuba.

Whitefield reports that Sprint, alongside Verizon Wireless, began offering roaming service for its customers visiting the island late in 2015, connecting its service once again to ETECSA. US companies can now do business in Cuba despite the embargo and can sell PC equipment, telecom services, and

assist with the development of Cuba's telecom infrastructure. New regulations from September 2015 would allow "…telecom companies to have a presence on the island through subsidiaries, branches, offices, joint ventures, franchises, agencies or other business relationships with ETECSA, other businesses or individuals (Whitefield)."

American MNCs' interest in the Cuban market is palpable, coming on the heels of the rapprochement of US-Cuban relations and perhaps a final end to the embargo. It is too early to tell what shape these relationships will take. The requirement of working alongside—instead of as an alternative to—ETECSA signals that while the authoritarian island-state is willing to open itself up to infrastructure development guided by outsiders, it is not ready to relinquish control of the media or reduce its limitations on expression and association.

State Policy Regarding Internet Penetration and Use

In the past, Freedom House reports that it was common for some residents to construct their own illegal hookups to the Internet and would serve their neighborhood. These connections served to provide information regarding entertainment and email, and at the behest of the administrators were apolitical in content. They did not provoke the ire of the state until May 2014 when ETECSA's drive for profits led it to root out its competition. While it is unremarkable that the state would seek to aggrandize its own monopoly, it is evidence of the validity Guerra's assessment of what politics and the Internet will be like "after Fidel." Instead of clamoring for the Internet for greater participation in the political process, democratization, or at least criticism of the government, there is proof that Cuban citizens already practice self-censorship. Such a dynamic is unlikely to change quickly in the coming years as the state maintains its hold on the telecom industry.

There are two basic appraisals of the meaning of the opening of US-Cuban relations for the Internet in Cuba. First, is the kind offered by Bustamante, who reported in June 2015 on the increasing tourism (a jump of 35 percent) the island had experienced since the announcement of rapprochement in December. The *turistas* that bring demands for hyperconnectivity cannot be accommodated by the contemporary Cuban infrastructure. As such, the inclusion of foreign ICT firms like IDT and Verizon will be a boon to tourists and citizens alike. Bustamante's conclusion in "Connecting Cuba to the World," was optimistic: "These improved connections and heightened access—both virtual and real—almost as an

unavoidable consequence will help bring real and permanent change to every other aspect of Cuban society." Such a viewpoint misses the persistent power of the state which is an error that cyber-pessimism authors like Morozov would be quick to point out reeks of technological determinism.

On the other hand, Elizabeth Llorente reports that progress in the ICT sector has been hampered by the Cuban government. While there have been strides in increasing Internet penetration, like the Wi-Fi hotspots, they are hampered by the nature of Cuban political economy. US State Department's Deputy Assistant Secretary for South America and Cuba Alex Lee said that "The Cuban government…still clearly prefers to channel all business opportunities to state-run enterprises." There is a push-pull in which the state wants more access but is hampered by lack of understanding of the fundamentals of banking and credit and the desire to monitor who gets access and how it is used. Llorente adds that since both of its greatest protectors—and financial supporters—have dried up, Cuba has little choice but to relinquish some amount of control.

David Adams of *Reuters* reported that according to the US State Department, Cuba has pledged to increase access dramatically by 2020, connecting 50 percent of households and getting mobile phones into 60 percent of the population's hands. Telecom equipment was one of the first exemptions from the embargo after December 17, 2014. The unnamed official stated that Cuban leaders are aware that by denying the Internet they deny people knowledge and "opportunity to grow as an economy and as a people." But the promises of broadband penetration, whether 50 percent or 90 percent by 2020 (if either of those figures are possible), is met with the challenge of the persistence of the Cuban state apparatus. A May 2013 policy statement already sets the boundaries on content; the Internet cannot be used to politically undermine the state: "public security, the integrity, the economy, independence, and national security (Human Rights Watch 2015)."

ZunZuneo

Of all the stories about the Cuban intranet and its relationship to the broader World Wide Web, none is more bizarre and anachronistic than that of US-sponsored microblogging platform ZunZuneo. ZunZuneo was named after the sound of an indigenous Cuban hummingbird, specifically its "buzz," an homage to the 'tweet' of another more famous microblogging platform, Twitter. The project was undertaken by the US Agency for International Development (USAID) that works on development projects

that include infrastructure development and policies that would grow a state's ICT sectors. The Associated Press broke the story in 2014 telling how the covert operation was orchestrated by Joseph McSpedon, a USAID official working for the Office of Transition Initiatives, which was created after the collapse of the Soviet Union. The service would make use of leaked cell phone numbers from an informant at Cubacel and use the SMS platform as a microblogging site for those who could afford cell phones in Cuba (less than 20 percent of the population).

The plan was to hide the existence of the platform entirely from the Cuban government, and to present it to consumers as a genuine business model. USAID sought to cover the plan using "a byzantine system of front companies using a Cayman Islands bank account, and recruit executives who would not be told of the company's ties to the U.S. government (Arce, Butler, and Gillum)." End users would also not know that the US government was behind the buzz. "This is absolutely crucial for the long-term success of the service and to ensure the success of the Mission." The Mission, as it were, was to replicate the experience of Iran, Moldova, and the Philippines, in which Twitter and social media were instrumental in orchestrating serious challenges to the government. It was hoped that by the time the service reached a critical mass, "smart mobs" could initiate a Cuban Spring. Such hopes seemed fruitless, because at its peak its user base was only 40,000, less than a quarter of the number anticipated at the program's outset.

Eventually, USAID, acting through the front of Creative Enterprise, gave up on trying to find a buyer for the service to legitimize it as a real business, and funding dried up for ZunZuneo by 2012. The program was indeed costly, because the service subsidized the costs of the SMS messages, and "…what sane company would take over an operation that involved forking over tens of thousands of dollars to the Cuban government in perpetuity to subsidize texts about the weather or music concerts (Tufekci)?" The only vestige of the service is its Facebook page, pointed out by *Washington Post* journalist Adam Taylor. It contains some of the promised apolitical, entertainment content alongside a slowly increasing coverage of Internet freedom around the world (including the infamous Anonymous image of the Guy Fawkes mask).

Long serving as an instrument of US foreign policy, USAID was criticized for working covertly in Cuba along with several bases in the Latin American and Iberian regions. In Congressional hearings,

Senator Patrick Leahy (D-Vt), who coordinates USAID's budget, said USAID should never be used for regime change. American magazine *Politico* called the plan the "Bay of Tweets," and "bone-headed," not only because of the obvious embarrassment of a failed American attempt at indirect intervention in Cuban affairs, but also the impact it might have on actual Internet activists all over the world and their reputations as legitimate representatives of democratic movements or otherwise critics of the state. The Cuban reaction was critical in tone: Josefina Vida, director of US affairs at Cuba's Foreign Ministry said the program:

> …shows once again that the United States government has not renounced its plans of subversion against Cuba, which have as their aim the creation of situations of destabilization in our country to create changes in the public order and toward which it continues to devote multimillion-dollar budgets each year.
>
> The government of the United States must respect international law and the goals and principles of the United Nations charter and, therefore, cease its illegal and clandestine actions against Cuba, which are rejected by the Cuban people and international public opinion…

Oddly, this episode showed little evidence that the Cuban people saw the Internet as a harbinger of freedom. While Yonai Sánchez may receive a lot of attention in the US and beyond for her critical and at times subversive blog, most Cubans simply view the Internet as an avenue to communicate with family overseas. Ernesto Guerra, a blogger and Havana University student commented that if the platform had begun to become more politically revolutionary in tone, it would have raised suspicions that likely would have been shared among educated Cubans around the country. "If I had started getting subversive messages or death threats or 'Everyone into the streets,"' he laughed, "I would have said—OK—there's something fishy about this. But nothing like that happened."

Instead, ZunZuneo might be a better example of the American foreign policy attachment to norms about Internet freedom and the F2C. Or this episode could serve as an illustration of how misplaced cyber-utopian hopes are about the power of technology to transform politics.

USAID top official Rajiv Shah said that the intention of USAID was "Working to improve platforms of communication is a core part of what USAID works to do," Shah said. "It's inaccurate that [the program] goes beyond that." USAID's blog post claimed that the AP story was misleading, and that there was no intention to overthrow the Communist government, but simply to overcome the "information blockade" present in Cuba (Stampler and Rhodan). What may be true is that while USAID top officials worked to

overcome the information blockade, those on the ground that sought to complete the program may have genuinely believed it to be much more akin to the democratic founts of the Middle East.

Yet those optimistic workers fell into the trap of technological determinism and failed to appreciate the resiliency of state power. The episode is best appreciated as an example of each extreme view of Internet freedom—as liberator or insidious tool of the enemy—writ in miniature.

***

Cuba is a unique addition to this study, but fundamental as a representative of the few states who have chosen to largely leave technological progress and the Internet behind like North Korea and Eritrea. As a small, politically-isolated state, the necessary infrastructure for meaningful access is at best several years away thanks to the recent thawing between Cuba and the US. Havana still excludes access for most unless one can afford to use the navigation halls or Nauta cards, both priced exorbitantly high in order to bring hard cash onto the island. Regime type and political culture are good predictors of Cuba's relationship to the F2C, and the lack of widespread availability and self-censorship will likely survive for many years as Internet penetration increases and the Castro regime becomes part of history.

Iran

Iran has embraced the Internet with reservations; primarily, the state envisions the Internet as a condition for economic growth, and it must filter content based on religious and political grounds. Like China, Iran is pursuing cyber sovereignty norms, but is doing so by trying to protect its Internet users from the outside through SHOMA, a domestic intranet that would be an alternative to the perceived Western-controlled Internet. Unlike any other case explored, concerns about increases in Internet penetration are largely absent from both state bureaucracies and foreign commentators alike. Instead, most concentrate on issues related to limitations on content and violations of users' rights, especially after the failed Green Revolution. Nevertheless, the limited capacity and reliable statistics indicate a state that is struggling to manage the rise of a technology it cannot entirely control.

Background

Iran has a population of 81,824,270 people, ranking 17th in the world and second in the region to Egypt. Over 99 percent of the population is Muslim, of which are 90-95 percent are of the Shi'a denomination. Islam plays a central role in politics and society in Iran and as such affects the way the state sees the Internet. Its area is 1,648,195 km^2 (18th in the world), and is situated at a crossroads among different civilizations with Turkey to West, the Indian subcontinent to the East, and Central Asia to the north. In a radical transformation over the course of a century, 73.4 percent of its population lives in an urban area, with 6 major metropolises with populations of 1.5 million or more[67]. It has the 19th largest economy in the world with a GDP of $1.334 trillion, with a heavy reliance on petroleum and natural gas. This equates to $17,100 GDP/capita, which correlates to a bourgeoning middle class, ranking it 96th in the world. Like Indonesia, the state is heavily involved in the economy, either directly or indirectly. "The Iranian government directly owns and operates hundreds of state-owned enterprises and indirectly controls many companies affiliated with the country's security forces (CIA 2015)."

Looking at its ICT technologies[68], Iran has 30.59 million landlines, ranking 10th in the world; one phone is plugged in for approximately every 38 people in the country. Cellular phones outpace landlines, with 68.9 million in the country, placing it 22nd in the world. Still, such numbers do not equate to the

[67] Tehran (capital) 8.432 million; Mashhad 3.014 million; Esfahan 1.88 million; Karaj 1.807 million; Shiraz 1.661 million; Tabriz 1.572 million (2015)

[68] CIA Factbook 2014

penetration levels seen elsewhere in the world, especially in the archetype states, where in most cities penetration reaches saturation levels. In total, there are 22.59 million Internet users in Iran (which totals approximately 28.3 percent of the population) which ranks the state 26th in the world in number of users, at least according to the CIA. This usage is concentrated among urban residents. Yet like Indonesia, statistical estimates about penetration vary widely and are discussed below.

"Iran entered the twentieth century with oxen and wooden plough. It exited with steel mills, one of the world's highest automobile accident rates, and, to the consternation of many, a nuclear program (Abrahamian 33)." Its modern history requires a disentanglement of sometimes competing forces: nationalism, monarchy, Islam, and foreign interests over its natural resources.

The Iranian Constitution is simultaneously recognizable as a modern instrument of the state and alien as it weaves together mosque and state in a way that is unthinkable for liberals. In Article 2, the document states that the Islamic Republic is a system based on belief in first, "One God" and his sovereignty over temporal domains, and second that God has given divine revelation through prophets and imams so that they might set forth laws (*sharia*) that govern human behavior on Earth. The reliance on sharia is not unique to Iran; eleven countries in the MENA region rely on it for both personal and criminal law, with other countries relying on it for personal law or in particular regions, like Indonesia. Nevertheless, the religious tone of the state colors the relationship with traditional civil rights. Article 3 of the constitution outlines the states' duties, which includes providing free education and using the press to raise public awareness for the attainment of moral virtues. In the same article, it is also the duty of the state to fight both imperialism and corruption and to eliminate poverty. Additionally, the dictates of foreign policy states that the Republic must attempt to establish the "political, economic, and cultural unity of the Islamic world" while being duty-bound to treat non-Muslims with the principles "Islamic justice and equity, and to respect their human rights (Article 14)."

The disconnect between liberal norms and sharia law also appears in the dialogue between Iran and the Human Rights Committee. The body challenged Iran's actions relating to Internet freedom and its incompatibility with the legal mandates of the ICCPR. In its third periodic report (2011), Iran reiterates that civil rights must coexist along the five principles of the Iranian Republic. For instance, "…the constitution considers man as free yet responsible toward God, i.e. the feeling of freedom is to be

attended by a sense of responsibility before God (610)." While there are protections for expression and the inviolability of correspondence, all must be circumscribed by the law that seeks to protect both the security and the religious identity of the Republic.

The HRC took issue in 2011 with the creation of the web-crime unit created two years earlier, which in some form continues to operate today. It asked Iran to comment upon the practice of the blocking of websites after the Green Revolution (CCPR/C/IRN/Q/3). The reply makes the case that *all media* is subject to legal controls in accordance with mandates of public morality and chastity. Additionally, there "is also a serious demand of the people from the Government and the State to stand against those who heedlessly and purposefully violate the rights of people to privacy and disclose their private information." The argument is that those who use the Internet for actions that may embarrass the state or threaten social harmony are validly controlled or punished. The decision to characterize discourse on the Web as part of all media is a unique if questionable argument. To be fair, where the line between an individual and the media begins and ends on the Internet is far less clear than in print or on television, but seeing tweets and edited publications as posing the same danger is fallacious.

The Special Rapporteur Report on Human Rights in Iran reported in 2014 that the situation of human rights on the Web was not improving. He lamented that users were sentenced to a combined 123 years for simple comments against the government posted to Facebook. One user made the comments in Britain, but was arrested upon her arrival in Iran. While President Hassan Rouhani had promised to ease restrictions, 5 million websites remain blocked, many of which are related to the arts and social groups. "In its response to the draft report, the Government noted that it (like many countries) blocks all immoral websites in the arts or social groups."

All rights and duties are constitutionally bound to serve Shi'ism. This sentiment extends to institutions like the press, education, and by extension the Internet. While it is tempting to dismiss theocracy as a veil of the concentration of power among political elites, Shi'ism is a dominant strain in political discourse in Iran. This has had a profound effect on how the Internet has been diffused, what obstacles users face, and what content is available.

The Internet in Iran

Background. Iran began its relationship with the Internet in academia. The Institute for Research in Fundamental Sciences (IPM) in Tehran first brought BITNET to Iran in 1992 through the Trans-European Research and Educational Networking Association, a network similar to UUCP in technical specifications that many states initially used before full connection to the World Wide Web. It established an early domestic network among Iranian universities, IRANET, in 1993. In March 1994 the facility was given the license to register domain names for the state. At the same time, with private modems legalized, it established the earliest full-time Internet connection in the MENA region (Burkhart and Goodman).

Early Internet was largely uncensored and unhindered by the Iranian state. Rahimi (2008) says that restrictions placed on ISPs were largely on paper only. Iranian authorities, like so many others, saw the Internet as a positive tool that would reflect cultural values, a "gift to spread the word of the prophets (43)." Melissa Lerner (2010) affirms this early freedom on the web, commenting that it affirmed "the original ideology of the Islamic Republic as a supporter of modern technology as a means to promote and secure its authority (559)." Lerner's article on virtual social movements in Iran warns that even at that early stage, the Internet should not be considered a panacea. Many theorists like Tilly and Putnam had argued that the Internet may encourage isolation in social movements, but student movements in Iran proved that this was not necessarily a valid concern. More telling for Lerner was the inevitable insertion of the state into the fray, encouraging anti-democratic voices within "Weblogistan" and cracking down on activists.

Repression of virtual dissent did not begin in until 2001, due to the lack of technological knowhow and to economic demands. Rahimi (2003) paints the Iranian attitudes towards the Internet as unique in the MENA region; unlike the UAE or Saudi Arabia, the state actively sought the expansion of its infrastructure (105). Rahimi's hopes that Internet users could challenge the power of the state, however limited, appears quixotic in the face of Iranian reputation today as one of the most repressive states with regards to rights on the web.

> In the words of an Iranian dissident, "At night, every light that is on in Tehran shows that somebody is sitting behind a computer, driving through information roads; and that is in fact a storehouse of gunpowder that, if ignited, will start a great firework in the capital of the revolutionary Islam (111)."

Morozov's analysis is poignant here. While Rahimi acknowledges that one should be careful of attributing too much transformative power to the Internet and the ability of the state to react to challenges to its power on the web, the desire to see the Internet as a legitimate challenger to the state is palpable.

In the initial years of Internet use, speeds were comparable to other developing states. Until 1997, Iranian Internet was limited to 96,000 bps, or approximately 0.09 Mbps. Internet use was dependent on satellite connections with Europe and Canada; in order to improve these speeds the state invested in infrastructure. Sprint set up a sophisticated 2 Mbps connection with DCI, the subsidiary of the state-owned Telecommunications Company of Iran (TCI) that operates the public data network. Seymour and Burkhart report conflict between the state's support of infrastructure development and ideology, and that such conflicts inhibited Internet and other ICT penetration. The state had been worried about the Western "cultural onslaught," exhibiting early evidence for about cyber sovereignty claims, although markedly different from China. While China makes the argument that the Internet is an important setting for the "public opinion struggle," and that it can be used to foster unity and harmony, the concern over content is primarily about the strength of the state. In Iran, the Internet is an extension of the shaping of Iranian identity and the struggle of the Revolution against the influence of its enemy from without, the West.

Internet penetration and geographical divides. Official estimates of Internet penetration in Iran vary greatly[69]. The CIA World Factbook reports in 2014 a penetration rate of 28.3 percent. The same year, the ITU reported penetration at 39 percent, up from 14 percent just five years earlier. Yet, ITU statistics are reliant upon reports filed with the agency by the domestic government agencies in charge of ICT and national statistical offices (ITU 2015b), though the agency claims to verify these numbers, calling itself "the reliable source of ICT statistics."

National statistical sources are even more uneven. The Iranian National Internet Development Management Center (MATMA), a subsidiary of the Ministry of ICT, reported penetration to be 49 percent in 2014. This discrepancy was actually lessened from 2013, in which the center reported penetration at 61 percent of the population. It appears that 2015 is another boon for Internet penetration in the country,

[69] This is problem is acknowledged by Pourghadiri (2014) and Rahimi (2015).

with a news report from the *Islamic Republic News Agency*, an official government-run newspaper, reporting penetration at a whopping 82 percent! "By the end of 21 June 2015, the number of the Internet users in Iran reached 61,709,929 with the Internet connections at 43,026,279 (IRNA)." While they report that dial-up connections were still in use (approximately nine percent of all connections), broadband expanded to nearly half of all Internet users by September. The tendency to exaggerate official statistics in not unique to Iran— Indonesia is said by various sources to do the same. The desire for states to do so is not certain; speculation points to attempts by the state to appear to be able to provide services at rates that the public might expect, or to exceed those expectations.

Similar to the difficulty of finding national statistics, information on Internet penetration within Iran is difficult to discover. Iranian official statistical agencies appear to be missing vital statistical reports, and ISPs like the Telecommunications Company of Iran is particularly opaque. Admittedly, part of the problem is language but cases like China and Russia where both the language and script are different, information is simply more widely available. The statistics on provincial penetration rates are only available second hand in the form of the Iranian Students News Agency, run by university students with funding from the government. Their findings are reproduced in Table 16.

Table 16 Iranian Internet penetration by province
(Iranian Students News Agency 2013)

Province	**Internet penetration**
Mazandaran	83.85%
Tehran	78.55%
Esfahan	70.48%
Khuzestan	68.4%
Semnan	65.45%
~~	
Lorestan	43.89%
Sistan and Baluchestan	41.77%
Kerman	40.79%
South Khorasan	39.82%
North Khorasan	39.57%

The chart is remarkably consistent. Mazandaran Province likely enjoys relatively high levels of Internet penetration due to its location on the Caspian Sea which makes it a good location for tourism and supporting the oil industry. The least penetrated provinces like the Khorasan provinces and Kerman are landlocked and primarily agrarian. Theses provinces are also among the most ethnically diverse in Iran,

so the lack of ICT buildup might be a reflection of overall development disparities in the country, but this is conjecture because these types of inconsistencies are seldom addressed in the media or official literature. Nonetheless, disregarding the top five provinces, the gap of only 25 percent between the least and most connected provinces is suspect. Most large states must combat physical and economic hurdles to ICT development. First, geographic barriers pose physical limitations to spreading infrastructure across large swaths of land. Mountain ranges crisscross Iran along with vast desert regions. Second, states must often prioritize infrastructure development for communities that would immediately benefit from sophisticated Internet access, including areas with major cities or those connected to global trade. Combined, these conditions—which are not absent in Iran—make such uniform penetration rates unlikely.

The only other mention of domestic Internet penetration rates comes in the form of a news report from the Mehr News Agency, a quasi-independent organization that is owned by the Islamic Ideology Dissemination Organization, which is part of the Ministry of Culture. In its December 2014 report, the ICT Minister for Iran Mahmoud Vaezi promised to connect 30,000 villages to broadband Internet by the first quarter of 2016. Currently, 97 percent of villages have at least one landline, and so the goal of delivering to so many villages is not without precedent; recall in the Russian case, connections were being built alongside preexisting transportation infrastructure. The goal of getting fixed lines to villages with 20 houses or more is possible, but the accuracy of these claims absent reliable data is hard to ascertain.

How can these disparities be accounted for? The questions appear to mount when attempting to assess Internet penetration in Iran. Why are there such discrepancies between the CIA, ITU, and Iranian ICT Ministry total figures? Why do national statistics vary so widely from year to year? Are the provincial totals anywhere close to accurate, or are they either fabricated deliberately to make the state look good or out of an inability to properly assess Internet access? The possible answers come from Moheballi, Shirazi, and Bazargan (2013), who regularly report on Iranian ICTs to the ITU in their World Telecommunications/ICT Symposiums. In the most recent report, they discuss the main challenges to ICT measurement in Iran:

- Lack of a model or conceptual framework for defining indicators in policy documents
- Unclear and ambiguous definitions of national indicators
- Unacceptable level of awareness and communications among stakeholders
- Lack of updated and exact data
- Lack of technical capacity for ICT measurement
- Governing body for ICT measurement
- Lack of enough financial resources in the responsible organizations
- Security and privacy issues
- Lack of coordianation among stakeholders, special ICT statistics users
- Unacceptable level of timely and exact reporting to international bodies
- Low importance of ICT measurement in government organization and private sector (Moheballi, Shirazi, and Bazargan)

Fundamental problems like the lack of communication among various stakeholders, the lack of expertise in gathering ICT statistics, and the disregard of the importance of measuring ICT performance all point to the inadequacies of the available statistics through the DCI and news agencies like the Iranian Student News. It is necessary to treat any statistics provided by the Iranian government with suspicion. Whether the Iranian government is intentionally trying to fool its population or the rest of the region with inflated numbers is merely conjecture, but it may be that combined with the fact the unintentional reality of having no reliable means of providing such information.

Speed and cost. Freedom House (2015) reports "painfully slow" connection speeds that compromise meaningful access throughout the country. Peak speeds are among the lowest in the world, capping out at 6 Mbps for download, whereas average speeds are much lower. Political pressures from the state have limited speeds for a long time. In 2006, the state arbitrarily imposed slower connections for home Internet users, capping speeds at 128 Kbps. The fear was articulated by an aytollah in a call to revoke the mobile Internet licenses before young minds could be poisoned by "dirty pictures and clips (Edbrink)." This cap was recently lifted and in 2014 increased to 10 Mbps, still notably 40 percent less than the FCC minimum for broadband in the US. Akamai has nothing to report on Internet speed in Iran, while testmy.net reports an average of 1.6 Mbps downstream and a mere 355 Kbps upstream. Clerics are divided between the scientific, and undoubtedly commercial, opportunities for meaningful access and the issues over cultural and political challenges to the status quo.

Reported speeds reveal that while speed caps may have been officially lifted, users experience poor speeds that are slower than even the Russian Far East. One has to go to Arctic Circle to find anything comparable in this study.

Table 17 Reported Internet speeds in Iranian cities
(testmy.net 12 April 2016)

City (Province)	Downstream	Upstream
Isfahan (Isfahan)	1.5 Mbps	395 Kbps
Karaj (Alborz)	1.5 Mbps	430 Kbps
Tehran (Tehran)	1.4 Mbps	342 Kbps
Shiraz (Fars)	1.3 Mbps	364 Kbps
Tabriz (East Azerbaijan)	746 Kbps	238 Kbps
Ardebil (Ardebil)	618 Kbps	337 Kbps
Kish (Hormozgān)	566 Kbps	182 Kbps

Outside of important cities, speeds are largely below 1 Mbps, below the standard for viewing most webpages in 2016. TCI holds an effective monopoly over bandwidth, and resells it to public and private small ISPs at rates eleven times their own cost (Freedom House 2015 427). For example, the cost of a 10 Mbps connection is $79.9 per month in 2016 (Numbeo), almost twice of all other utilities of a typical apartment combined, at the highest percentage of salary in this study besides Cuba, at 16.99 percent. A 2/1 Mbps connection with unlimited data transfers to Pars Online, Iran's second largest ISP, would cost a user $131 per month, far exceeding comparable plans in the US.

Iran is nevertheless praising its increased access, mainly through mobile technologies. IranCell, a subsidiary of TCI, claimed to have 12.5 million 3G subscribers covering 35.8 percent of the population in all of the provinces. 4G is being rolled out as well with coverage in 82 cities. This report was filed with the ITU, and therefore is mostly dependent on reports and statistics provided by TCI itself, and is therefore questionable.

Internet Service Providers

The state is increasing connectivity, both through landline connections and through smartphones, though to what degree is uncertain. Yet the meaningfulness of access is hampered by capped speeds, the filtering of content, and the quasi-monopoly of ISPs. Iran's mixed economy is characterized by a large public sector and a heavy reliance on oil and natural gas; as such, the telecommunications market operates largely at the behest of the state. The Telecommunications Company of Iran (TCI) is the main provider of the Internet and sells bandwidth to other ISPs. While privatized in 2007, TCI is owned primarily by the Iranian Revolutionary Guard Corps.

In 2015, Tehran announced the licensing of at least twelve new mobile providers through MVNO platforms that would compete with the IranCell and MCI. Raad reports that the addition of these enterprises would further incentivize badly needed infrastructure upgrades that the established companies had been undertaking since 2014. "[MVOPs] would ultimately give the freedom of choice denied until recently to Iran's consumers." Such sentiments have sufficient reasons for optimism, as they would spur competition and infrastructure development. Yet, like all MVOPs, these new providers would purchase airtime/bandwidth from established mobile providers, all indirectly controlled by the state.

As ISPs have been privatized as a result of a five-year plan by the government, they are still heavily controlled by the state. In the past, the OpenNet Initiative reports that ISPs were put charge of filtering content that was deemed inappropriate by the state, but enforcement was not uniform. Since then, they have developed more centralized filtering systems that bypass the ISPs' control. All cybercafés must monitor users, including using closed-circuit television surveillance and are forced to use bandwidth provided by the state or route traffic through Iranian government-made filter boxes. Moreover,

> Website owners must register their sites with the Ministry of Culture and are then subject to requests to remove particular posts deemed unacceptable by the government. The 2009 Computer Crime Law (CCL) makes service providers, such as blogging platforms, responsible for any content that appears on their sites (Freedom House 2015 432).

Iran places the onus on controlling content partly on the middle men, so that despite privatization, the state is still very much in control.

SHOMA: An Iranian National Information Network

Most Western media outlets are primarily concerned about the development of a unique, domestic network that would exist alongside the global Internet if they show concern about the issue of access in Iran. Having gone through several iterations, SHOMA is a national information network that was first conceived in 2006 by the Iranian cabinet as part of the fifth Five-Year Plan. It was to be developed three stages: first, establishing an independent network that separated local and global traffic for all government installations and in all provinces; second, moving all Iranian websites to domestic servers; and third, establishing domestic equivalents of familiar services, including an operating system, email, and search engine.

> SHOMA is a network not unlike the Internet - its infrastructure consists of switches, routers and data centers. If users request data located on a data center inside the

> country, their traffic will not leave the country, and will remain inside the network…SHOMA is intended to be a private and secure internal network (Small Media).

The national network would look much like its broader counterpart, but its purpose is threefold, reflecting the dynamic relationship the Iranian state has with the Internet. First is the theocracy's desire to establish an *Internet-e-Paak*, or a "pure Internet" that would not require the close monitoring that current Internet use does. Second, having a domestic Internet would allow the state a defense against cyber-attacks. The validity of this belief is questionable, considering that global traffic will run alongside the network, presumably using at least some of the same equipment. Any vulnerabilities to the global connection points could therefore make SHOMA susceptible as well. Third, the state claims that the network would be faster and more reliable than what users currently enjoy. By blaming poor speeds on connections on hardware over which the state has no control, it appears that Tehran is attempting to pass blame for their speed caps and poor service on the lack of domestic controls over the technology. Particularly, it promises that 60 percent of families in Iran would have access to SHOMA at 20 Mbps, speeds that far exceed the average speeds enjoyed by netizens today.

Since its announcement in 2006, Iranians and outside commentators have raised concerns about what SHOMA would mean for increasing the state's control over access. Not only would the service be limited to Iranian-hosted websites, the greater control of the state over networking equipment could mean that the state could shut off access to both SHOMA and the Internet when it was deemed necessary, while keeping the administration's connections intact. It might also mean that monitoring users would be made far easier.

Reza HaghighatNejad provides the latest update on the "Halal Internet" in February 2016[70], a name that mostly Western journalists have given this concept in a bit of satirical commentary. HaghighatNejad claims that the project really dates to 2003, and much like many other aspects of ICT in Iran, figures on funding and completion dates widely vary and are unreliable.

> Nasrollah Pazhmanfar, a hardliner MP and a former member of the Supreme Council of Cyberspace, said the government expects the project to be completed within 11 years — figures that fly in the face of statements issued during the end of Ahmadinejad's presidency, which boasted that the project was 90 percent complete.

[70] HaghighatNejad writes for IranWire, a "joint venture" of Iranian journalists in the diaspora. Highly critical of the government, any insights must understood within the context that has a high potential for bias.

HaghighatNejad claims that the intranet is still in the “PowerPoint phase” and that the concerns that the SHOMA could replace the WWW are at best more than a decade away. Nevertheless, the article also reports upon throttling of the Internet ahead of parliamentary elections and other measures the state regularly takes to control discourse and access to the web. It would not be surprising if SHOMA was simply a proposal that has yet to find the political will to find expression, but nevertheless it does not appear to be simply a dream never intent to be brought to fruition. Steps that the Iranian government has taken after the sanctions have lifted, including meeting with ICT officials from other Not Free states, signal that that an Internet-e-Paak is still in the works, even if it is years away.

The pursuit of an alternative network to run parallel to, and at times instead of the Internet, speaks to the cyber sovereignty norm in important ways. First, there is the technological nationalism element that is common to other proponents of the norm like China and Russia, which seeks to replace perceived dependency on foreign technology by pursuing national alternatives. ASL19, an NGO working to subvert content filters in Iran, explains that the national network is highly tied to conceptions of cyber security. As Richard Clarke explains in his somewhat hyperbolic text, *Cyber War* (2012), one of the acute dangers of conflict in the Internet-dependent age of commerce is that foreign production of hardware and software leaves users vulnerable to attacks because of mistaken or intentional programming errors. Tehran in part justifies the pursuit of SHOMA on this basis, claiming that “’it is a national need that this network is constructed as expeditiously as possible,’ [Mohammad Hassan Entezari, head of Supreme Council of Cyberspace] said (ASL19).” Additionally, the pursuit of SHOMA and cyber security measures also promise to improve Iran’s IT industry in general, potentially employing thousands and catching the Iranian economy up to global standards.

Second, this domestic network is taken on for the express purpose of making sure the content lives up to Iranian cultural standards. While Russia, China, and Cuba all proclaim that they use the Internet rhetorically to promote party propaganda and social harmony, the Iranian vision is different. Tehran sees the Internet as useful for the proclamation of Islamic principles that would impact citizens’ daily lives. At the same time, SHOMA would help to minimize or eliminate dangerous outside influences. This goes beyond the Chinese use of the Internet as a propaganda tool, and is part of Iran’s view of its place in the world. Since its inception, the Islamic Republic has taken its anti-Western ideology as part of

its mantle, and their view of the Internet as an extension of that influence is hardly surprising. The agency that the state takes in creating their nation-states' culture means that at its fullest expression, the Internet must be part of this vision.

State Rhetoric Regarding Internet Access and Use

Through the Mehr News Agency, and presumably other news outlets, Tehran reports on its progress in freeing itself from technological dependence. Events in 2015 center around further strides to technological nationalism and new foreign partnerships that would assist the state in reaching that goal after many economic sanctions being removed.

The year began with a report of the launch of domestic search engine, Yooz. Persian for cheetah, the project is meant to improve speeds and security, and is especially designed for searches conducted in Persian. The impetus is clearly techno-nationalist in tone: "Mehdi Naghavi said Google was gradually turned into the 'spine of the internet usage' and the Iranian project will help in crawling out of the compulsion (Sridharan)." By developing alternatives, Iranian netizens would not be subject to foreign sanctions on the web and removing hurdles that academics currently face, but no articles specified what that meant. Parsijoo is another Iranian search engine that launched in November and is rumored to include an email platform, downloadable content, local directories, and e-commerce applications. Like Yooz, it is meant to replace the public's dependency on platforms like Google, and the *Financial Tribune* reports that limited broadband availability and technical complexities had hampered the progress of both.

In June, Khamenei issued the sixth Five-Year Development Plan. He predicted an eight percent annual growth rate in addition to the establishment of SHOMA. He claimed that he would be expanding content fivefold while simultaneously engaging in "intelligent filtering" and "targeted participation" in cyberspace. The Ayatollah envisions aligning citizens' experience in cyberspace to the cultural vision of Iran itself. By November, it was reported that Iran hosted the most websites in the Middle East, ranking the state 4th in the world. The shift from foreign to domestic hosting is a consequence of state policy to encourage technological nationalism and cost-efficiency. Domestically hosted websites also are advantaged, apparently by state policy, by being directly connected to IXP ports, theoretically bypassing some of the slowdowns inevitable with distance and being routed several times over an infinite expanse.

Even more evidence for the cyber sovereignty norm is to be found with two high-profile meetings between Iranian officials and other prominent states that are proponents of the norm. In June, ICT minister Vaezi met with Miao Wei, his counterpart in China. The meeting's purpose was twofold: first, it sought to reassert that cooperation would be necessary to overcome some of the influence of foreign technology in domestic spheres (particularly the US); and second, it signaled a partnership between Iran and China in completing SHOMA. They agreed to form a special working group to operationalize the task. In October, Vaezi met with Russian counterpart, Nikolai Nikiforov, primarily to discuss the norms of cyberspace sovereignty but also some business opportunities. Vaezi reports that:

> …during the meeting we discussed a wide range of topics including the breaking of US monopoly on internet, cooperation on research and development, information security mechanisms, developing and strengthening domestic social networks and the opening office of Russian search engine Yandex in Tehran for easier access.

It is a curious thing that Iran makes such extensive claims for cyber sovereignty but fails to see the irony in introducing more foreign technology like that of Russia's search engine.

Domestic attitudes toward the Internet in Iran are hard to come by, especially quantitative survey data. The only available data is the Kull et al. survey from 2008. Support for press freedom was among the weakest in the survey, with 65 percent arguing that the news agencies should be free from government controls, 45 percent saying the government should be able restrict access to preserve stability, and only 32 percent arguing that should be able to read whatever they want on the Internet.

***

As the final case in the Not Free category, Iran exhibits some of the characteristics that typify Internet policy in both China and Cuba. Many of the policies that the state undertakes to limit penetration and meaningful access are done in the name of the maintenance of social harmony. Unlike China, its political identity as an Islamic state colors censorship and surveillance policies differently for Iranian users than for Chinese. While both states advocate for cyber sovereignty norms, Iran is more virulent in its attacks against the corrupting influence and intentions of the West and the US in particular. Like Cuba, Iran has experimented with ways to make access less meaningful (by slowing speeds) and pursuing its own intranet. While it seems the SHOMA is no more than a policy goal as of 2016, the intention behind the Internet-e-Paak is an obvious challenge to the F2C. Nevertheless, within the Iranian constitution and its dialogue with the Human Rights Committee, it must frame these as deviations rather than alternatives

to Internet freedom. For instance, the SHOMA is framed as something necessary to make the Internet safe for Iranians, thereby implicitly recognizing that Internet access is necessary in the 21st century, albeit with conditions.

Chapter 7: Comparison and Discussion

This chapter will proceed in two parts. First, comparisons will be drawn among the cases, discussing the responses to the F2C norm; these findings are summarized in the Appendix. Second, these findings will be discussed in relation to this study's contribution to IR theory, addressing the limitations inherent in its methodology, and suggesting areas of future research.

Demographics and History with Complementary Rights

Most of the cases observed are large, powerful states according to population, size, and GDP. The three primary cases are among the top ten in the world according to land mass, population, economy, and number of Internet users, with the US and China in the top three for each of these measures. Every case besides Cuba has had to overcome geographic problems that inhibit technological penetration and use amongst its population that in turn exacerbate existing inequalities. The US, China, Russia, Brazil, Mexico, and Iran have struggled with urban-rural divides, with each state other than China having about 75 percent of its population living in cities. Traditionally underserved areas—from tribal lands in the US, to the Far East in Russia, the interiors of China and Brazil, and the farmlands of Mexico and Iran—have lower rates of penetration. This fact is aggravated by the presence of ethnic minorities, which traditionally have less political power and cannot make significant demands on the state or the private sector.

In regard to culture, ideology, and political history, the US, Russia, and China share few characteristics with each other or any other states in this study. The US, former colony turned colonizer, has a long history struggling to reconcile civil rights with political expediency. While the early 20th century saw limitations on speech as a result of the specter of war, the right of the state to restrict expression was more narrowly limited under the premise of the likelihood and immanency of threats to security. Terrorism has challenged the status quo of rights in the US, and the law is slow to react to developments in technology that federal authorities have used in the name of security. Economic ideology has meant limited options for state involvement in infrastructure development or as a provider of Internet access.

Russia's limitations on civil rights reach back to its early modern history and it has struggled deciding its identity as either European or Asian. The authority of its various governments has been legitimated through the pursuit of power and greatness, and not by the consent of the governed, and has

resulted in a troubled relationship with democracy and the balancing act between freedom of expression with stability and security. The Polity data set labels Russia as an anocracy. While its history of communism has led perhaps to an easier acceptance of the role of the state in the provision and extension of access through Rostelecom, the state often justifies its Internet limitations through the frame of cyber sovereignty and responding to the perceived threats posed by the United States.

China, like Russia, has a history with communist rule dating to 1949, and like Russia, its relationship with the most important manifestations of state-run communism ended by the 1970s. Unlike Russia, China is more easily labeled authoritarian, due to the overwhelming and unchecked power of the Chinese Communist Party. While there had been some minor experimentations with civil rights within the early 20th century Chinese nationalist movement, rights and duties are seen in Chinese politics through the lens of communitarianism and social hierarchy. The state justifies intervention into Internet use in terms of stability and unity. Increasing access is pursued for economic development. At times the government will also frame the issue in terms of equity and to improve the responsiveness of government, but not for purposes of expression, association, assembly, or privacy and expressly against anything that might disrupt order.

Brazil and Mexico share many characteristics. Each is a powerful leader in Latin America, but the former has double the population and is four and a half times larger geographically. Each has a long history of colonization and achieved independence in the 1820s. Their post-independence histories are characterized by tumultuous politics, dealing with ethnic disparities and populism, a series of military coups and dictatorships, and finally the resurgence of democracy, though this took place earlier in Mexico than Brazil. Each of these states has struggled with realizing the ideal of civil and socioeconomic human rights. The 20th century was characterized by undemocratic systems, in Brazil by a bureaucratic military regime, and in Mexico by the one-party rule of the PRI. Each state continues to struggle with living up to ideals embodied in its constitutions because of structural inequality and political malfeasance.

The Philippines and Indonesia also share many characteristics. While the Philippines is smaller in all measures with one third of Indonesia's population, only 16 percent of its geographic area, and a GDP that is 74 percent smaller, their cultural characteristics, political histories, and problems with penetration mirror each other. Both are archipelagos with thousands of islands that have disproportionate

populations scattered among them. Each has cities with high concentrations of educated, middle class digital natives and islands that have been traditionally underserved by technological advances. Their urbanization rates are 44 percent and 54 percent, respectively. Both are located in Southeast Asia with an extensive history of outside influence from various sources: China, India, Arabia, and various European nations. Each have Muslim populations, with Indonesia having the largest Muslim population in the world, and both have fundamentalist populations that have demanded more autonomy. The Philippines' struggle with Muslim fundamentalists in Mindanao is conflictual and violent, while Indonesia has accommodated demands for sharia law by having a semi-autonomous province located on Sumatra.

Both were colonized by European powers, but for the Philippines Spanish rule was replaced by American, which explains the prevalence of English, while Indonesia was ruled throughout its colonial history by the Dutch. The Japanese held both archipelagos, in different manners, during WWII, and both had unstable democracies during the 20th century sharply punctuated by one-man rule over the course of many decades. As a result, both states endure the legacy of patronage and corruption that in some form continue to be manifest today. Both must deal with ICT companies entrenched within the state, and have to varying degrees attempted to overcome these limitations.

Cuba and Iran are the outliers of this study, partially by design. Both states are well-known for their restrictions on Internet use and the manner in which they limit access, engage in censorship, and monitor their citizens' Internet usage. Beyond this, both have historical legacies that are punctuated by American intervention into domestic politics that have dramatically shaped their outlook on international relations and the Internet. Both, too, have rhetorically supported socioeconomic rights. The manifestation of these rights, however, have taken on cultural or political peculiarities. In Iran, the centrality of Shi'ism after the Revolution has meant that all duties and rights are centered on the belief in "One God," and that media, including the Internet, should conform to the demands of religion and the stability of the state. The belief may eventually result in the creation of an Iranian intranet that would once and for all rid Iranian netizens from the disrupting influences of the larger World Wide Web. The importance of Cuba's Revolution to its Internet use also should not be forgotten. While Cuba is undergoing a liberalization of sorts with the slow dismantling of the US trade embargo, so far the state has held the reigns to the Internet close.

Characteristics of the Internet

The US was the earliest to adopt the protocols that have become synonymous with the Internet, having invented both the Internet's precursor and the protocols themselves. TCP/IP became the networking standard in 1985, and was adopted during various years between 1990 and 1996 for by of the other states in the study, with Cuba being the final adoptee. In eight of the nine cases, networked computing was first to be found in academia, which sought to bring sophisticated computing to various domestic college campuses and to link research projects across the globe. During the Cold War, the US and the Soviet Union both pursued networking or cybernetics through the military, either to enable communication in the case of a nuclear attack or to efficiently monitor its industries. ARPANET would ultimately give birth to the online bulletin boards, email platforms, and the World Wide Web, but due to idiosyncrasies in Soviet politics, cybernetics never developed beyond competing networked systems across Russia. The Philippines relied on IBM to set up its connections, likely as a result of cronyism. Cuba is unique case in which Internet adoption relied on a state-run institution, CENAI, with an overseas affiliate. While it had a computing sector dating back to the Batista regime, the industry never developed, likely in part due to the failure of the Soviet Union's own cybernetics industry.

The reliability of Internet penetration rates and the baseline measurement of access vary from case to case. Iran and Indonesia's own estimates vary dramatically from the CIA's, with a range of 12 percent to 54 percent difference. Other estimates usually vary less than 5 percent, but there is no standardization of practice. The variance is likely a result of capacity gaps and the degree to which the national governments have set up routine, reliable measures of access throughout their territory. Penetration rates range from 16 percent in Indonesia to 87 percent in the US, with the average of the selected cases around 44 percent. Free states have higher penetration rates than all others, and Partly Free more so than those in the Not Free categories: the US (86.8 percent) is higher than Russia (53.4 percent) and in turn higher than China (46.0 percent), Brazil (53.4 percent) is higher than Mexico (41.1 percent) and Cuba (27.5 percent), the Philippines (39.4 percent) higher than Indonesia (16.7 percent). As Pew (2014b) has noted, there is a strong correlation (0.76) between Internet access and increased demands for Internet freedom.

Despite the fact that mobile Internet may become problematic as it is adopted at higher rates, many states see mobile access as an alternative to fixed Internet. Each of the cases studied other than Cuba is ranked in the top 15 states in terms of mobile penetration figures with China, the United States, and Indonesia leading in absolute numbers. When calculated as a percentage of population however, Russia, Brazil, and the Philippines lead all other cases with rates exceeding saturation levels. Smartphone ownership is not as frequently recorded, but as consumers replace aging technology, smartphones are the popular choice. Zuckerberg notes that while smartphone adoption may be climbing, full use of the technology remains out of reach for many due the high cost of data plans. This was the impetus for Facebook's zero-rated Free Basics plan.

In its various forms, the digital divide is pervasive throughout this study. As noted above, a primary cause is geography. In the US, Russia, China, Brazil, Mexico, and Iran large swaths of rural, underpopulated land has made necessary infrastructure for access and broadband prohibitively costly. Similarly, the thousands of populated islands that make up Indonesia and the Philippines make it financially difficult for fixed infrastructure to be installed on remote locations. For the private sector, such investments without the promise of short-term profits leave little motivation for companies to take on the cost alone. The World Bank calls broadband a "club good," that requires intervention, generally from the state, in order to create conditions that make fair distribution possible. Each of these cases has adopted a different combination of methods to counteract the geographic divide. Many states and netizens see the problem of the digital divide through the lens of equality and a right to access (the US, Brazil, the Philippines, Mexico, and Indonesia). The impetus for China and Russia is primarily economic, framing the problem of the digital divide as lost economic opportunities and often cite statistics such as that a 10 percent increase in access leads to a 1.5 percent rise in GDP. Iran has a troubled relationship with access, with the history of capping speeds and maintaining high costs through its quasi-monopolistic, state-owned ISPs. Its SHOMA project, which would provide safer, faster, and reliable Internet, would limit content in order to create an "Internet-e-Paak" that would be in line with fundamentalist Shi'a.

Other manifestations of the digital divide have been addressed sporadically in each of the countries. The socioeconomic divide has been addressed through programs and legal instruments like ConnectforGood, HUD, Mexico Conectado, and the Marco Civil da Internet, recognizing that access is

problem of human rights and social justice. The provision of access furthers goals including equality of opportunity in areas like education and employment. The Philippines and Indonesia have indirectly dealt with the issue of unequal access while addressing the geographic divisions in their respective archipelagos. For instance, the Palapa Ring Projects are meant to bring greater access to regions traditionally unserved by infrastructure development. These islands also are home to greater proportions of impoverished citizens, but the project is undertaken in the name of equality of opportunity and the modernization of infrastructure and is not explicitly framed as a problem of social justice. The only other state to directly tackle this issue is China, claiming that increasing Internet penetration will lead to social progress in addition to growing its economy. Such language is indicative of China's communist ideological identity, which has long justified the state's authoritarian measures and restrictions on civil liberties by claiming that it is helping the masses. Whether the state plays this role sincerely is another matter, but the framing of the issue of access in this way is indicative of its ideological context.

Speed and cost are other defining characteristics of the meaningfulness of access. The US and Russia have the highest average speeds of this study, with 14.2 and 11.6 Mbps download speeds, respectively. The average speeds for all remaining cases, besides Cuba, are 5.9 Mbps or less, and are largely a determination of the availability of infrastructure and the structure of the ISP market. Costs for fixed line connections vary greatly in each case, with five cases at or below the UN's baseline of a connection costing less than 5 percent of a user's average monthly salary. In the cases of the Philippines and Indonesia, exorbitant costs are a consequence of the market, especially in the former. Duopoly has plagued the Philippine telephone and ISP markets; potential competitors to the entrenched providers are hindered from driving costs down because of the lack of peering and other policies. For Iran and Cuba, high costs are a consequence of state policy to control users. The Iranian state has had policies in place to discourage meaningful access, including controlling prices and through speed caps that limit Internet use. The prohibitive costs associated with Internet use in Cuba is partially related to limiting the number of Internet users, but is also motivated by the desire to bring hard currency into the island's economy.

Internet Service Providers and their Regulation

The relationship between the state and industry is one of the main manifestations of a nation's political economy. In the case of the Internet industry, the ISPs' identity, the level of competition, and

their relationship with the state dictate the manner and quality of Internet access. States that encourage competition, as in Brazil, find that access is widened with increases in efficiency and competitive pricing. In all three of the archetype states examined, power is concentrated asymmetrically, in the private sector in the US, and with the state in both Russia and China. Access is thereby hampered by limitations in the market or the goals of the state.

While ISPs are private in the US, the market share is concentrated among five national providers who wield enormous power in deciding coverage areas and influencing the policies that regulate them. The FCC has been battling ISPs since 2007 over issues like net neutrality and zero-rating schemes. It has only recently established itself as a legal regulator of the Internet under Title II of the Federal Communications Act (1934), and the FCC continues to be seen as the underdog in this arena. ISPs also challenge efforts that may help bridge the digital divide. They commonly undermine municipal broadband projects by arguing that they would artificially hamper competition and successfully advocate for laws against them. They have also argued against the low-cost provision of fiber by Google in low-income areas, again claiming that they would lead to unfair competition. The role of the state in the American economy is generally seen as suspect by citizens and business alike. Additionally, whether true or not ICT professionals in the US have long believed that the industry produced innovation with fair pricing without intervention from the state, and so by definition the FCC is seen as a burden rather than a boon.

Unlike in other areas of comparison—demographics, the nature of the digital divide, and policies aimed at increasing access—states with similar political culture do not share similarities in their respective ISP markets. The Philippines and Indonesia both have hybrid marketplaces with some mixture of private and public ownership, but the Philippines is characterized by one powerful player, the heavily state-connected PLDT with 70 percent of the fixed Internet market and 52 percent of the mobile market, with Globe making up a large portion of what remains. The Philippines' regulatory agency, NTC, while charged with creating a more competitive marketplace, has remained weak in the light of entrenched interests and cronyism that continues to characterize the relationship between the PLDT and the state. Indonesia's market enjoys healthier competition among multiple players, though small and medium ISPs do not provide sufficient competition that could improve prices or speed. This is a consequence of the idiosyncratic development of the Internet and marketplace in each state's history, with the APJII

instrumental in the introduction of Internet infrastructure in Indonesia in the late 1990s. Its regulatory agency has been challenged due to high licensing fees, but retains more power over its ISPs than its Philippine counterpart.

Brazil and Mexico's markets are similarly varied. While both are entirely privatized, Brazil's is characterized by a diverse range of players, with several nationwide ISPs like Embratel and Telefonica and many medium and small ISPs serving distinct locales. Brazil's telecommunications regulation agency, Anatel, has worked to increase access through the CGI.br, consultations for the Marco Civil da Internet, and coordinates the licensing of small ISPs to bring services to underserved areas. Mexico's América Móvil controls 80 percent and 70 percent of the fixed line and mobile markets, respectively, with the next biggest competitor, Axtel, controlling just 6 percent of fixed Internet subscriptions. Brazil's diverse market has been a matter of policy, engineered by tax breaks and financial incentives, and the Mexican state has only recently begun the process of dismantling Slim's empire through IFETEL, whose powers were not concretized until July 2014. To date, the anti-trust body has only declared América Móvil to be the dominant provider in violation that no one company can control more than 50 percent of a given market. Mexico is moving in the direction of Brazil, but it will take many years to dismantle the engrained power of a company owned by one of the richest men on the planet.

Russia's ISP market is shifting. In its early years, Internet providers were numerous, perhaps as a consequence of shock therapy and the rapid privatization of many industries ushered in by the collapse of the Soviet Union in the 1990s. Since then the Russian government has enacted policies that have forced ISPs to comply with policies that are financially burdensome and that enable the state to monitor access and censor content. Owned by the state, Rostelecom is the main provider of access and is the institution that is pivotal to decreasing the digital divide. The Ministry of Communication and Mass Media regulates the industry and is appointed by executive decree, much like the US, but in Russia such controls are more important. The centrality of economic and technological modernization above concerns for liberal values play out in the Russian ISP industry and its limitations on access and users' freedoms. Additionally, the state has asserted itself in other ways into the industry, requiring providers to employ expensive monitoring equipment and their existence being subject to the state's discretion.

China's curious economic structure is apparent in its ISP industry. Nominally communist, China's economy is state-controlled yet simultaneously subject to market conditions. Inefficiencies in the ISP market resulted in the filing of an anti-trust suit by the People's Congress and forced its decentralization in 2008. While China Unicom, China Telecom, and China Mobile must now compete with each other for customers, all are still directly responsible to the state for carrying out all of its restrictive policies on use and content. Combined with state-owned IXPs and backbones, these moves assure the state continues to have direct control of the Internet. As with all the cases in the Not Free category, the engine of regulation, the CNNIC, is directly tied to the authoritarian state and has little independent influence on policy making.

The other Not Free states' ISP markets are also highly centralized. Iran's TCI is not directly state-owned, but its majority shares are controlled by the Revolutionary Guard, which may be a matter of happenstance rather than evidence that the private sector having real control over the market or that possibility becoming a reality anytime soon. After all, Iran's economy is highly dependent upon the public sector, and it is reasonable that the state would desire to retain control of such a vital industry, even if indirectly. Cuba's ETECSA is directly owned and operated by the state. New services brought by American providers are concentrated in Havana, and it has been signaled that these will be given in conjunction with rather than in competition with the state. Despite rapprochement, the state's control over the market is likely to remain airtight.

Efforts to Increase Internet Penetration and Bridge the Digital Divides

One of the demands of the F2C is that by claiming citizens have a right to access the Internet, the state is obligated to assist in the provision and spread of that access. The means adopted by each of these states have been dependent on political culture and the nature of each case's political economy. States in the Free and Partly Free categories have adopted a wide range of policies aimed at increasing Internet penetration, often partnering with the private sector to find innovative solutions to geographic or socioeconomic causes of unequal levels of access within their state. As the sole providers of access, states in the Not Free category have no such partnerships and included plans to increase access within the larger schemes of economic development.

National Broadband Plans. In providing blueprints for states to increase access, WSIS recommended in 2003 that states develop "forward looking and sustainable national e-strategies (11)" in consultation with the private-sector and civil society. As technological advancement and the overall the level of development range greatly around the world, WSIS recommended that each plan be developed in accordance not only with the main goals of WSIS, i.e. to bring ICT development in line with the MDGs, but also be appropriate considering social and political contexts. Four out of the nine cases have developed plans in line with WSIS's recommendations—the United States, Brazil, Mexico, and Indonesia—though notably later than WSIS's 2005 deadline. China and Iran have adopted approaches within five-year development plans, and the remaining states have yet to do so.

Adopted in 2010 "Connecting America" promised that by 2020, 100 million households would have broadband capable of 100 Mbps download speeds, a sophisticated connection even in 2016. In addition the 100^2 promise, the plan contained other mechanisms to spread access, including increasing public places of access and funding through Universal Service Funds. The plan was framed within the context of the geographic and socioeconomic divides, and updates have continually noted that while progress has been made, stark contrasts among rural, tribal, and lower SES populations mean that people continue to be left behind. While the US has been part of the WSIS action plans since 2003, the free-market perspective on the relationship between the state and ICT corporations limits the role of the state. Ambassadors for International Communications and Information Policy have repeatedly seen the role of states is to enable the market to do its job (Kaspar). FCC policy and update reports are absent mention of WSIS and other international obligations despite American participation, but instead often make comparisons to Asian tigers and European states in reference to the how US is falling behind (see Crawford, *Captive Audience*). Framed within the US being the inventor of this important technology, the persistence of the digital divide is regularly seen as unacceptable.

Brazil's National Broadband Plan was also adopted in 2010 and sought to extend service to remote and rural areas and make 1 Mbps connections available for 40 million households by 2014. While access has increased in the interceding years, critics are skeptical of the impact of the incentives laid out within the plan, with less than 10 percent of providers claiming to have taken advantage of the financial incentives. The plan is best understood as complementary to the framework of Brazil's larger efforts to

increase Internet penetration and access, and while it has been part of the WSIS process, its reliance on a multistakeholder model has displaced the state in some ways.

Mexico introduced its National Digital Strategy in 2013. Unlike Brazil, it neither contains set targets nor prioritizes norms related to the F2C and Internet freedom. Instead, the document connects ICT development to economic growth. However, it does acknowledge the effects access has to education and job opportunities and discusses how they are boon for achieving human rights.

Indonesia's plan, produced in 2013, is commensurate with the vision as originally presented by WSIS. The prerequisites of the plan include "government leadership, national commitment, multi-sector synergy, and public-private partnerships." By 2019, it hopes to achieve urban speeds of 1 Gbps and individual speeds of 1 Mbps nearing 100 percent. Far less ambitious than other states, the plan is a reflection of what is achievable within the timeframe given the extant infrastructure.

Russia's unnamed targets for broadband penetration by 2018 were produced by the Ministry of Communications and Mass Media, and reflects other such plans, laying out targets for fixed (5 million households with 100 Mbps capability) and mobile broadband (20 million new 4G customers per year). Like Indonesia, the modest targets are a reflection of current infrastructure capabilities.

Both Iran and China have included ICT development within the larger frameworks of 5-year economic plans, a reflection of the centrality of the state in each case's political-economic arrangement. , Like other national broadband plans, China has adopted targets for mobile and fixed lined penetration increases. Iran's intranet, the SHOMA network, was included in its most recent five-year plan. SHOMA is a drastic representation of the state's intervention into the provision and use of Internet for its citizens, both China and Iran's plans are a reflection of the state's desire to shape the Internet into its own vision of the state's political culture. For China, it is a reflection of economic progress and social harmony, and with Iran the plan is meant to make a pure Internet that would exist beyond the corrupting influence of the West.

For various reasons, the Philippines and Cuba all do not have long-term Internet provision plans. For the Philippines, the entrenchment of the PLDT and the relative weakness of the state to direct policy may have discouraged the design of a plan that may never meet with any success. Cuba, the outlier of this study, is slowly increasing Internet penetration in a country that has had only a handful of users of a

system that is antiquated and forcibly limited. The state may prove resilient to the political rapprochement with the US, but at this point there is little need, both from a technical and political standpoint, for the state to develop Internet penetration policies that are currently practically nonexistent.

State-Sponsored Studies. The presence of routine, state-sponsored studies that investigate Internet penetration rates and the digital divide is a reflection political will and capacity. All states in the Free and Partly Free categories, save the Philippines, have bureaucracies in place that routinely measure and publish studies regarding access. The NTC and other Filipino institutions do not have much power, so the lack of studies may be reflection of cronyism in that important financial resources may be diverted from labor-intensive and expensive work. These measures are important for national broadband plans and reports to the ITU, which depends on such institutions for their own gauge of the growth of the Internet around the world. China's CNNIC also collects reliable statistics.

Cuba's current Internet access points are directly controlled by the state, either through Wi-Fi or community "navigation halls," all supplied by ETECSA, so such studies would be redundant. The motivation for Iran's poor record of Internet penetration statistical collection is unclear. A state that is so concerned with how the Internet used by its citizens should desire to know where, when, and who goes online; it may be that the stated ICT rates are greatly exaggerated.

Rights-based Access Statement. Four of the nine cases examined have issued or attempted to issue either constitutional or other legal statements assuring that Internet access is a right to be enjoyed equally among all of its citizens. These statements are written within the context of the larger scope of rights associated with Internet freedom that have become synonymous with the relationship between politics and the Internet today, including privacy and net neutrality. They appear only in the Free and Partly Free categories among the Philippines, Brazil, Indonesia, and Mexico.

The Philippines and Indonesia, as states with similar political cultures and problems relating to access, have both adopted rights-based statements that are the result of consultation with various stakeholders concerning Internet access. These generally include the state, NGOs, ICT professionals, and end-users. The Philippine Magna Carta is focused on how civil rights are to be understood on the Internet while the Jakarta Declaration included initiatives to expand access, including last-mile access and backbone infrastructure completion. The reason for the lack of a push for infrastructure buildout in

the Philippines's crowd-sourced version is not directly clear, but may be a consequence of the document's origins. Unlike the Jakarta Declaration which grew in part thanks to the Digital Divide Institute, the Magna Carta was a reaction to a controversial cybercrimes bill that may have limited meaningful access, so it fails to extend the scope of access beyond the threats to civil rights the law had made.

Brazil has risen to its influential status as a result of its Marco Civil da Internet, a document that touches on freedom of expression, privacy, net neutrality, and a host of other rights to be enjoyed on the web. Like the Philippine document, the rights framework was partly crowd-sourced and found its origins in reaction to a controversial cybercrime bill that had the potential to limit meaningful access. It goes further than the Philippine version, creating an obligatory role for the state in the provision of ICT infrastructure and regulation of the industry. Similarly, Mexico's Internet para Todos gathered signatures for a petition to include Internet access as a civil right in an amendment to the Mexican constitution. Such a move is not unprecedented and illustrates the commitment the Mexican state has to increasing meaningful access.

None of the cases from the Not Free category have produced any legislation that guarantees citizens' access or limits the state's power on the web. Neither the US nor Russia have produced such artifacts, either. For Russia, the increasing power of the state and its growing presence in the provision of Internet may partly explain its absence, in addition to the little demand from the public and support for the Putin regime, and that access has been spreading throughout the country, albeit slowly. American political culture and the power of ISPs have been influential in the US in shaping Internet policy, prioritizing private efforts over PPPs and municipal broadband. Internet pioneers like Vint Cerf and ICT professionals are vocal against the idea of framing the Internet as a human right, despite the fact that nearly three-quarters of Americans from two surveys think it should be seen as such. It may be that the combination of government power, entrenched Interests of ISPs, and the ICT professionals' narrative of technological innovation works together against the formulation of such a policy. In the meantime, a relatively weak public agency, the FCC, works piecemeal in reaction to NGO and other grassroots efforts on issues like privacy, piracy, and neutrality.

Tax incentives. Only two states actively use the power of fiscal policy to encourage further Internet penetration through the private sector. Naturally, as states in the Not Free categories are the ISPs or directly control ISPs, such policies would be redundant. Cronyism in the Philippines would also logically favor incumbent ISPs against any measures designed to encourage domestic competition.

Brazilian tax policy, as conceived by the national broadband plan, has encouraged infrastructure buildout in rural areas by reducing or eliminating taxation on ISPs. Similar programs are available for ISPs that connect public schools. Sales tax has been exempted on smart phone technologies at their point-of-sale that would encourage users to purchase the necessary equipment to make use of wireless technologies.

Some municipalities in the US have used tax incentives to encourage municipal-level buildouts. AT&T other ISPs have challenged these incentives, arguing that they should have "right of first refusal" when cities are considering the adoption of GONs (Gustin). The failure of major private ISPs to provide service should be enough to preclude such an argument from being taken seriously, but ISPs continue to frame municipal broadband as an unfair competitor. The debate over municipal broadband continues, so far in favor of entrenched interests.

Regulatory Efforts and Legislation. Five of the nine cases examined have taken up measures to further regulate ISP sectors. All three of the states from the Free category have done so with varying support from the public. The FCC reclassified ISPs as public utilities allowing the agency authority to regulate pricing and practices that might be deemed as against norms of net neutrality. The Philippines "Fair Competition Act" that was passed in December 2014 was to break up duopoly conditions of the Filipino ISP markets, but as of yet it has not passed any legislation or policies that have been reported as having an effect on the PLDT or Globe. In addition to framing the Internet as a right and assuring other civil liberties be upheld on the web, the Marco Civil da Internet upholds policies like net neutrality and privacy.

Mexico and China, in different manners, have taken steps to forcibly breakup de facto monopolies. The Federal Institute of Communication was created by the "Pact for Mexico" that was designed to break up the empire enjoyed by América Móvil. The efforts are ongoing, and while Mexico is following in some of Brazil's footsteps, it has a way to go. China's anti-trust legislation declared that its

ISPs were in violation of the law, and required reorganization. China Mobile, Unicom, and Telecom run each region's branch semi-autonomously, and compete with one other in both fixed and mobile Internet provision markets. These steps may lead to greater and more efficient provision of access in China, but says little regarding the meaningfulness of that access.

Public access. The direct provision of access in community centers is one approach states have taken to addressing the divides that persist within their territories and populations. The US federal government does not usually participate in the direct provision of access in public places, but indirectly supports its availability in libraries and other municipal-level community points of access. HUD's program that would wire broadband in housing projects is an exception, and may signal more such policy initiatives in the future.

Brazil, Mexico, and the Philippines have all undertaken projects to provide free access in central locations within municipalities that is tied to their manifestations of the digital divide. Community eCenters (Philippines), Knowledge Labs such as those found in Piraí Digital City (Brazil), and telecenters provided by Mexico Conectado are grassroots projects that intend not only to provide connections to its citizens, but to provide digital literacy courses and assistance with other issues about learning to make full use of the Internet. Other cases have public access areas, but they are not touted as anything particularly special. For Cuba, public access is a way in which the state limits access for most Cubans. Government initiatives to overcome problems of digital literacy are absent.

Public-Private Partnerships. PPPs can take many forms. In every case, PPPs function in areas where public or club goods are pivotal to the development of particular communities, but are unattractive to be independently developed by private sector. In the cases examined, they run the gamut from partnerships undertaken for the construction of infrastructure, as temporary service providers, or providing public access areas in communities.

For the US, despite the objection from national ISPs, PPPs take the form municipal broadband projects. They most-often succeed when framed as temporary or as "alternative delivery systems," that divert attention from public-sector involvement in the traditionally conceived private markets. In the provision of public access for communities, municipalities pay private ISPs for their service more or less like any other consumer, it should not be properly conceive as a PPP.

The Philippines has begun a PPP centered on the development of TVWS, partnering with Microsoft to benefit from unused television frequencies to bring broadband to underserved areas. As the World Bank suggests, such an arrangement is ideal in states with entrenched private sector actors and weak bureaucratic controls. Likewise, Brazil's Cinturão Digital Belt project laid out cable across the state of Ceará, with the municipal government footing the bill of a 2,600 km build out. Through taxation and other incentives, small and medium ISPs were encouraged to extend the cable's capacity to end users.

NGOs. Non-governmental organizations aimed at providing further Internet penetration and meaningful access are active in the US, the Philippines, Indonesia, Brazil, and Mexico. Two organizations, Mexico's Internet para Todos and the Philippines's Democracy.Net.Ph were coalitions of groups and NGOs that petitioned their government to include access as a right or legal protections for its use. Mexico's Fundación ProAcceso and America's Connect for Good both work at the community level to provide training in digital literacy and provide other prerequisites to meaningful Internet use, like free access and cheap hardware. The Digital Divide Institute, a collaboration between Western and Southeast Asian academics, advises in Indonesia the proper utilization of Internet infrastructure

Russia's NGOs have been repeatedly challenged in the past several years, with a law passed in May 2015 that bans NGOs that the government claims as "undesirable." The power of the state in the realm of the provision of access has meant relatively little in the providing of free access or training. Still, grassroots projects like the Glasnost Defense Foundation and other civil rights advocates contest limitations on content and violations of users' rights perpetrated by the Russian state. Civil society is truncated in Iran, China, and Cuba as a result of both regime type and political culture.

Special Projects. In four cases states have taken additional, unique steps to increase access or otherwise provide new avenues of access.

The US's Connect Home program is a partnership between the federal Housing and Urban Development program and service providers in 28 pilot communities. Each pilot is a reflection of the existing partnership, but all will provide low or no cost broadband based on the model developed by the ConnectforGood model in Kansas City. Funds for the program are budgeted out of existing funds for the HUD.

Brazil's NETmundial conference of 2014 was conducted to present an alternative to the American-centric model of Internet governance. Multistakeholder governance was not a new concept, but stands in contrast to perceptions of US dominance in the wake of the Snowden revelations and the multilateral model encouraged by some in the ITU.

Indonesia's Palapa Ring projects are meant to enable connections among its lesser populated islands that are far removed from the urban centers of the state. Not a PPP, the ring projects are funded through universal service obligations, much like the proposed Lifeline program in the US. The approach is reliant on the market to make the most efficient use of the infrastructure once completed. Backers of the Palapa Ring's first project were also subject to the whims of the market in a different way, backing out of the project in the midst of the global recession.

Finally, Iran's SHOMA project, long-conceived and promised stands in contrast from other special projects and efforts through NGOs and PPPs to extend access. While it promises to do just that, the state's intranet efforts are meant to create a culturally acceptable web. Ideas considered heretical or dangerous to the Islamic Revolution normally found on the global Internet can be avoided. Presumably, SHOMA would enable easier surveillance of Iranian netizens that may use to platform in ways that the government disapproves.

Taken together, Free and Partly Free states have been the ones that have taken the biggest strides to increase Internet penetration in addition to meaningful access. While Russia and Not Free states have adopted medium-term goals, these have been almost exclusively driven by the state and its apparatuses and designed to enhance the states' control of content and monitoring of use. At varying levels, the US, the Philippines, Brazil, Mexico, and Indonesia have each addressed the divides between urban and remote, rich and poor using the rhetoric of the F2C while acknowledging the importance of access to educational and employment opportunity and membership in the political community.

Restrictions on Access and Other Limitations on Internet Use

States can simultaneously work to increase Internet penetration while inhibiting meaningful access in ways that are a reflection of political culture and context. There are two main methods. First and more directly, through policy or happenstance ISPs may be dependent on the state-owned infrastructure like IXPs and fiber. Second is the monitoring of access. While it largely characterized by

Freedom House as violation of users' rights, an examination of the practice is warranted as users "self-censor" themselves and do not use the Internet in ways that would be meaningful, and that such practices are indicative to a case's overall relationship to Internet freedom.

None of the states in the Free or Partly Free categories, save Russia, own or directly control the infrastructure that enables Internet access. For Russia, the Ministry of Communication and Mass Media requires ISPs to purchase foreign Internet traffic directly from state-controlled providers. This policy signals another avenue for the state to restrict access as an expression of techno-nationalism. The degree to which techno-nationalism serves merely as a guise for further state intrusion into Internet use is unclear, but to consider them one in the same is a mistake. Techno-nationalism can be seen as a reaction to perceived national security threats, whereas cyber sovereignty is more all-encompassing view of the role of the Internet and its relationship to the state.

The governments of China and Iran control the infrastructure connecting their Internet to the outside world. China has demonstrated its degree of control by shutting off access to entire regions or areas in times conflict. By exploiting the infrastructure owned by the TCI, Iranian authorities have developed ways to filter content and websites from their users. Despite the completion of an undersea cable connecting Cuba with Venezuela, ordinary Cuban users have not benefitted from the faster possible speeds made possible by the infrastructure improvements. Instead, government officials may use the improved download speeds, but the rest of domestic traffic is routed through the older and slower technology. It could be a consequence that Cuban officials not having the sophistication to filter content efficiently, and would prefer in the meantime to rely on the limitations of technology to do their work for them, with most websites being content-heavy that would easily frustrate users relying on slower connections.

Four of the six cases from the Free and Partly Free categories do not regularly monitor access or restrict content. However, the two archetypes states do so in important ways and have been the subject of scrutiny by the media, ICT professionals, and the public. While the US continues to struggle to increase Internet penetration and overcome the unequal access to broadband like all geographically large and diverse states, its credibility as a champion of Internet freedom has been tarnished by the revelations related to the PRISM program. Realistically, the method and extent of the data collection by the program

pales in comparison to scope and levels of coercion explored in other cases in this study like China and Iran. The NSA collects metadata purportedly for the purposes of curbing threats to national security, particularly terrorism, and investigators are not supposed to know the identities to whom the data belongs. In order for a formal investigation to be opened, a court (albeit a closed, secret court) must judge if there is sufficient cause. It uses voluntary cooperation from at least nine US companies, including Facebook, Google, Microsoft, and Yahoo. Yet recent battles over privacy reveal that while some elements of the American case are in favor of restricting Internet freedoms by the likes of the NSA and FBI, others see such invasions of privacy as inimical to consumers' expectations. Apple's refusal in April 2016 to unlock the San Bernardino terrorist's iPhone illustrates the fact that the relationship between the state and ICTs in the US is contested rather than hierarchical.

Unlike its Not Free counterparts, Russia's desire to control the Internet is complicated because its early development was accomplished under the auspices of the private sector. With the concentration of his power, the Putin regime continues to take steps to circumscribe content and monitor citizens' access. The state blocks "dangerous" websites related to suicide-promotion and child pornography. In themselves, such curtailments seem benign, but that the state takes these measures means it has the capacity and willingness to do so for other that challenge the power of the government.

China, Iran, and Cuba all directly monitor citizens' access to varying degrees. China requires ISPs to report illegal content and activity to the government, thereby contracting out the task in order for ISPs to keep their license. For places of public access in Iran, closed-circuit television monitor users' use, while in Cuba navigations halls are one of only two widely available avenues of access.

Defining Problems and Evidence of the F2C

Each of the archetype cases has unique defining problems that inhibit Internet penetration and meaningful access. For the US, the ISP fixed and wireless markets are dominated by few players, especially considering that availability for each is not nation-wide. Competition is stymied and companies like Verizon, Time-Warner, and AT&T hold enormous power. The continuing fight over net neutrality, in different and creative manifestations, pits these powerful companies against a bureaucracy that was empowered only recently to regulate the industry. Legal challenges to the reclassification are expected to continue.

Russia's moves towards an Internet Security Doctrine and a proposed intranet are indicative of a desire to further centralize and coordinate control over the medium. Its reclassification from Partly Free to Not Free stems from the shifting power of the regime itself, moving from relatively off-hands approach during the 1990s and the waves of liberalization after the collapse of the Soviet Union to the increasing centralization of power around the Kremlin today. For China, efficient Internet broadband rollout has been hindered by its near-monopolistic market and the state's attempts to create competition is meant to circumvent the high-costs and inefficiencies inherent in any such model.

The Philippines and Indonesia share similar problems to the hindrance of Internet penetration and meaningful access. In both cases, there is stark urban-rural divide perpetuated by market forces and the bottom line of large ISPs or associations. These inequalities are reinforced by preexisting disparities in technological dispersion, literacy, and socioeconomic status. Each state's political culture is marred by endemic patterns that disadvantage smaller ISPs and challenges to the status quo, especially patrimonialism and cronyism. As such, their bureaucracies remain relatively weak in developing or enforcing policies that would encourage anything but the pursuit of profit at the expense of efficiency.

Brazil can be viewed as a precursor to the Mexican relationship with Internet freedom, having started their relationship with Internet access in the early 1990s with an ICT environment that is eerily similar to what Mexico's is like today. Embratel was a subsidiary of the state-owned telecom Telebras, which had near-universal monopoly until the state stepped in (Norm 004-1995) to create rules that would not allow the ISP to charge higher fees to users and to encourage competition. By 1998 the state forcibly de-monopolized Telebras, much in the same way Mexico is currently doing to equally monopolistic, though privately-owned, América Móvil. Beneath the all-important layer of poor market environment, both Mexico and Brazil suffer from the inhibiting effects of the digital divide, shaped by territorial difficulties and differences in SES.

Internet penetration in Iran is inhibited by unreliable record keeping and strategies that do not go beyond broad goals. While the state's five-year plans have included the impetus for the SHOMA, it is not clear at this time whether this Iranian intranet is approaching anything near completion. It may have been hampered by the embargos or other difficulties in the importation of necessary equipment, but as

Freedom House correctly notes, the level of control that the network would give the state over users is concerning. There are no programs that address the meaningfulness of access.

Access in Cuba is likely to change dramatically in the next few years, considering the thawing of tensions that have shaped the Cuban political climate for nearly six decades. The ability to import equipment in addition to the demands of tourists who will visit Havana will likely increase speeds for some. Nonetheless, the resiliency of the state should not be underestimated; the methods that the Castro regime have used to solidify their power will not be erased when they are gone. The singular ISP and woefully outdated telecommunications infrastructure are problems that will persist despite a changing of the guard in a state run by *el Sistema*. The impetus for foreign ISPs to build out beyond Havana is questionable as a consequence of the lack of a marketplace.

All of the states in the Free and Partly Free categories, save Russia, show strong evidence of the acceptance of the norms of the Freedom to Connect. In the US, politicians have used the F2C as rhetoric in the wake of the Arab Spring and as a way to justify the multistakeholder model of governance of the Internet in contrast with the state-centered model supported by illiberal states.

The disparities between this type of rhetoric and the US federal government's actions through the PRISM program and the FBI makes such support for the F2C seem hypocritical. Yet the realist tendency to view state action through the "billiard ball" lens misses that bureaucracies and other manifestations of pluralism that can and do often work towards different ends. Policies do not have to be consistent. The Department of Housing and Urban Development can support the F2C while the National Security Agency works against Internet freedom. The FCC can fight to uphold net neutrality while the courts and local politicians empower ISPs. Google and Connect for Good can partner to bring broadband to the urban underprivileged, while Verizon and Comcast can work against municipal broadband projects as dangerous to the competitive market. It is of note, however, that each of these battles take place *within* the framework of the F2C. While their claims about the viability of the marketplace and innovation are thinly veiled attempts to protect corporate self-interest evidenced by widespread and expensive lobbying efforts, Verizon's protests against GONs must be framed as hindering the advancement of Internet penetration and innovation and not simply hurting their bottom-line. Boli and Thomas highlight the drive to couch self-interest in global culture:

> The burden of proof lies on self-interested actors to demonstrate that more than self-aggrandizement animates their action, even though their action promotes purposes like progress or growth. Just as medieval merchants met this burden of proof by paying for masses in the town cathedral, even quintessential self-interested actors feel compelled to demonstrate their collective concerns: Mobil sponsors public broadcasting productions, George Soros supports numerous charitable organizations. Higher virtue is reserved for those who act as agents of others, subordinating personal gain to broader concerns. (295).

The US lacks the nationally coordinated efforts among states, NGOs, and the private sector to increase access in ways that are present in the Philippines, Brazil, Indonesia, and Mexico. In the archipelagos, the demands have been addressed by legislation that require ISPs to be responsive to consumer demands to increase penetration, efficiency, and transparency. This has been done through coalitions among the consumers, NGOs, and corporate partnerships have used online petitions and other means to present their demands to the government. Such a methodology is one-way street, with those at the receiving end of policy demanding change to varying degrees of success.

In the Latin American cases, states have become partners with NGOs and ISPs with the aim of improving Internet penetration and meaningful access. Through PPPs and legislation, and in Brazil with the early creation of the Internet steering committee, the state has been an integral player in shaping policies that embody the F2C. NETmundial, in addition to providing an alternative model of Internet governance, also has platforms of equality, digital inclusion, and connects Internet access to traditional civil liberties including expression, association, and privacy.

Russia and the Not Free cases have asserted ideas that are framed through the lens of cyber sovereignty. The argument that the state should retain control over their citizens' use of the Internet as a matter of policy has numerous justifications. For China and Russia national security ranks high on the list, arguing that internal and external threats necessitate state control over infrastructure, epitomized for China by shutting off access in areas of political conflict. Such actions are seen as temporary necessities, an abrogation of otherwise necessary access to technology that is pivotal to the 21st century Western notions of economy and life.

Perceived threats to state ideology are common among these four states as justifications for limiting both Internet penetration and content and are far more engrained in policies surrounding the Internet. Each state sees information on the Internet as a threat to its culture or its conception of a healthy society. Russia's control of pornography and sites associated with suicide are the tamest

explanation for such intrusions on access, but the power to regulate has grown to include attacks on Russia's Orthodoxy and the criticism of the state. China's promotion of social harmony justifies placing limitations on the criticisms of the government and has resulted in self-censorship that is common among Chinese netizens. Iran shows the strongest predilection to assert the importance of morality in its limitations to Internet use, typified by steps to cap speeds, create its own intranet, and condemn the West as using the technology to undermine the Islamic Republic. Just as the Iranian constitution uses Western political structures to legitimize its unique political culture and authority, Iran's relationship with the Internet is similarly disingenuous. The state aligns the technology with its vision of politics and its worldview as a reaction to the challenges to the power that it enabled during the Green Revolution.

As in most other respects of this study, Cuba remains an outlier. One could argue that it neither supports nor challenges the F2C. The Internet in Cuba remains woefully backward as a consequence of economic stagnation and embargo, and as a consequence access is limited by geographic availability and speed. The state provides navigation halls and wireless access as an apparent means to raise funds rather than enable meaningful access for anything beyond contacting family outside of Cuba and whatever materials might be contained on its intranet. Yet the state does not suggest that it should be free develop its own sophisticated Internet in absence of the norms and associated rights as is the case in China, Russia, and Iran. The state does not prioritize increased Internet penetration or meaningful access and opt-outs of the financial benefits that Internet access might have on the country's GDP.

The degree to which the assertions of cyber sovereignty and techno-nationalism stand as an alternative to the F2C or as an exception have yet to be determined. Instead, it may signal that the state has been forced into dialogue with the expectations of state behavior surrounding the Internet. This viewpoint is evidenced by the defiant proclamation that "China's Internet is open," and the assertions in the 2010 White Paper that access does not impede Chinese citizens' rights of privacy and enhances political participation. Whether the Chinese government truly believes these conditions are in place for its Internet users is questionable at best, but that the most illiberal state on the web feels it must justify its position in a long document is a start.

Concluding Thoughts

This study sought to discover first, the normative development of Internet access as a component of Internet freedom and second, how states have reacted to various demands that would further enable meaningful use of the Internet. Access is more than being able to plug in an Ethernet cable or connecting a smartphone to Wi-Fi, and can include elements of digital literacy, affordability, and efficiency. States take a variety of steps to assure or deny access depending upon their understanding of the importance of the Internet and the immediate benefits access can bring its citizens. Evidence for the impact of the Freedom to Connect or a right to access is present in five cases: the US, Brazil, the Philippines, Mexico, and Indonesia, and correlates loosely with Freedom House's assessment of these states. Not Free states' policies on increasing Internet penetration have not demonstrated strong adherence to the framework of a right to access, but instead pursue the promise of economic growth tied with the technology. Each of these four states has taken measures to curtail access when it deems it necessary framed in terms of national security or the maintenance of social harmony.

This concluding section discusses each of the study's hypotheses, asking to what degree the F2C is similar and dissimilar to previous normative developments and then how IR theory can help to explain the effect this norm has had on state policy. It will then address some of the limitations of the methodology about the predictive power of the theoretical framework and suggest some further areas of research and its applicability to Internet freedom research writ large.

Normative development of Internet freedom and access. The first hypothesis tested was that the Freedom to Connect is an emerging norm in the international system that is being advanced by traditional and non-traditional norm entrepreneurs. Chapter 3 addressed the frames that surround the F2C and the identity of the actors who are constructing the narrative. The frames vary according to the identity of the entrepreneur and of how they understand the media's role in enabling human rights.

The F2C or right to access has taken on different interpretations according to the entrepreneur and the context in which it is advocated. Sandholtz and Stiles argue that normative discourse transforms norms' substantive content, their specificity, and authoritativeness. The study of the F2C's entrepreneurs and the reactions from states have revealed four major dimensions and their related phenomena:

- Physical infrastructure penetration
    - Wired components: IXPs, backbones, last-mile wired services
    - Mobile components: Base transceiver stations, TVWS
- Digital literacy
    - Correlated to SES and overall literacy
    - Knowledge of benefits of Internet
    - Content in primary language
- Meaningful access
    - Relative speed: does capacity of connection make Internet use fast/efficient for desired content?
    - Cost: can users go online without "breaking the bank" or is reliable, fast service cost-prohibitive?
- State interventions regarding access
    - The provision of public access points, PPPs, municipal broadband
    - State-as-ISP, monitoring and censorship with ISP consent, ability to disconnect users

At the outset of this study, it was assumed that access equated to the physical manifestations of the Internet—routers, servers, fiber, satellites—and the provision and control of this equipment by states and powerful ISPs. Instead, the meaning of access takes on deeper dimensions according to many entrepreneurs so that it can enable democratic participation and help in the provision of information, healthcare, education, and jobs. Digital literacy is a problem for many developing states in which SES and demographic factors work together to make simple physical access relatively worthless. When people in the developing world can use a computer or smartphone, they cannot find information in an efficient manner due to poor speeds or cannot afford plans that provide reliable service. The state also regularly intervenes into the issue of access, either proactively by providing public access or teaming with the private sector to expand infrastructure or services. Finally, illiberal states use several means to inhibit access, sometimes by throttling speeds, often by monitoring users or limiting content, or in the most extreme interventions by switching off access to entire areas.

Traditional norm entrepreneurs work from the top-down, advocating that the international system and states adopt policies in line with their demands. The most prominent of these platforms have been associated with the UN, and the F2C finds advocates in WSIS and the Special Rapporteur for Human Rights. WSIS advocates for closing the digital divide and promoting equal access, in addition to connecting access to the SDGs and the problem of Internet governance. The last has been the stickiest point for the ITU and WSIS, cemented in a divide between states that prefer multilateral to multistakeholder governance. Combined with the fact that the IGF cannot create binding policy, the impact of the UN on Internet governance has not been direct and is a questionable representation of the

normative discourse regarding Internet freedom. But the ITU and WSIS have had an impact on the development of policies surrounding access. Following the recommendation of the ITU and WSIS, many states have developed regional and national strategies to expand access which started being adopted by 2010 (US, Brazil, Indonesia, Russia, China, and Iran); these plans become important points of coordination among those promoting Internet diffusion within their states. Along with the Special Rapporteur, WSIS places the issue of access with the broader scope of human rights. The WSIS+10 outcome document highlights the necessity for access to economic and human development, while La Rue directly connects expression and association with undisrupted access. While the platforms have not created hard international law, the best practices and connections to human rights laid out by the action plans and reports have validated the continued importance of the UN in shaping normative discourse in this area of transnational behavior.

Other organizations working on international platforms have shaped the dialogue of Internet freedom and F2C, notably the World Bank and NETmundial. Along with APEC, the World Bank frames access in terms of economic growth and development. Noting the digital divide, each organization sees inequality as a hindrance to the potential for economic growth in the 21st century, which often bypass industries that are no longer required passages to contemporary economies.

NETmundial was touted as an alternative to the UN and development models of Internet governance and rights, calling for a richer multistakeholder model that would include the powerful actors that have a direct impact on Internet penetration and use. The group frames its work upon the necessity to increase Internet use to enable economic opportunity and to promote human rights. The crowdsourced model of the continued work of NETmundial is borrowed from Brazil's Marco Civil da Internet, and highlights the changing nature of normative development in the international system.

NGOs are active on the international and domestic levels, and are tied together through hyperlinked social networks. Prominent international NGOs like the Internet Society work at meetings like WSIS stock-taking events and are in turn associated with regional and domestic affiliates. Those like the Internet Society and WSIS are the ones generating "symbolic master frames" on which states and NGOs base their platforms and actions. For instance, the Digital Divide Institute, a regional NGO that worked in Indonesia to formulate and implement the Jakarta Declaration on Meaningful Broadband, highlights its

affiliation with Google, national governments, and the UN system. While they "support and applaud" the ITU's efforts relating to broadband within their FAQ, they claim that their understanding of the digital divide does not appreciate the particular contexts in which states are trying to implement meaningful broadband work. The ITU "…does not claim to consider how to establish the *political will* to implement ITU's own policy recommendations [emphasis in original]." The Institute is an important node in Southeast Asia, translating these broad policy recommendations into workable solutions like the Jakarta Declaration.

These patterns are repeated by local NGOs and associations working in Free and Partly Free states. Internet para Todos works with organizations that are directly interested in telecommunications reform, like Mozilla Mexico and Wikimedia Mexico, but do not directly deal with the NGOs constructing the master frames. Conversely, the Fundacion Proaccesso works among local NGOs along with international partners ranging from Google, Cisco, the UN Information Centre, and the World Bank. Brazil's NETmundial, while being a state initiative, sought to promote a new, albeit complementary "master narrative" which was coordinated with the CGI.br and 1net, a Uruguayan advocacy network along with numerous NGOs and MNCs interested in expanding Internet access and human rights.

Facebook and Google have undertaken initiatives in collaboration with local governments and ISPs to provide access in innovative ways. These are undertaken absent from hyperlinked social networks, instead relying on partnerships with mobile ISPs in countries where these initiatives are launched. The primary motivation for Free Basics and Project Loon are profit, but nonetheless have benefited local access initiatives in Latin American and Southeast Asia. While equality of access and the language of human rights are often used by these companies, their identity as enormous corporate entities with interested shareholders must drive these expensive and time-consuming projects. The apparent lack of collaboration with the state has tarnished the reputation of Facebook and Free Basics where the criticisms over neutrality have led to the dismantling of its arrangements in India and possibly slow its rollout elsewhere. Keeping this lesson in mind, the expansion of these and related projects by powerful MNCs still depend on the rhetoric of Internet freedom and the F2C, further deepening their meaning.

Not Free states contain none of these dynamics. The negligible power of NGOs in each of these states combined with the overwhelming power of the state and its control over or ownership of ISPs mean there is little room to advocate for increasing penetration that would bridge any of the manifestations of the digital divide.

The cyber sovereignty claim is a predictable reaction to the of the F2C norm life-cycle process as described by Sandholtz and Stiles. One of the difficulties of the F2C is that its demands are confrontational to the states outside the liberal international society based upon civil liberties and the free market. As most norm development is, there is evidence that the cyber sovereignty norms that challenge the F2C are in fact reactionary. "…one or more transnational actors provokes an interaction (or series of interactions) with another, which forces an interpretation or enunciation of the global norm applicable to the situation (Sandholtz and Stiles 8)."

The story begins with the Iranian Green Movement, which resulted from perceived irregularities in a national election and was bolstered by the use of social media. The importance of Twitter was not lost on observing states, which in turn reacted to the role technology played in assisting activists' organizational efforts by tightening their own controls on access and stepping up censorship efforts. In January 2010 Clinton remarked on the importance of rights on the Internet and articulated the "freedom to connect" as a reaction to the threats to expression on the web by authoritarian states. China published its White Paper on cyber sovereignty in June of that year rebuffing the idea that actions on the web should be free from government intrusion. By September 2011, China, Russia and Central Asian states submitted a brief to the General Assembly further asserting their belief that sovereignty should extend to cyberspace. Sovereignty in general has been a powerful norm in UN discourse due to its enshrinement in the Charter and has often been used as a fallback in response critiques over domestic human rights abuses. In reaction to the brief, the UN affirmed the right of sovereignty but reminded the states of their human rights obligations, both through human rights instruments and the general international acceptance of their basic principles.

Whether the cyber sovereignty defense that is being articulated is a full-fledged alternative normative development to the F2C is questionable. Sandholtz and Stiles argue that the normative process is not linear, and that the violation of a norm or rule is not evidence is disintegration or

meaninglessness. For instance, when powerful domestic actors break the law, they are not making *new* law but instead incur costs like fines or jail-time. The development of a new norm would be predicated upon how many other actors violated the rule and their justification for doing so. One of the conditions of Sandholtz and Stiles is the presumption of some measure of a liberal international society, tied to the solidarist British school that sees the development of new norms as a continuation of the ones that are complementary to norms that are pervasive for members of that society. The "foundational metanorms" of international society, they claim, are based on the belief in individual dignity and is evidence by universality and equality (1). The number of states that are Not Free total 30 percent of the 65 states examined by Freedom House and are concentrated in Asia, the Middle East, and the northeast part of Africa, and cyber sovereignty finds little support outside of these arenas and regime types. At its most powerful manifestation, cyber sovereignty will be limited to already authoritarian states.

The F2C is an emerging norm in the international system whose strongest effect is seen within the established international society that contains domestic and international agreements to protect liberal rights and equality. The international system, through the methods of "naming and shaming" by Freedom House's Index and the UN periodic reviews have forced those outside this liberal society to justify the actions of the state that impinge upon the right to access. China, Russia, and others have taken great pains to prove that Internet access is being increased to the benefit of their citizens, and that the restrictions placed on access and content are unfortunate but necessary aberrations due to problems that seem of genuine concern—suicide, drug trafficking, pornography, or the advocacy of violence. An inherent right of the state to censor, monitor, and control the actions of everyday citizens for the stability of the state is not part of the official discourse, but they only assert that sovereignty precludes critique of these practices. While this may be Russia or China's intent throughout the ways they inhibit access, they must use the language and tools supplied by international society. The hegemonic nature of the international society, made up of the US, Europe, and perhaps Latin America, sets the rules of the game in terms of access and the state's relationship with its Internet users.

Social movements on the web are not a new phenomenon. Studies of the Internet's effect on the foundation and organization of these movements goes back to the popular adoption of the web in the middle of the 1990s. There is evidence that hyperlinked social networks and informal social media

connections fuel the development of the F2C norm alongside UN and MNC platforms. The breadth of their effect on states is curtailed by the strength of the civil society in general and the degree to which the state controls access and content. Crowdsourcing the implementation of norms is a new phenomenon for IR that needs further investigation.

The F2C's impact on state behavior. The second hypothesis tested sought to explain how this norm affects state policy about the distribution and availability of Internet access. It used the Freedom House's *Freedom on the Net* rankings to predict whether the states examined would have a proactive or reactive response a right to access. State reactions have largely fell in line with the assessments made by Freedom House. When this study began, Russia had been categorized as Partly Free but since has moved to qualify as Not Free due to increases in censorship and monitoring of citizens. This study has shown that all states have taken measures to increase Internet penetration, but the framework justifying these measures taken by states diverge into two camps.

First, the US, the Philippines, Brazil, Mexico, and Indonesia all have framed their efforts to increase access using the rhetoric of the F2C, equality of opportunity, and human rights. This positive, proactive response to the multiple dimensions of access signal an acceptance of the larger Internet freedom regime that includes institutions like WSIS, the ITU, and the HRC. There is a powerful argument that the broader understandings of regimes beyond states is at work in Internet freedom, as the content of the F2C is shaped both by the likes of WSIS and the Digital Divide Institute. While international institutions more often shape and articulate the metanorms associated with a right to access, feedback from states and NGOs loop together to identify directions in which Internet freedom should be pursued and how the Internet is diffused.

Constructivism emphasizes the impact of norms, identity, and culture on behavior in the international system. Moreover, their malleability allows normative discourse that is constructed on the international level to have a meaningful impact on the states and cultures where they are applied (Sandholtz and Stiles). WSIS, the ITU, and the HRC construct the "master narratives" of Internet freedom and the F2C is interpreted by states, NGOs, and netizens according to their culture and market conditions. The right to access in the Philippines is largely a means to challenge the entrenched interests that keep the PLDT as a monopoly provider, while in Brazil it has transformed into the need to address

the inequality feedback loop of the digital divide, while in the US it has become the affirmation of net neutrality principles. Actors on the ground influence the master narratives over time. Cybersecurity has become part of the WSIS agenda thanks to state demands, but with different meanings: privacy, the vulnerability of data, minors or vulnerable populations being able to access explicit or questionable content, DDoS attacks, and so forth. As Sandholtz and Stiles suggest, the construction of norms operate in a feedback loop, and in this way the F2C is no different. The identity of entrepreneurs contained within these loops, however, is the remarkable change from earlier normative development, and it is likely that future normative development both inside and outside the realm of Internet freedom will look much the same. International platforms, hyperlinked networks, social media, and crowdsourcing will all be places to look for entrepreneurial activity to have an effect on the construction of normative platforms and their implementation.

Regime theory and the British school both view the central importance of norms and identity of actors in shaping and reacting to policy. The biggest difference between these approaches is methodology, the former emphasizing formal modeling while the latter utilizing qualitative methodology and interpretation. Evans and Wilson suggest that these approaches can be complementary, with the British school explaining the historical rise and prominence of certain regimes within international society. The solidarist school is especially pertinent in this regard.

The British school's conception of international society looms over the Internet freedom regime and explains the repeated connections between the F2C and human rights, particularly civil and political rights like expression, assembly, and privacy. International society is liberal, consisting of first the West and later expanding to include parts of the democratizing, developing world including Latin America and democratic states in Southeast Asia. Foot, Gaddis and Hurrell (2003) and Hurrell (2007) maintain that international society is faced with the problem of coming together to solve transnational problems and that its members are both unequal and have important differences in identity and priorities. Despite these difficulties, they present five reasons why international society cannot "retreat to pluralism" that applies the problems of Internet diffusion, the digital divide, and Internet freedom in general: 1) the interdependence among economic, social, and security concerns, 2) that structural changes mean that states need to coordinate to tackle these problems, 3) that citizens' expectations over the role of states

have increased, 4) the expectation that international society should exist to solve these demands, and 5) the changing global distribution of power. The authors anticipate that norm creation in the era of "globalization" is no longer solely the realm of states, but that transnational actors can shape expectations about the behavior of states and develop norms that they had little or no hand in creating. The importance of the hyperlinked social movements and the impact of crowdsourcing upon domestic policy and state rhetoric has had enormous impact upon how Internet freedom is understood and how the F2C has been articulated by the UN and other international platforms. Food, Gaddis and Hurrell continue that:

> Within the solidarist order states are no longer to act for themselves as sovereigns but rather, first, as agents for the individuals, groups, and national communities that they are supposed to represent—hence the move towards sovereignty as responsibility—and, second, as agents or interpreters of some notion of an international public good and some set of core norms against which state behaviour should be judged and evaluated (41).

Many of the Internet freedom and F2C advocates—Facebook, Google, the Digital Divide Institute, WSIS, the US State Department, the HRC—have framed the problem of access as transnational problem in which everyone should be connected and as integral to economic and social development, disaster relief, and healthcare. Naturally each of these actors has various goals in promoting the F2C. For MNCs, their primary goals are profit and the expansion of their marketplaces. US foreign policy is reflected in hortatory statements about the F2C from the State Department. The Digital Divide Institute's work reflects the academic and practical desires to extend access in a culturally relevant manner. These various and potentially conflictual goals work together to shape the normative discourse surrounding Internet. They are neither good nor bad in themselves, and work as both functional and abstract ideologies according to context and purpose.

The UN is not a mouthpiece of this liberal society but its agencies and organizations are often a proxy for the articulation of the outputs of the major policy initiatives. The UN also serves as a place for illiberal states to articulate their demands as seen through a letter to the General Assembly regarding cyber sovereignty and the periodic reviews conducted by the HRC. Nevertheless, the UN's dialogue with states that fail to live up to human rights norms illustrates how these states' actions are seen as incompatible with liberal international society in general and the regimes that make it up. Buzan clarifies that solidarism should not be considered synonymous with cosmopolitanism, and it is apparent that

illiberal states are not forming an alternative society based on some other set of norms. Instead, their priorities remain centered on state power.

For Free and Partly Free states, realism's emphasis on state power and its ability to shape norms is revealed better in issue of Internet governance rather than Internet freedom. Since the Snowden revelations announced the hypocrisy in American actions regarding Internet freedom in general, US foreign policy has largely been silent. To be fair, Clinton and Obama's rhetoric immediately followed the Arab (false) Spring, and it would take another window of opportunity to test the US's political will to use its power to shape the frames of Internet freedom. In the meantime, domestic policy in the US continues to follow along the line of the F2C through agencies like the FCC, HUD, and domestic NGOs, despite facing an uphill battle with ISPs. In this normative power vacuum, Brazil appears to be stepping forward to fill the gap as evidenced by both its domestic and foreign policy, enacting the Marco Civil da Internet utilizing feedback from users and pursuing privacy resolutions in the General Assembly. Mexico appears to be following in Brazil's footsteps and is attempting to become a tech hub in its own right. Nevertheless, there are some setbacks here too, including the ongoing controversy swirling around President Rousseff and the introduction of a new cybercrime bill in Brazil that appears to be much like SOPA.

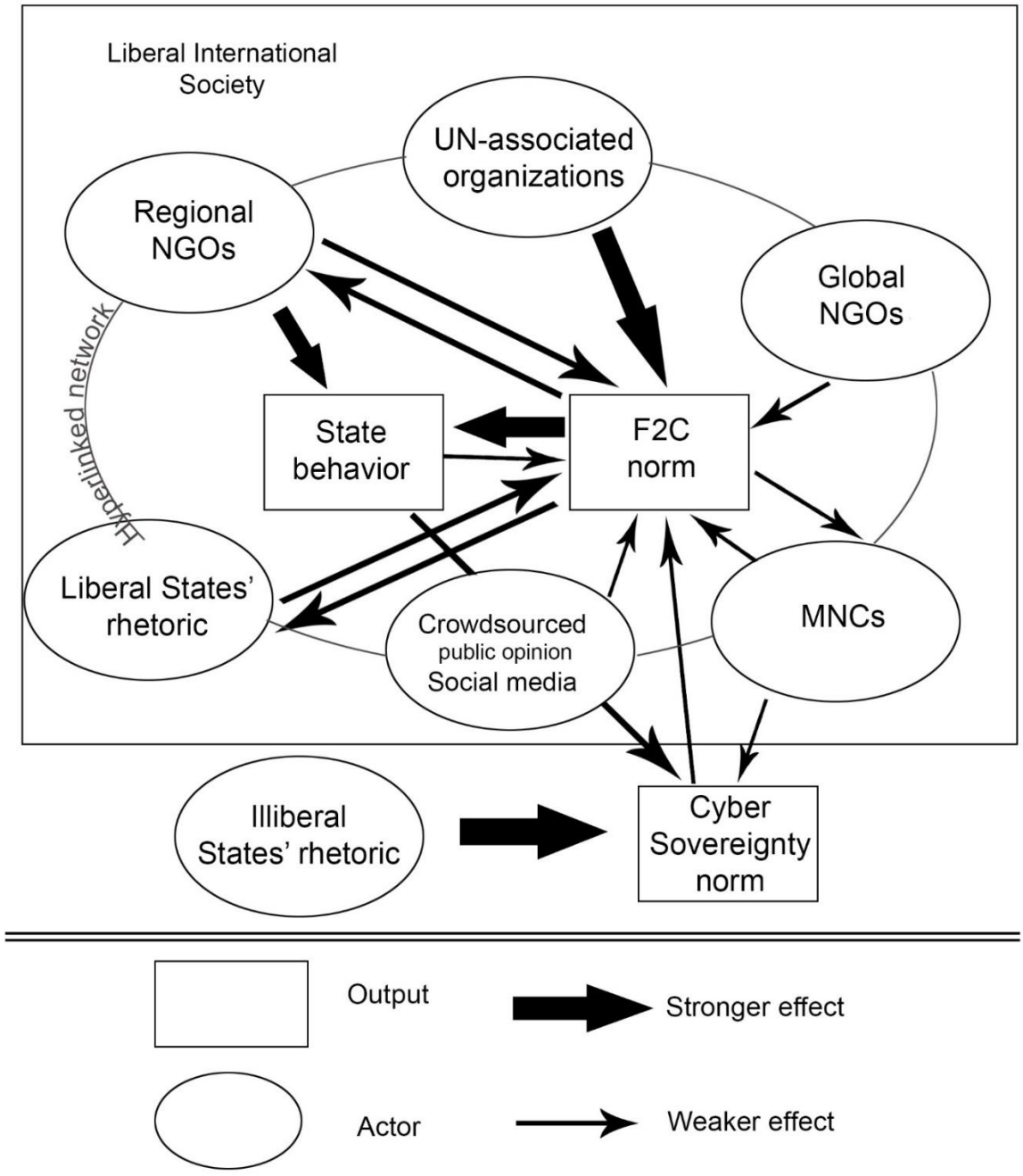
Second, Not Free states have not used the norms associated with the F2C or Internet freedom to justify their policies associated with increasing penetration and meaningful access. Russia stands between Free states and its Partly Free counterparts in terms of its rhetoric; while giving primary consideration to economic growth, Russia has used the language of participation and equality, but has not emphasized these benefits to be the focus of its plans. Along with China, Iran, and to some extent Cuba, Russia has taken actions through those same international institutions to assert its own norms about the relationship between the state and the Internet. Cyber sovereignty is a concept first articulated by China whose mantle has been taken up by other states found in Freedom House's scheme in the Not Free category. Realism indicates that these states have the power to transform normative discourse because they can mold morality/norms international system. Is the F2C threatened by this rhetoric?

I contend that cyber sovereignty is a defensive reaction to the perceived threats to the power of these illiberal states. Applying either in the virtual or actual world, sovereignty norms are inherently limiting, only signaling a fallback to the idea that states should be left to their own devices. China and

Russia are not obligated to give any attention to the F2C or Internet freedom and could pursue their domestic and foreign policy never having entered into a dialogue with rights advocates. Instead, they have framed their needs as exceptions to otherwise valid norms of Internet freedom in terms of how they interpret the need to maintain order and social harmony within their state. These derogations are similar to other human rights instruments, in which states do not claim that these rights are inherently illegitimate or invalid, but claim that do not apply to them in particular circumstances.

A summary of these insights are contained within the matrix that follows. It is certainly not a simplistic (or pretty) chart, but does convey the overlapping loops among the actors involved in the creation of the F2C and how it shapes state policy.

Figure 6 Matrix of the F2C, State Policy, and Cyber Sovereignty



Additionally, while concerns over spying uncovered by Wikileaks and Snowden are in themselves valid, illiberal states have used them as a window of opportunity to validate practices that they were doing anyway. These contextual exceptions to otherwise valid norms in the likely overblown threat posed by a Western-dominated Internet again do not form a basis for action in themselves. The push for multilateral

control of Internet governance, a topic strictly speaking separate from Internet freedom, is the strongest area where these states may have an impact on policy. Brazil's multistakeholder approach that is aligned with the F2C and Internet freedom seems to have won, with ICANN's transfer to multistakeholder model to be quietly completed in September 2016.

Limitations and areas of future research. The main limitation of the study is that it cannot establish a definite causal relationship between the development of the F2C and particular state policies. Finnemore and Sikkink's model of constructivism describes normative development to be a linear process, a cycle in which norms emerge, states react through rhetoric and the development of policy, and become concretized as part of the ideology and identity of state. Sandholtz and Stiles cycle theory of normative change better reflects the normative development of the F2C in which states contest and thereby construct the meaning of the F2C according to contexts in which they must meet the demands of the norm. The inclusion of the various aspects of access into shaping what the F2C really means—ISP markets, the digital divide, cyber security, social media—has been the result of the disputes (phase II) of the incompleteness and internal contradictions of this new norm.

In short, this study is limited because the F2C is a norm in the early stages of development. If the origins of WSIS is taken as its earliest benchmark (the 1998 ITU Plenipotenary conference), the F2C is less than 20 years old. This problem is magnified due its subject. The rapid pace of the development of technology has meant that states and other actors have had to make their policies about telecommunications diffusion and access at a disadvantage. Policy and law have an overwhelming tendency to be reactive, and when added to bureaucrats' mediocre understanding of infrastructure demands and how quickly ICTs change, normative development will be behind the times. Pledges to bring 3G technology to remote corners of the world by targets that range between 2017 and 2020 seem insufficient considering the ubiquity of 4G in the developed world and the rapid development of 5G that is expected to begin being rolled out early in the next decade.

Another weakness is that while patterns have emerged from the formation of the F2C by various entrepreneurs and from cases that were observed, they are not enough to make predictions about other regions' and states' reactions. How the F2C might be interpreted in European or African states, its relation to existing human rights standards, and how the state and MNCs shape their telecommunications

markets, cannot be extrapolated from Latin America or Southeast Asian cases. The plasticity of normative discourse around Internet freedom means only that researchers should look for contextual clues that would be relevant within the setting of the state in which they study.

Three other areas of future research stand out. One of the main contributions of this study to IR is a deeper understanding of normative development and discourse in generally, and specifically, determining how the F2C relates to other norms contained within the Internet freedom regime. How do hyperlinked networks and crowdsourcing change the way in which international norms that influence state behavior differ from the past? In what ways might we see more of these types of input during normative development and implementation in the future? For many entrepreneurs and states, the F2C came within a package of protections, duties, or rights related to the use of technology and the Internet. Does the debate over censorship work any differently from the right to access? How do privacy protections relate to the practice of surveillance within the context of exigent circumstances of national security? There is a clear argument that access is fundamental while censorship and monitoring can be temporary or necessary only given a particular need or overall context. As the surveys revealed, many users are willing to truncate their rights in the name of the protection from cyber threats or to hunt terrorists on the Web. Is access substantively different from how it is used, or are these rights indivisible, interdependent, and interrelated as other human rights are conceived?

The evolution of the cyber sovereignty deserves attention. I have argued here that as it stands today, the assertion of sovereignty in the virtual realm is a reaction to perceived demands and critiques upon state practices the limit access and violate users' rights. While it cannot form an alternative norm or regime, the degree that other states assert this defense of their actions that violate the principles of Internet freedom and the F2C will have an impact on how the norm is interpreted in local contexts and its frames. WSIS and the HRC have already acknowledged national security concerns within their articulations of the F2C, but they maintain the primacy of human rights as the focus of concern. The question will be if this powerful idea can have an even greater effect on the F2C that would substantially change its meaning.

Finally, tangential to the F2C and Internet freedom, the governance of the Internet has become an increasingly contested space among states. The insights of realism and the impact of regimes have

the greatest explanatory power in the development of ICANN past its American roots to a multistakeholder non-profit corporation. While technical management does not have a direct impact on how the Internet is used, the discourse over who gets control over the increasingly perceived important technology has been a place of contestation for the past several years. The exposure of the PRISM program has given a window of opportunity for greater criticism of the US and the drive for multilateral or multistakeholder control. Studying how states have reacted to the perceptions of inequity in Internet governance and how they relate their understanding of Internet freedom is worthy of attention.

***

The Internet and can be conceived as a right in itself and something necessary to achieve other rights in the 21st century. Political participation and economic development are increasingly dependent on meaningful access, and it is difficult to imagine areas of life in the developed world that have not been transformed by this technology. Developing states may be able to at least partially bypass some of the hurdles to economic, social, and political growth through the medium.

But the spread of the Internet is by no means equal or even guaranteed. Digital divides persist and require the intervention of powerful actors—states, MNCs, IGOs—in order to be overcome. Power on the web is taking shape in different ways from the past and is perhaps even more diffuse. Nevertheless, states remain front and center in the question of access, and they can take steps to increase its meaningful use or curtail it according to its own interests.

Appendix: Summary of Statistics and Policies on Internet Access from Selected Cases

		Free		
		US	Philippines	Brazil
Demographics	**Population**	321,368,864	100,998,376	204,259,812
	Rank	4	13	6
	Land mass (km^2)	9,833,517	300,000	8,515,770
	Rank	3	73	5
	Urbanization	81.60%	44.40%	85.70%
Economics	**GDP**	$17.97 trillion	$693.4 billion	$3.276 trillion
	Rank	3	31	8
	GDP/capita	$56,300	$7,000	$16,200
	Rank	19	153	12
ICTs	**Landlines**	129,400,000	3,090,000	44,100,000
	Rank	3	47	8
	Cellular phones	317,400,000	113,000,000	280,700,000
	Rank	5	13	6
	Percentage of Population	98.77%	111.88%	137.42%
	Internet users (CIA)	276,600,000	39,200,000	108,200,000
	Percentage of Population	86.80%	39.40%	53.40%
	Rank (absolute)	3	17	6
	Internet percentage (ITU)			57%
	Internet percentage (Domes. Est.)			CGI.br: 50%
Internet Environment	**Adoption of TCP/IP**	1986	1994	1992
	Who?	Military/academia	IBM	Academia
	Internet/telecom regulator	FCC	NTC	Anatel
	Average speeds	14.2Mbps	3.2 Mbps	4.1 Mbps
	Cost (wired, 10Mbps, per month)	$50/month, 1.82%	$44.03, 14.28%	$19.80, 4.30%
	Cost (other)		$12/month, wireless	

	Major fixed ISPs	Verizon, Time-Warner, AT&T, Comcast, CenturyLink	PLDT (70%), Globe	Embratel, Telefonica, many medium and small
	State owned / Hybrid / Private	Private	Hybrid	Private
	Symmetric or Asymmetric?	Symmetric	Asymmetric	Symmetric
	Major mobile ISPs	Verizon, AT&T --> T-Mobile, Sprint	Smart (PLDT; 52%) , Globe	Telefónica's Vivo, América Móvil's Claro, Telecom Italia's TIM Brasil, and the domestic player Oi
	State owned / Hybrid / Private	Private	Hybrid	Private
Digital Divide	**Long-term Broadband Plan**	National Broadband Plan (2010)	Not available	National Broadband Plan (2010)
	State-sponsored studies	OBI Technical Paper	Not available	Brazilian Internet Steering Committee, ICT Households
	Tax or financial incentives	Via municipalities	No	Reduce or eliminate taxation on ISPs building infrastructure
	Regulatory legislation for expansion	FCC Title II	Philippine Fair Competition Act	Marco Civil da Internet
	Rights based access statement	No	Magna Carta for Philippine Internet Freedom (pending)	Marco Civil da Internet
	Public access	Libraries	Community e Centers	Piraí Digital City, Knowledge Centers
	PPPs	Municipal Broadband	TVWS	Cinturão Digital Belt
	NGOs	Connect for Good	Democracy.Net.Ph	
	Special projects	ConnectHome		NETmundial

Laws restricting access	**Monitoring of access?**	PRISM	No	No; declarations of privacy on the Internet
	Providers dependent on state infrastructure?	No	No	No
Take-Away	**Defining problems**	Net neutrality, few competitors, PRISM	Urban-rural divide exaggerates digital divide; culture of cronyism	Speed; digital divide
	Evidence of F2C	HUD's ConnectHome program	Coalitions among consumers, NGOs, business partnerships that demand more responsive legislation	Coordinated efforts of states, NGOs, and ISPs through various means: taxation, PPPs, law; CGI.br

		Partly Free		
		Indonesia	Mexico	Russia*
Demographics	**Population**	255,993,674	121,736,809	142,423,773
	Rank	5	12	10
	Land mass (km^2)	1,904,569	1,964,375	17,098,242
	Rank	15	14	1
	Urbanization	53.70%	79.20%	74%
Economics	**GDP**	$2.676 trillion	$2.149 trillion	$3.471 trillion
	Rank	10	12	7
	GDP/capita	$10,600	$18,000	$23,700
	Rank	133	90	79
ICTs	**Landlines**	29,670,000	21,100,000	39,430,000
	Rank	11	14	7
	Cellular phones	319,000,000	102,200,000	221,000,000
	Rank	4	14	7
	Percentage of Population	124.61%	83.95%	155.17%
	Internet users (CIA)	42,400,000	49,500,000	84,400,000
	Percentage of Population	16.70%	41.10%	59.30%

	Rank (absolute)	14	12	7
	Internet percentage (ITU)	16%		
	Internet percentage (Domes. Est.)	APJII: 28%	INEGI: 44.39%	
Internet Environment	**Adoption of TCP/IP**	1994	1990	1991
	Who?	Academia	Academia	Academia
	Internet/telecom regulator	Ministry of Communication and Infomatics	Federal Telecommunications Institute, Ifetel	Ministry of Communication and Mass Media
	Average speeds	3.9 Mbps	5.9 Mbps	11.6 Mbps
	Cost (wired, 10Mbps, per month)	$26.37, 8.58%	$21.89, 3.79%	$5.71, 1.08%
	Cost (other)			$14/month
	Major fixed ISPs	Telkom, Indosat, First Media	América Móvil (Telemex; 80%), Axtel (6%)	Rostelecom (39%), ER-Telecom, Vimple.com, MTS, Telecom, AKADO
	State owned / Hybrid / Private	Hybrid	Private	Hybrid
	Symmetric or Asymmetric?	Symmetric	Asymmetric	Quasi symmetric
	Major mobile ISPs	Telkomsel, Indosat, Axiata	América Móvil (Telcel; 70%), Movistar (20%)	MTS, Megafon, VimpleCom and Tele2
	State owned / Hybrid / Private	Hybrid	Private	Private
Digital Divide	**Long-term Broadband Plan**	Indonesian Broadband Plan (2013)	National Digital Strategy 2013-2018	Unnamed 2012-2018 ICT goals
	State-sponsored studies	Bureau of Indonesian Statistics	INEGI's MODITUH	The Public Opinion (FOM) Foundation
	Tax or financial incentives	No	No	No
	Regulatory legislation for expansion	No	Forcible breakup of de facto monopoly	No

	Rights based access statement	Jakarta Declaration on Meaningful Broadband	Yes; via Internet para Todos and constitutional amendment	No
	Public access	No	Mexico Conectado telecenters	No
	PPPs	No	No	No
	NGOs	Grameen Foundation: micro franchises; Digital Divide Institute	Fundación Pro Acceso ; Internet Para Todos	Glasnost Defense Foundation
	Special projects	Palapa Ring Projects	No	No
Laws restricting access	**Monitoring of access?**	No, but some manipulation of content	No	Blocks access to "dangerous" websites; required to install monitoring devices
	Providers dependent on state infrastructure?	No	No	Ministry requires ISPs to purchase foreign Internet traffic directly from state-controlled service providers; Proposed Russian intranet
Take-Away	**Defining problems**	Urban-rural divide exaggerates digital divide; culture of patronage	Poor market environment	Internet Security Doctrine: further centralization
	Evidence of F2C	Coalitions among consumers, NGOs, business partnerships that demand more responsive legislation	Coordinated efforts of states, NGOs, and ISPs through relatively various means: PPPs, law	Primarily economic; some lip-service to rights; preliminary assertion of cyberspace sovereignty
*Russia was ranked under the Partly Free category when this study began. It has since been recategorized as Not Free by Freedom House.				

		Not Free		
		China	Iran	Cuba
Demographics	**Population**	1,367,485,388	81,824,270	11,031,433
	Rank	1	17	80
	Land mass (km^2)	9,596,960	1,648,195	110,860
	Rank	4	18	106
	Urbanization	55.60%	73.40%	77.10%
Economics	**GDP**	$19.51 trillion	$1.334 trillion	$128.5 billion
	Rank	1	19	76
	GDP/capita	$14,300	$17,100	$10,200
	Rank	112	96	131
ICTs	**Landlines**	249,400,000	30,590,000	1,260,000
	Rank	1	10	67
	Cellular phones	1,300,000,000	68,900,000	2,500,000
	Rank	1	22	144
	Percentage of Population	95.07%	84.20%	22.66%
	Internet users (CIA)	626,600,000	22,590,000	3,000,000
	Percentage of Population	46.00%	28.30%	27.50%
	Rank (absolute)	1	26	85
	Internet percentage (ITU)		39%	
	Internet percentage (Domes. Est.)	China Internet Watch48.8%	MATMA 2014: 49%	
			Islamic Republic News Agency 2015: 82%	
Internet Environment	**Adoption of TCP/IP**	1992	1994	1996
	Who?	Academia	Academia	State
	Internet/telecom regulator	China Internet Network Information Center	Ministry of ICT	Ministry of Informatics and Communications
	Average speeds	4.1 Mbps	1.6 Mbps	512Kbps-2Mbps
	Cost (wired, 10Mbps, per month)	$17.37, 1.83%	$79.90, 16.99%	N/A
	Cost (other)	$7.88/month (mobile)		$2/hour
	Major fixed ISPs	China Unicom, China Telecom	Telecommunications Company of Iran	ETECSA

	State owned / Hybrid / Private	State	Hybrid	State-owned
	Symmetric or Asymmetric?	Asymmetric	Asymmetric	Asymmetric
	Major mobile ISPs	China Mobile	IranCell	Cubacel
	State owned / Hybrid / Private	State	Hybrid	State-owned
Digital Divide	**Long-term Broadband Plan**	Within Five-Year Plans	Within Five-Year Plans	No
	State-sponsored studies	CNNIC	No	No
	Tax or financial incentives	No	No	No
	Regulatory legislation for expansion	Forcible breakup of de facto monopoly	No	No
	Rights based access statement	No	No	No
	Public access	No	No	"Navigation halls"
	PPPs	No	No	No
	NGOs	No	No	No
	Special projects	No	SHOMA	No
Laws restricting access	**Monitoring of access?**	ISPs required to report illegal content	Yes, CCTV	"Navigation halls"
	Providers dependent on state infrastructure?	Yes	Yes	Reroute traffic from cable to satellite
Take-Away	**Defining problems**	Unique, artificial competition in state-controlled market	Lack of governmental records, strategy	One ISP; dependency on MNCs
	Evidence of F2C	Cyberspace sovereignty	Cyberspace sovereignty with cultural addition	Cyberspace sovereignty, without clear articulation

Works Cited

Adams, David. 2015. “Cuba aims to ramp up Internet access: U.S. State Department official.” *Reuters*. 30 March 2015, http://reut.rs/1GbYOz0; accessed 6 November 2015

AFP. 2013. “Vladimir Putin signs anti-gay propaganda bill.” *The Telegraph*. 30 June 2013. http://www.telegraph.co.uk/news/worldnews/europe/russia/10151790/Vladimir-Putin-signs-anti-gay-propaganda-bill.html; accessed 2 September 2015

Agcaoli, Lawerence. 2015. “PLDT strengths Southern Luzon fiber optic cable network.” *The Philippine Star*. 17 June 2015. http://www.philstar.com/business/2015/06/17/1466620/pldt-strengthens-southern-luzon-fiber-optic-cable-network; accessed 17 January 2016

Agência Estado. 2010. "Barreto advocates creating 'constitution' of the Internet.” *G1 Brazil*. 13 May 2010. http://g1.globo.com/brasil/noticia/2010/05/barreto-defende-criacao-de-constituicao-da-internet.html; accessed 11 December 2015

AHRC. 2007. “THAILAND: AHRC hosts anti-internet censorship petition.” Asian Human Rights Commission. 28 March 2007. http://www.humanrights.asia/news/press-releases/AHRC-PL-013-2007/; accessed 29 January 2016

Akamai. 2015. “Q4 2015 Report.” *Akamai’s State of the Internet Report*. Vol. 8.4

Al Jazeera. 2013. “Mexican Senate approves telecoms-reform bill.” *Al Jazeera America*. 1 May 2013. http://www.aljazeera.com/news/americas/2013/05/2013515845225187.html; accessed 6 January 2016

Alam, Johar. 2003 “Indonesian Internet Exchange (IIX).” *APJII: IIX*. http://www.iix.net.id/library/Iix_history.pdf; accessed 26 October 2015

Alexander, Marcus. 2004. “The Internet and Democratization: The Development of Russian Internet Policy.” *Demokratizatsiya*. Vol. 12.4.

Alves, Joedson. 2014. “Brazil's Rousseff lets Obama off the hook for NSA spying.” Reuters. 21 June 2014. http://www.reuters.com/article/us-brazil-usa-espionage-idUSKBN0FF2H820140710#VVobjFjzIsiLA0ld.97; accessed 11 December 2015

Anderson, Collin. 2013. “Iranian Internet Infrastructure and Policy Report.” *SmallMedia.co.uk*. July-August 2013. https://smallmedia.org.uk/sites/default/files/u8/iiipjuly.pdf; accessed 23 March 2016

Anderson, Martina et al. 2015. “European Parliament resolution on child sex abuse images online (2015/2564 (RSP)).” *European Parliament*. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT+MOTION+B8-2015-0227+0+DOC+XML+V0%2F%2FEN; accessed 18 June 2015

Anderson, Phil. 2002. “Fox inaugurates first phase of e-Mexico program.” *BN Americas*. 16 July 2002. http://www.bnamericas.com/en/news/technology/Fox_inaugurates_first_phase_of_e-Mexico_program; accessed 2 January 2016

Andersson, Henrik “HAX.” 2015. “European Parliament: You may limit fundamental rights on the internet.” *5th of July Foundation Blog Post*. https://hax.5july.org/2015/03/11/european-parliament-you-may-limit-fundamental-rights-on-the-internet/; accessed 18 June 2015

APEC. 2015. “APEC Telecommunications and Information Working Group.” *APEC.* http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information.aspx; accessed 18 June 2015

APJII. 2013. “ICT Development Index will be compiled annually.” *APJII*. 25 July 2013. http://www.apjii.or.id/read/article/apjii-at-media/183/ict-development-index-akan-disusun-setiap-tahun.html; accessed 24 October 2015

APJII. 2015. “About Us.” Indonesian Internet Service Provider Association https://translate.google.com/translate?sl=auto&tl=en&js=y&prev=_t&hl=en&ie=UTF-8&u=http%3A%2F%2Fwww.apjii.or.id%2F%23&edit-text=&act=url; accessed 31 October 2015

Arabshahi, Payman, 1997. “The Internet in Iran: A Survey.” *Iranian.com.* 9 June 1997.

Arroyo, Federico Hernández. 2014. “Mexican Telecommunications and Broadcasting Law to enter into effect 13 August 2014.” *Global Media and Communications Watch*. 5 August 2014. http://www.hlmediacomms.com/2014/08/05/mexico-new-telecommunications-and-broadcasting-law-to-enter-into-effect-13-august-2014/; accessed 2 January 2016

Asmolov, Gregory. 2010. “Russia: Authorities to Eliminate “Digital Divide” in 2010.” *Global* Voices. 7 March 2010; https://globalvoices.org/2010/03/07/russia-divide/; accessed 16 September 2015

AT&T. 2015. “AT&T Launches 4G in Mexico.” 12 October 2015. http://about.att.com/story/4g_lte_launches_in_mexico.html; accessed 9 January 2016

Aviles, Mary, Ellery Roberts Biddle, Taisa Sganzerla, and Sarah Myers West. 2015. “Netizen Report: Will Brazil Give Up on Defending Digital Rights?” *Future Tense: Slate*. http://www.slate.com/blogs/future_tense/2015/09/30/netizen_report_will_brazil_give_up_on_defending_digital_rights.html; accessed 12 April 2016

Ayson, Jim. 2011. “Up the Philippines to the Internet.” Word Press Blog https://jimayson.wordpress.com/2011/08/13/the-night-benjie-hooked-up-the-philippines-to-the-internet/; accessed 12 January 2016

Baker, Peter and David E. Sanger. 2013. “Obama Calls Surveillance Program Legal and Limited.” *New York Times*. 7 June 2013.

Ball, James and Benjamin Gottleib. 2012. “Iran preparing internal version of Internet.” *The Washington Post*. 20 September 2012. https://www.washingtonpost.com/world/national-security/iran-preparing-internal-version-of-internet/2012/09/19/79458194-01c3-11e2-b260-32f4a8db9b7e_story.html; accessed 10 November 2015

Barbosa, Alexandre F. 2015. “ICT Households 2014.” Brazilian Internet Steering Committee. TIC_Domicilios_2014_livro_electronico.pdf; accessed 30 November 2015

Barkin, J. Samuel. 2003. “Realist Constructivism.” *International Studies Review*. Vol. 5.2.

Barlow, John Perry. 1996. “A Cyberspace Independence Declaration.” *Electronic Frontier Foundation*. http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration; accessed 5 April 2013

BBC. 2012. “Google attacks UN’s internet treat conference.” *BBC.com*. 21 November 2012. http://www.bbc.com/news/technology-20429625; accessed 7 June 2015

BBC. 2016. “India blocks Zuckerberg's free net app.” BBC.com 8 February 2016. http://www.bbc.com/news/technology-35522899; accessed 2 March 2016

Beech, Hannah. 2014. “Michelle Obama Defends Free Internet in China Speech.” *Time.com*. 22 March 2014. http://time.com/34314/michelle-obama-defends-free-internet-in-china-speech/; accessed 30 July 2015

Bejtlich, Richard. 2015. “Dark Cloud: Why CloudFlare's Deal with Baidu Could Haunt US Tech Companies.” *Motherboard*. 15 September 2015. http://motherboard.vice.com/read/cloudflare-baidu-partnership-yunjiasu-china; accessed 4 October 2015

Bellamy, Alex. J. 2005. *International Society and Its Critics.* NY: Oxford University Press.

Benkler, Yochai. 2006. *The Wealth of Networks: How Social Problems Transform Markets and Freedom*. New Haven: Yale University Press.

Benkler, Yochai. 2011. “A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate.” *Harvard Civil Rights-Civil Liberties Law Review*. Vol. 46.2.

Berners-Lee, Timothy. 1989. “Information Management: a Proposal.” CERN. http://www.w3.org/History/1989/proposal.html; accessed 3 December 2013

Bertoni, Eduardo. 2013. “Brazil: the New Internet Freedom Champion?” Internet Policy. 15 October 2013. http://www.i-policy.org/2013/10/brazil-the-new-internet-freedom-champion-.html; accessed 25 November 2015

Bertot, J.C., K. Sigler, A. McDermott, E. DeCoster, S. Katz, L.A. Langa, and J.M. Grimes. 2011. “2010-2011 Public Library Funding and Technology Access Survey: Survey Findings and Results.” *Information Policy and Access Center: University of Maryland*; http://plinternetsurvey.org/analysis/public-libraries-and-community-access; accessed 5 July 2015

Bildner, Eli. 2013. “A Map of Two Chinas: Internet Penetration and Economic Development.” *The Atlantic*. 23 January 2013. http://www.theatlantic.com/international/archive/2013/01/a-map-of-two-chinas-internet-penetration-and-economic-development/267424/; accessed 9 October 2015

BitsNet. 2015. “Internet Service Provider.” http://www.bits.net.id/index.php/services/internet-service-provider; accessed 1 November 2015

Bleijenbergh, Inge. 2010. “Case Selection.” in *Encyclopedia of Case Study Research*. eds. Albert J. Mills, Gabrielle Durepos and Eiden Wiebe. Thousand Oaks, CA: SAGE Publications, Inc.; http://dx.doi.org.ezproxy.gc.cuny.edu/10.4135/9781412957397.n26.; accessed 010315

Blue, Violet. 2012. “Exclusive: ITU ‘failed,’ says former policy chief.” CNET.com. 12 December 2012. http://www.cnet.com/news/exclusive-itu-failed-says-former-policy-chief/#!; accessed 7 June 2015

Blum, Andrew. 2012. *Tubes: A Journey to the Center of the Internet*. New York: Harper Collins.

Bo, Xiang. 2015. “China grants loans to Benin for broadband project.” *Xihuanet.* 24 February 2015. http://news.xinhuanet.com/english/china/2015-02/24/c_134013713.htm; accessed 10 October 2015

Boli, John and George M. Thomas. 1999. *Constructing World Culture International Nongovernmental Organizations Since 1875*. Stanford University Press.

Brahm, Eric. 2005. “International Regimes.” *Beyond Intractability*. Eds. Guy Burgess and Heidi Burgess. Conflict Information Consortium, University of Colorado, Boulder. http://www.beyondintractability.org/bi-essay/international-regimes; accessed 6 March 2013.

Branigan, Tania. 2012. “China cut off internet in area of Tibetan unrest. *The Guardian*. 3 February 2012. http://www.theguardian.com/world/2012/feb/03/china-internet-links-tibetan-unrest; accessed 18 October 2015

Broadband Commission on Sustainable Development. 2016. “About Us.” Broadband Commission on Sustainable Development. http://broadbandcommission.org/about/Pages/default.aspx; accessed 2 March 2016

Broadband Communities. 2012. “David Isenberg.” *Broadband Securities Mag*. http://www.bbcmag.com/2013s/13bio/Isenberg-david13.php; accessed 10 June 2013

Brodkin, Jon. 2013. “ISP lobby has already won limits on public broadband in 20 states.” *ARS Technia.* 12 February 2014. http://arstechnica.com/tech-policy/2014/02/isp-lobby-has-already-won-limits-on-public-broadband-in-20-states/; accessed 30 June 2015

Brodkin, Jon. 2016a. “Comcast and Charter may soon control 70% of 25Mbps Internet subscriptions.” *Ars Technica.* 26 January 2016. http://arstechnica.com/business/2016/01/comcast-and-charter-may-soon-control-70-of-25mbps-internet-subscriptions/; accessed 8 June 2016

Brodkin, Jon. 2016b. “’AT&T is the villain’ in city broadband fight, Republican lawmaker says.” *Ars Technica*. 4 February 2016. http://arstechnica.com/tech-policy/2016/02/att-is-the-villain-in-city-broadband-fight-republican-lawmaker-says/; accessed 6 February 2016

Brodkin, Jon. 2016c. “T-Mobile urges FCC to “tread lightly” on video throttling and zero-rating.” *Ars Technica*. 5 February 2016. http://arstechnica.com/business/2016/02/t-mobile-urges-fcc-to-tread-lightly-on-video-throttling-and-zero-rating/; accessed 6 February 2016

Brodkin, Jon. 2016d. “Verizon’s mobile video won’t count against data caps—but Netflix does.” *Ars Technica*. 5 February 2016. http://arstechnica.com/business/2016/02/verizons-mobile-video-wont-count-against-data-caps-but-netflix-will/; accessed 6 February 2016

Brodkin, Jon. 2016e. “AT&T sues Louisville to stop Google Fiber from using its utility poles.” *Digital Trends*. 25 February 2016. http://arstechnica.com/tech-policy/2016/02/att-sues-louisville-to-stop-google-fiber-from-using-its-utility-poles/; accessed 26 February 2016

Brodkin, Jon. 2016f. “Tom Wheeler defeats the broadband industry: Net neutrality wins in court.” *Ars Technica*. 14 June 2016. http://arstechnica.com/tech-policy/2016/06/net-neutrality-and-title-ii-win-in-court-as-isps-lose-case-against-fcc/; accessed 14 June 2016

Brunner, Grant. 2012. “China is turning its ISPs into internet police.” *ExtremeTech*. 28 December 2012; http://www.extremetech.com/internet/144330-china-turning-its-isps-into-internet-police; accessed 2 October 2015

Bruno, Luciana. 2014. “Broadband program draws to a close full of suspicion.” *Exame.com*. 30 September 2014. http://exame.abril.com.br/brasil/noticias/programa-de-banda-larga-se-aproxima-do-fim-cheio-de-criticas; accessed 6 December 2015

Buechler, Steven M. 1995. “New Social Movement Theories.” *The Sociological Quarterly*. Vol. 36.3.

Bull, Hedley. [1977.] 2002. *The Anarchical Society*. Fourth Edition. New York: Columbia University Press.

Bull, Hedley. 1966. “International Theory: The Case for a Classical Approach.” *World Politics*. Vol. 18.3.

Bureau of Statistics. 2015. “Communications.” Indonesian Bureau of Statistics. http://www.bps.go.id/Subjek/view/id/2#subjekViewTab3|accordion-daftar-subjek2; accessed 24 October 2015

Burkhart, Grey E. Seymour E. Goodman. 1998. "The Internet gains acceptance in the Persian Gulf." *Communications of the ACM*. Vol. 41.3.

Bustamante, Fabián E. 2015. "Connecting Cuba to the Rest of the World." *Pacific Standard*. 9 June 2015. http://www.psmag.com/nature-and-technology/connecting-cuba-to-the-rest-of-the-world; accessed 6 November 2015

Buzan, Barry. 1993. "From International System to International Society: Structural Realism and Regime Theory Meet the English School." *International Organization*. Vol. 47.3

Buzan, Barry. 2004. *From International to World Society? English School Theory and the Social Structure of Globalisation*. West Nyack, NY: Cambridge University Press.

Cadei, Emily. 2014. "How Brazil is Becoming a Leader in Internet Freedom." Ozy. http://www.ozy.com/fast-forward/how-brazil-is-becoming-a-leader-in-internet-freedom/32166; accessed 25 November 2015

Cadei, Emily. 2014. "Why Brazil May Rule the Internet." *USA Today*. 20 June 2014. http://www.usatoday.com/story/tech/2014/06/20/ozy-brazil-internet/11084053/; accessed 26 November 2015

Canal AR. 2015. "Nokia and Proacceso open new technology lab in Mexico." 22 July 2015. http://www.canal-ar.com.ar/21918-Nokia-y-Proacceso-abren-nuevo-laboratorio-tecnologico-en-Mexico.html; accessed 29 December 2015

Carnegie, Paul J. 2010. *The Road from Authoritarianism to Democratization in Indonesia*. NY: Palgrave Macmillan

Carr, E.H. 1964. *The Twenty Years Crisis*. NY: Harper Perennial. Reproduced by *Mount Holyoke College*. https://www.mtholyoke.edu/acad/intrel/carr.htm; accessed 25 November 2012

Carvalho, Fernando, Flavio Feferman, Peter Knight, Glenn Woroch. 2014. "Private-public partnerships for expanding broadband access: Lessons from the Cinturão Digital do Ceará Network in Brazil, 20th ITS Biennial Conference, Rio de Janeiro, Brazil, 30 Nov. - 03 Dec. 2014.

Castro, Giselle. 2015. "Dilma Rousseff and Facebook advertise free internet partnership for low-income population." *HuffPost Brasil*. 10 April 2015. http://www.brasilpost.com.br/2015/04/10/dilma-parceria-facebook_n_7044546.html; accessed 6 December 2015

Cerf, Vinton G. 2012. "Internet Access is Not a Human Right." *New York Times Opinion Pages*. 4 January 2012. http://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html; accessed 3 December 2013

Cesar, AALP. 2015. "Historia del Internet." *Time* Toast. http://www.timetoast.com/timelines/historia-del-internet-d8ac8c99-3df9-4bf4-b48f-14e8b137568c; accessed 4 January 2016

Chandra, Rizkan. 2013. "Creating Effective Broadband Through Meaningful Broadband Access & Services." Indonesia Digital Network Congress. 13 November 2013. http://media.wix.com/ugd/7efb06_76ebd1c3922a4013856021bb89dfe089.pdf; accessed 1 November 2015

Checkel, Jeffery T. 1998. "The Constructivist Turn in International Relations Theory." *World Politics*. Vol. 50.2

China Daily. 2001. “China Railcom Launches Operation.” *China Internet Information Center.* 13 August 2001. http://china.org.cn/english/DO-e/17470.htm; accessed 18 October 2015

China Internet Watch. 2015a. “China Internet Statistics Whitepaper.” *CIW*. http://www.chinainternetwatch.com/whitepaper/china-internet-statistics/; accessed 3 October 2015

China Internet Watch. 2015b. “China Mobile Internet Trend 2015.” *CIW*. 7 October 2015 http://www.chinainternetwatch.com/14949/china-mobile-internet-2015/; accessed 12 October 2015

China Unicom. 2015. “Prices for 4G Mobile Phone Packages.” *China Unicom*. http://www.10010.com/; accessed 8 October 2015

CIA. 2013. “World Factbook: Country Profiles.” *US Central Intelligence Agency.* https://www.cia.gov/library/publications/the-world-factbook/geos/us.html; accessed 15 June 2016

CIO Staff. 2006. “Group: Yahoo Helped Jail Third Chinese Journalist.” *Chief Information Officers*. http://www.cio.com/article/2446900/security-privacy/group--yahoo-helped-jail-third-chinese-journalist.html; accessed 11 October 2015

Citizen Lab. 2014. “IGF 2013: An Overview of Indonesian Internet Infrastructure and Governance.” *Citizen Lab and Canada Centre for Global Security Studies*. 20 January 2014. https://citizenlab.org/2013/10/igf-2013-an-overview-of-indonesian-internet-infrastructure-and-governance/; accessed 30 October 2015

CitizenLab. 2012. “Iran’s National Information Network.” *Munk School of Global Affairs: University of Toronto*. 9 November 2012. https://citizenlab.org/2012/11/irans-national-information-network/; accessed 20 November 2015

CIW. 2015. “China Smartphone Penetration Rate to Reach 38.6% in 2015.” *China Internet Watch.* 12 October 2015. http://www.chinainternetwatch.com/14941/urban-smartphone-users-half-new-equipment-next-year/; accessed 12 October 2015

Claude, Inis L. 1971. *Swords into Plowshares: The Problems and Progress of International Organization*. 4th Edition. NY: Random House.

Clinton, Hilary. 2010. “Remarks on Internet Freedom.” *U.S. Department of State Newseum*. www.state.gov/secretary/rm/2010/01/135519.htm; accessed 29 February 2012

CNBC. 2015. “ICANN oversight remains with U.S.” *CNBC Videos*. August 2015. http://finance.yahoo.com/video/icann-oversight-remains-u-140000093.html; accessed 4 March 2015.

CNET. 2009. “Finland makes 1Mb broadband access a legal right.” *CNET.com*. http://news.cnet.com/8301-17939_109-10374831-2.html; accessed 30 May 2015

CNNIC. 2012. “The Internet Timeline of China 1986-2003.” *China Internet Network Information Center.* 28 June 2012; http://www1.cnnic.cn/IDR/hlwfzdsj/201306/t20130628_40563.htm; accessed 2 October 2015

CNNIC. 2015. “The 35th Statistical Report on Internet Development in China (January 2015).” *China Internet Network Information Center.* 20 July 2015; http://www1.cnnic.cn/IDR/ReportDownloads/201507/P020150720486421654597.pdf; 4 October 2015

Coelho, Franklin and Maria Helena Cautiero Horta Jardim. 2011. "Piraí, Brazil, Transforms Education with Help of Technology Integration." *Intel Learning Series*. http://www.intel.com/content/www/us/en/education-solutions/brazil-transforms-education-study.html; accessed 6 December 2015

Cohen, Noam. 2011. "Egyptians Were Unplugged, and Uncowed." *NY Times*. 20 February 2011.

Collier, David. 2011. "Understanding Process Tracing." *PS: Political Science and Politics*. Vol. 44.4.

Common Cause. 2015. "Preserving the Internet." *CommonCause.org.* http://www.commoncause.org/issues/media-and-democracy/preserving-the-internet/; accessed 7 February 2016

Connect Indonesia. 2015. "Indonesia Aims to Beat Malaysia in Internet Access by 2019." Connect Expo Indonesia 2015. 15 September 2015. http://www.connectindonesia.net/indonesia-aims-beat-malaysia-internet-access-2019. Accessed 31 October 2015

Connecting For Good. 2016. "About Us." http://www.connectingforgood.org/; accessed 4 February 2016

Coons, Chris. 2012. "Internet Freedom is a Human Right." *HuffPost Politics: The Blog*. 10 May 2012. http://www.huffingtonpost.com/chris-coons/internet-freedom-is-a-hum_b_1506042.html; accessed 12 April 2015

Cortell, Andrew P. and James W. Davis. 2005. "When Norms Clash: International Norms, Domestic Practices, and Japan's Internalisation of the GATT/WTO." *Review of International Studies*. Vol. 31.1

Costa Rica Supreme Court. 2010. "12790 Exipediente: 09-013141-0007-CO" http://200.91.68.20/pj/scij/busqueda/jurisprudencia/jur_texto_sentencia.asp?nValor2=483874; accessed 30 May 2015

Cranston, Maurice. 2001. "Human Rights: Real and Supposed (1967)." in *The Philosophy of Human Rights*. Ed. Patrick Hayden. St. Paul, MN: Paragon House.

Crawford, Susan. 2013. *Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age*. New Haven, CT: Yale University Press.

Cruz, Neal H. "PLDT-Digitel mega-deal violates law." *Inquirer.net.* 27 May 2011. http://opinion.inquirer.net/5472/pldt-digitel-mega-deal-violates-law; accessed 15 January 2016

Cuban Constitution of 1976 (Amended 2002). Articles 53, 57, 58.

Culberston, Lauren. 2015. "Tumblr, Vimeo, Meetup, Kickstarter, Etsy, Union Square Ventures Support the FCC in Defending Net Neutrality as Intervenors in Court, File Opening Arguments." *Internet Freedom Business Alliance*. 21 September 2015. http://www.netfreedom.us/wp-content/uploads/2014/10/9.21.15ReleaseFinal.pdf; accessed 5 February 2016

Cultradigita. 2010. "Marco Civil da Internet: seus direitos e deveres em discussão [Internet Civil Framework: Their Rights and Duties Discussed]." http://culturadigital.br/marcocivil/debate/; accessed 11 December 2015

Dalangin-Fernandez, Lira. 2015. "Guess which legislation has been at the House of Representatives the longest? Nope, not RH bill." *Interaksyon*. 9 March 2015. http://www.interaksyon.com/business/106530/guess--which-legislation-has-been-at-the-house-of-representatives-the-longest-nope-not-rh-bill; accessed 16 January 2016

Dano, Mike. The 5 big issues the wireless industry is hiding from at this year's MWC." Fierce Wireless. 23 February 2016. http://www.fiercewireless.com/story/5-big-issues-wireless-industry-hiding-years-mwc/2016-02-23; accessed 26 February 2016

DeCosse, Sarah A. 1999. "Cuba's Repressive Machinery: Human Rights Forty Years After the Revolution." Human Rights Watch. http://pantheon.hrw.org/legacy/reports/1999/cuba/; accessed 8 November 2015

Demand Progress. 2013. "Campaigns." *Demand Progress.org*. http://www.demandprogress.org/campaigns/; accessed 15 June 2013

Democracy Now! 2013. "About." http://www.democracynow.org/about; accessed 3 December 2013

Democracy.Net.Ph. 2014. "Full Text of the Magna Carta for Philippine Internet Freedom (MCPIF)." http://democracy.net.ph/full-text/; accessed 18 January 2016

Digital Divide Institute. 2013. "Indonesian Breakthrough!" http://www.digitaldivide.org/#!ddi-indonesia/c22n6; accessed 1 November 2015

Domanski, Robert J. 2013. *Who Governs the Internet? The Emerging Policies, Institutions, and Governance of Cyberspace*. Ph.D. diss. CUNY Graduate Center.

Donahoe, Eileen and Maria Laura Canineu. 2015. "Brazil as the Global Guardian of Internet Freedom?" *Human Rights Watch*. 13 February 2015. https://www.hrw.org/news/2015/02/13/brazil-global-guardian-internet-freedom; accessed 25 November 2015

Duran, Rebeca. 2013. "Brazilian Regions." The Brazil Business. 21 October 2013. http://thebrazilbusiness.com/article/brazilian-regions; accessed 6 December 2015

D'Urso, Joseph. 2015. "Poor urban women in developing world use Internet less than men, lack skills, cash – survey." *Reuters*. 21 October 2015; http://finance.yahoo.com/news/poor-urban-women-developing-world-182354157.html;_ylt=A0LEVvcA4CdWhy4AxJUnnIlQ;_ylu=X3oDMTByMjB0aG5zBGNvbG8DYmYxBHBvcwMxBHZ0aWQDBHNlYwNzYw--; accessed 21 October 2015

Dutton, William H., Anna Dopatka, Ginette Law, and Victoria Nash. 2011. "Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet." *UNESCO*. http://unesdoc.unesco.org/images/0019/001915/191594e.pdf; accessed 3 December 2013

Dynamic Spectrum Alliance. 2016. "About Us." http://www.dynamicspectrumalliance.org/; accessed 28 February 2016

The Economist. 2013a. "China's Internet: A Giant Cage." 6 April 2013.

The Economist. 2013b. "Big maq attack." 26 October 2013

The Economist. 2014a. "Planet Plutocrat: Our crony-capitalism index." 15 March 2014.

The Economist. 2014b. "China in Africa: Empire of the sums." 23 August 2014.

The Economist. 2016. "Suppressed in Translation: How Chines Versions of UN Covenants Gloss Over Human Rights. *Facebook post*. 23 March 2016

Edwards, Scott. 2012. “Is Internet Access a Human Right?” *Amnesty International: Human Rights Now Blog*. 10 January 2012. http://blog.amnestyusa.org/business/is-internet-access-a-human-right/; accessed 1 February 2016

Eha, Brian Patrick. 2013. “An Accelerated History of Internet Speed (Infographic).” *Entrepreneur*. 23 September 2013. http://www.entrepreneur.com/article/228489; accessed 30 June 2015

eLac. 2015. “Digital Agenda for Latin America and the Caribbean.” 7 August 2015. http://conferenciaelac.cepal.org/sites/default/files/15-00757_elac_digital_agenda.pdf; accessed 8 January 2016

Engel, KeriLynn. 2014. “How Brazil Leads the World In Internet Freedom.” *Who Is Hosting This?* 20 August 2014. http://www.whoishostingthis.com/blog/2014/08/20/brazil-internet-freedom/

Epstein, Dmitry, Karina Alexanyan and Bruce Etling. 2009. “The State of the Internet in Russia.” 1 July 2009. *Internet and Democracy Project.* http://blogs.law.harvard.edu/idblog/2009/07/01/the-state-of-the-internet-in-russia/; accessed 31 August 2015

Erdbrink, Thomas. 2013. “Iranians Gain Access to Facebook at Twitter.” *New York Times*. 16 September 2013.

Erdbrink, Thomas. 2014. “Tehran Unfetters Cell Phones, and the Pictures Start Flowing. “ *New York Times.* 2 September 2014.

Ericsson. 2012. “Telcel partners with Ericsson for 4G/LTE launch in Mexico.” 7 November 2012. http://www.ericsson.com/news/121107-telcel-partners-with-ericsson-for-4g-lte-launch-in-mexico_244159017_c; accessed 9 January 2016

Estevez, Dolia. 2014. “In A Surprising Move, Mexican Billionaire Carlos Slim To Sell Telecom Assets In Compliance With New Anti-Trust Rules.” *Forbes*. 9 July 2014. http://www.forbes.com/sites/doliaestevez/2014/07/09/in-a-surprising-move-mexican-billionaire-carlos-slim-to-sell-telecom-assets-in-compliance-with-new-anti-trust-rules/; accessed 6 January 2016

Estevez, Dolia. 2015. “Why Has Carlos Slim Slipped In Forbes' Billionaires Ranking.” *Forbes*. 19 November 2015. http://www.forbes.com/sites/doliaestevez/2015/11/19/slims-spokesperson-says-america-movils-losses-and-stock-price-slide-not-a-concern/; accessed 6 January 2016

Eu, Gou Thean. “Indonesia to change licensing model for mobile operators.” Digital News Asia. 12 February 2015. https://www.digitalnewsasia.com/mobile-telco/indonesia-to-change-licensing-model-for-mobile-operators; accessed 31 October 2015

Evans, Tony and Peter Wilson. 1991. “Regime Theory and the English School of International Relations of International Relations: A Comparison.” *Millennium: Journal of International Studies*. Vol. 21.3.

Eyerys. 2015. “Google's Project Loon In Indonesia: The Large Ambition To Deliver Internet Connectivity.” http://www.eyerys.com/articles/news/google-loon-indonesia-large-ambition-deliver-internet-connectivity#sthash.NMoOPsOy.dpuf; accessed 12 April 2016

Farivar, Cyrus. 2016. “DOJ, FCC chairman ok Charter/Time Warner Cable deal, with a few caveats.” *Ars Technica.* 25 April 2016. http://arstechnica.com/tech-policy/2016/04/doj-fcc-chairman-ok-chartertime-warner-cable-deal-with-a-few-caveats/; accessed 8 June 2016

The Federal Communications Commission. 2005. “Making Connections.” *Federal Communications Commission: Communications History*. https://transition.fcc.gov/omd/history/internet/making-connections.html; 29 June 2015

The Federal Communications Commission. 2010. “Connecting America: The National Broadband Plan (Executive Summary)” 17 March 2010.

The Federal Communications Commission. 2014. “Protecting and Promoting the Open Internet.” *FCC*. 15 May 2014. https://www.fcc.gov/document/protecting-and-promoting-open-internet-nprm; accessed 10 July 2015

The Federal Communications Commission. 2016. “2016 Broadband Progress report.” 29 January 2016. https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2016-broadband-progress-report; accessed 26 February 2016

The Federal Communications Commission. 2016. “National Broadband Map.” http://broadbandmap.gov/; accessed 9 March 2016

The Federal Communications Commission. 2015. “FCC Finds that U.S. Broadband Deployment is not Keeping Pace.” 29 January 2015. https://apps.fcc.gov/edocs_public/attachmatch/DOC-331760A1.pdf; accessed 3 July 2015

Ferraz, Ezra. 2014. “New study predicts smartphone penetration in the Philippines will triple by next year.” *Tech in Asia*. 4 August 2014. https://www.techinasia.com/philippines-mobile-smartphone-penetration; accessed 17 January 2016

Fierce Telecom. 2013. “Municipal broadband contenders: Bristol, Va.” *Fierce Telecom*. 10 April 2013. http://www.fiercetelecom.com/special-reports/municipal-broadband-contenders-bristol-va; accessed 8 July 2015

Fierce Wireless. 2015. “How Verizon, AT&T, T-Mobile, Sprint and more stacked up in Q3 2015: The top 8 carriers.” *Fierce Wireless*. 12 November 2015. http://www.fiercewireless.com/special-reports/how-verizon-att-t-mobile-sprint-and-more-stacked-q3-2015-top-8-carriers; accessed 26 February 2016

File, Thom. 2013. “Computer and Internet Use in the United States: Population Characteristics.” *US Census Bureau*. May 2013. https://www.census.gov/prod/2013pubs/p20-569.pdf; 25 June 2015

Financial Tribune. 2015. “Parsijoo to be Launched in the September.” 6 July 2015. http://financialtribune.com/articles/economy-sci-tech/20623/parsijoo-be-launched-september; accessed 22 November 2015

Finnemore, Martha and Kathryn Sikkink. 1998. “International Norm Dynamics and Political Change,” *International Organization*, 52. 4.

Finnemore, Martha. 1996. “Norms, Culture, and World Politics.” *International Organization*. Vol. 50.2.

Fogo-Schensul, Credence. 1997. “More Than a River in Egypt: Holocaust Denials, the Internet, and International Freedom of Expression Norms.” *Gonzaga Law Review.* Vol. 33.241

FOM Group. 2015. “Internet in Russia: the dynamics of penetration.” *FOM Group*. http://fom.ru/SMI-i-internet/12275; accessed 12 August 2015, translated by Google Translate

Foot, Rosemary, John Gaddis and Andrew Hurrell. 2003. *Order and Justice in International Relations*. NY: Oxford.

ForeverGeek. 2007. “What did Online Access cost (per hour) in 1995?” *ForeverGeek*. 16 April 2007. http://www.forevergeek.com/2007/04/what_did_online_access_cost_per_hour_in_1995/; accessed 10 March 2016

Fortunato, Michael William-Patrick, Jeffrey C. Bridger, Theodore R. Alter, Grace M. Emmerling, Kathryn J. Ortbal, Mike Schwartz, Glenn E. Sterner III and William Shuffstall. 2013. "Promoting Fair Local Organizing for Broadband Delivery: Suggestions for Community-Level Action in Persistently Underserved Communities." *Journal of Information Policy*. Vol. 3

Fox News. 2009. "Top French Court Declares Internet Access a Basic Human Right." 12 June 2009. http://www.foxnews.com/story/2009/06/12/top-french-court-declares-internet-access-basic-human-right.html; accessed 31 May 2015

Free Press. 2015. "Tell the FCC: NO to Buyouts and YES to Buildouts." *FreePress.com*. http://act.freepress.net/sign/internet_charter_twc/; accessed 28 July 2015

Freedman, Eric and Richard Shafer. 2010. "Ambitious in Theory but Unlikely in Practice: A Critique of UNESCO's *Model Curricula for Journalism Education for Developing Countries and Emerging Democracies*." *Journal of Third World Studies*. Vol. 27.1.

Freedom 2 Connect Foundation. 2015. "Home." http://f2cf.org/; accessed 10 June 2015

Fukuda-Parr, Sakiko. 2011. "Theory and Policy in International Development: Human Development and the Capability Approach and the Millennium Development Goals." *International Studies Review*. Vol. 13.

Fundação Getúlio Vargas. 2015. "Mission and History." Fundação Getúlio Vargas http://portal.fgv.br/; accessed 11 December 2015

Fundación Pro Acceso. 2015. "About Us." http://www.proacceso.org.mx; accessed 29 December 2015

Gallagher, Sean. "How an Indonesian ISP took down the mighty Google for 30 minutes." *Ars Technica*. 6 November 2012. http://arstechnica.com/information-technology/2012/11/how-an-indonesian-isp-took-down-the-mighty-google-for-30-minutes/; accessed 24 October 2015

Galloway, Alexander R. 2004. *Protocol: How Control Exists After Decentralization*. Cambridge, Mass: MIT Press.

Galloway, Alexander R. and Eugene Thacker. 2007. *Exploit: A Theory of Networks.* Minneapolis: University of Minnesota Press.

Gang, Qian. 2013. "Parsing the 'public opinion struggle'" China *Media Project, University of Hong Kong*. http://cmp.hku.hk/2013/09/24/34085/; accessed 1 October 2015

Gatto, Raquel. 2015. "The Brazilian Experience of Public Consultation for the "Marco Civil Da Internet" and The Data Protection Law." *Internet Society*. 3 February 2015. http://www.internetsociety.org/blog/latin-america-caribbean-bureau-public-policy/2015/02/brazilian-experience-public-consultation-; accessed 8 December 2015

Gerovitch, Slava. 2008. "InterNyet: why the Soviet Union did not build a nationwide computer Network." *History and Technology*. Vol.24.4.

Gjelten, Tom. 2011. "Beyond the Cyber 'Disarmament' Debate." *Army*. Vol. 61.3

GlobeScan. 2010. "Four in Five regard Internet as a Right." BBC World Service Poll. 7 March 2010." http://www.worldpublicopinion.org/pipa/pdf/mar10/BBC_Internet_Poll.pdf; accessed 29 January 2016

Goldkorn, Jeremy. 2012. “Lexicon History of the Internet in China.” *Australian Centre of China in the World.* https://www.thechinastory.org/lexicon/the-internet/; accessed 3 October 2015

Golubev, Vladimir. 2015. “Glasnost defence foundation digest No. 737.” *Glasnost Defense Foundation*. 28 December 2015. http://www.gdf.ru/digest/item/1/1341; accessed 29 January 2016

Goswami, Divakar. 2007. “Non-transparent licensing for Palapa Ring project?” LIRNEasia. 10 May 2007. http://lirneasia.net/2007/05/non-transparent-licensing-for-palapa-ring-project/; accessed 1 November 2015

Government of Mexico. 2013. “National Digital Strategy.” http://embamex.sre.gob.mx/italia/images/pdf/national%20digital%20strategy.pdf; accessed 10 April 2016

Greiff, Thomas. 1985. “The Principle of Human Rights in Nationalist China: John C. H. Wu and the Ideological Origins of the 1946 Constitution.” *The China Quarterly*. Vol. 103.

Gross, Grant. 2015. “There's more to municipal broadband than public funding, says report.” *PC World*. 21 July 2015. http://www.pcworld.com/article/2950717/theres-more-to-municipal-broadband-than-public-funding-says-report.html; accessed 22 July 2015

Grossman, Luis Osvaldo. 2015. “REPNBL approves R $ 526.4 million in 4G projects in 450 MHz.” 13 July 2015. *Convêrgencia Digital*. http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?amp%253Bpost_data=&infoid=40078&sid=17; accessed 6 December 2015

Guerra, Lillian. 2015. “What Happens in Cuba after Fidel?” *HuffPost: 90 Miles: Rethinking the Future of U.S.-Cuba Relations*. http://www.huffingtonpost.com/lillian-guerra/what-happens-in-cuba-afte_b_6489034.html; accessed 8 November 2015

Guerrero, Alora Uy. 2014. “#20PHnet: A timeline of Philippine Internet.” *Yahoo News Singapore*. 19 March 2014. https://sg.news.yahoo.com/timeline-philippine-internet-20th-anniversary-225454753.html; accessed 16 January 2016

Guerrini, Federico. 2015. “The Future Of The Internet Will Be Discussed In New York, This Week. But Nobody Seems To Care.” *Forbes*. 13 December 2015. http://www.forbes.com/sites/federicoguerrini/2015/12/13/next-weeks-discussion-in-new-york-could-shape-how-the-internet-is-governed-for-the-next-decade/; accessed 14 December 2015

Gustin, Sam. 2014. “AT&T: We Deserve Tax Breaks, Municipal Broadband Doesn't.” *Motherboard*. 3 September 2014. http://motherboard.vice.com/read/att-we-deserve-tax-breaks-municipal-broadband-doesnt; accessed 19 March 2016

HaghighatNejad, Reza. 2016. “Iran’s “Halal Internet” and the Battle for Online Freedom.” 17 February 2016. https://en.iranwire.com/features/7088/; accessed 14 April 2016.

Hague v. Committee for International Organization. 1939. 307 U.S. 496.

Hamilton, David. 2015. “Chinese Search Engine Baidu Partners with CloudFlare to Speed Up, Secure Chinese Websites.” *Web Host Industry Review (theWHIR)*. 18 September 2015. http://www.thewhir.com/web-hosting-news/chinese-search-engine-baidu-partners-with-cloudflare-to-speed-up-secure-chinese-websites; accessed 4 October 2015

Hansenclever, Andreas, Peter Mayer, and Volker Rittberger. 1997. *Theories of International Regimes*. New York: Cambridge University Press.

Hanson, Elizabeth C. 2008. *The Information Revolution and World Politics.* Lanham, MD: Rowman & Littlefield.

Harding, Luke. 2014. "Putin considers plan to unplug Russia from the internet 'in an emergency'." 19 September 2014. *The Guardian*. http://www.theguardian.com/world/2014/sep/19/vladimir-putin-plan-unplug-russia-internet-emergency-kremlin-moscow; accessed 1 September 2015

Hart, Thomas. 2014. "China's Broadband Strategy." *Eurobiz*. 14 February 2014. http://www.eurobiz.com.cn/chinas-broadband-strategy/; accessed 17 October 2015

Hauben, Jay. 2004. "Across the Great Wall: The China-Germany Email Connection 1987-1994." *Colombia University.* http://www.columbia.edu/~hauben/china-email.doc; accessed 3 October 2015

Heimann Christopher L., Gary L. Phillips, and Lori A. Fink. 2014. "Comments of AT&T Inc." Federal Communications Commission. http://apps.fcc.gov/ecfs/document/view?id=7521825939; accessed 10 June 2016

Herold, David Kurt. 2012. "Escaping the World: A Chinese Perspective on Virtual Worlds." *Journal of Virtual Worlds Research*. Vol. 5.2.

History. 2010. "Mexico Timeline." A+E Networks. http://www.history.com/topics/mexico/mexico-timeline; accessed 3 January 2016

Hobden, Stephen and John M. Hobson. 2002. *Historical Sociology of International Relations*. Cambridge: Cambridge University Press.

Hodge, Graeme A. and Carsten Greve. 2007. "Public-Private Partnerships: An International Performance Review." *Public Administration Review*. Vol. 67.3.

Hogg, Chris. 2010. "China restores Xinjiang internet." *BBC News*. http://news.bbc.co.uk/2/hi/8682145.stm; accessed 3 October 2015

Holeywell, Ryan. 2013. "Why Isn't the U.S. Better at Public-Private Partnerships?" *Governing*. February 2013.

Hollis, Martin and Steve Smith. 1991. *Explaining and Understanding International Relations*, Oxford: Clarendon Press.

Holmes, Allan. 2014. "How big telecom smothers city-run broadband." *The Center for Public Integrity.* 28 August 2014. https://www.publicintegrity.org/2014/08/28/15404/how-big-telecom-smothers-city-run-broadband; accessed 10 June 2016

Hong, Yu, Francois Bar, and Zheng An. 2012. "Chinese telecommunications on the threshold of convergence: Contexts, possibilities, and limitations of forging a domestic demand-based growth model." *Telecommunications Policy*. Vol 36.

Horrigan, John B. and Maeve Duggan. 2015. "Home Broadband 2015. *Pew Internet & Technology*. 21 December 2015. http://www.pewinternet.org/2015/12/21/home-broadband-2015/; accessed 1 February 2016

HOTlink Informática. 2012. "Introduction to the Internet." *HOTlink Informática.* http://www.hotlink.com.br/suporte/suporte-manual3.php; accessed 25 November 2015

HUD. 2015. “About the Pilot.” Department of Housing and Urban Development. http://connecthome.hud.gov/; accessed 9 February 2016.

Huerta, Esperanza and Rodrigo Sandoval-Almazán. 2007. “Digital Literacy: Problems Faced by Telecenter Users in Mexico.” *Information Technology for Development*. Vol. 13.3

Hughes. 2012. “Mexico’s National Satellite Broadband System.” Winter 2012. http://www.hughes.com/company/newsletters/winter-2012/mexicos-national-satellite-broadband-system; accessed 4 January 2016

Human Rights Watch. 2013. “Laws of Attrition: Crackdown on Russia’s Civil Society after Putin’s Return to the Presidency.” *Human Rights Watch*. 24 April 2013. https://www.hrw.org/report/2013/04/24/laws-attrition/crackdown-russias-civil-society-after-putins-return-presidency; accessed 10 September 2015

Human Rights Watch. 2015. “World Report 2015: Cuba.” *Human Rights Watch*. https://www.hrw.org/world-report/2015/country-chapters/cuba; accessed 8 November 2015

Hurrell, Andrew. 2007. *On Global Order: Power, Values, and the Constitution of International Society*. NY: Oxford University Press.

IBM. 2016. “IBM Exhibits: Philippines Chronology.” *IBM Archive*. https://www-03.ibm.com/ibm/history/exhibits/asia/Philippines_ch1.html; accessed 16 January 2016

ICT Office. 2015. “Life of a Modern Day Hero.” *Republic of the Philippines, Department of Science and Technology*. 5 November 2015. http://icto.dost.gov.ph/tech4ed/life-of-a-modern-day-hero/; accessed 12 January 2016

ICT Office. 2015. “Tech4ED Centers to provide equal opportunities in San Carlos City, Negros Occidental.” *Republic of the Philippines, Department of Science and Technology*. 14 December 2015. http://icto.dost.gov.ph/tech4ed/tech4ed-centers-to-provide-equal-opportunities-in-san-carlos-city-negros-occidental/; accessed 12 January 2016

ICT Office. 2016. “About Tech4ED.” *Republic of the Philippines, Department of Science and Technology*. http://icto.dost.gov.ph/tech4ed/tech4ed/; accessed 12 January 2016

ICT Office. 2016. “About Us.” *Republic of the Philippines, Department of Science and Technology*. http://icto.dost.gov.ph/transparency/about-us/; accessed 12 January 2016

IFT. 2016. “Quality of Service.” http://www.ift.org.mx/usuarios-de-internet/calidad-del-servicio; accessed 6 January 2016

IGF. 2013. “About the Internet Governance Forum.” *Internet Governance Forum.* http://www.intgovforum.org/cms/aboutigf; accessed 10 June 2013

Ignatius, Adi. 2007. “A Tsar is Born.” *Time Magazine.* 19 December 2007.

Insider Surveillance. 2014. “Cisco, Huawei and Semptian: A Look Behind the Great Firewall of China.” *Insider Surveillance*. 15 December 2014. https://insidersurveillance.com/cisco-huawei-and-semptian-a-look-behind-the-great-firewall-of-china/; accessed 19 October 2015

The Institute for Research in Fundamental Sciences. 2012. “About IPM.” http://www.ipm.ac.ir/about-IPM.jsp; accessed 12 November 2015

Instituto Nacional de Estadística y Geografía. 2014. “Los microdatos del Módulo sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (MODUTIH)."

http://www3.inegi.org.mx/sistemas/microdatos/encuestas.aspx?c=34519&s=est; accessed 1 January 2016

International Telecommunications Union. 2015. "ICT Facts and Figures: the World in 2015." 25 May 2015. http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf; accessed 9 April 2016

Internet Association. 2014. "Wireless Net Neutrality Survey." *Internet Association*. 30 September 2014. http://internetassociation.org/wp-content/uploads/2014/09/TIA-Wiress-Net-Neutrality-Survey.pdf; accessed 5 February 2016

Internet Para Todos. 2016. "Únete, colabora con nosotros." http://internetparatodos.mx/#; accessed 9 January 2016.

Internet Society China. 2013. "About Internet Society of China." Internet Society China. 20 July 2013. http://www.isc.org.cn/english/About_Us/Introduction/listinfo-15315.html; accessed 30 January 2016.

Internet Society. 2012. "Capitulo Mexico." 7 June 2012. http://www.isocmex.org.mx/historia.html; accessed 15 December 2015

Internet Society. 2012. "Global Internet User Survey 2012." *Internet Society*. https://www.internetsociety.org/sites/default/files/GIUS2012-GlobalData-Table-20121120_0.pdf; accessed 9 June 2015

Ipsos MediaCT. 2013. "Our Mobile Planet: Russia (Executive Summary and Data Set). *Google*. http://services.google.com/fh/files/misc/omp-2013-ru-en.pdf; accessed 15 September 2015

Iran, Defenders of Human Rights Center. 2013. "Human rights organisations call on Human Rights Council to renew Iran Special Rapporteur's mandate." http://www.humanrights-ir.org/?p=870; accessed 30 January 2016

Iranian Constitution of 1979.

Iranian Students News Agency. 2013. "Which provinces have the most Internet users?" 29 June 2013. http://isna.ir/fa/news/92040804109

IRNA. 2015. "Iran's Internet infiltration up at 82 pct." *Islamic Republic News Agency*. 11 September 2015. http://www.irna.ir/en/News/81830507/; accessed 15 November 2015

IS. 2013. "Who We Are." *Internet Society.* http://www.Internetsociety.org/who-we-are; accessed 12 June 2013

Isenberg, David. 1998. "Rise of the Stupid Networks." http://www.rageboy.com/stupidnet.html; accessed 11 June 2015

Isenberg, David. 2015. "About F2C 2015." *Isen.com*. http://freedom-to-connect.net/; accessed 1 June 2015

ITU and OECD. 2011. "M-Government: Mobile Technologies for Responsive Governments and Connected Societies." http://www.itu.int/ITU-D/cyb/app/m-gov.html; accessed 17 January 2016.

ITU. 1998. "Resolution 73 of the ITU Plenipotentiary Conference, Minneapolis, 1998." http://www.itu.int/net/wsis/docs/background/resolutions/73.html; accessed 10 April 2016

ITU. 2013. "Our Vision." *International Telecommunications Union.* http://www.itu.int/en/about/Pages/vision.aspx; accessed 30 September 2013

ITU. 2015a. "ITU Data Collection and Questionnaires." *ITU*. http://www.itu.int/en/ITU-D/Statistics/Pages/datacollection/default.aspx#questionnaires; accessed 18 November 2015

ITU. 2015b. "MTN Irancell claims 12.5 million 3G subscribers (Iran)." ITU: ICT Statistics Newslog. 22 September 2015; accessed 15 November 2015

Jackson, Robert. 2000. *The Global Covenant: Human Conduct in a World of States*. New York: Oxford University Press.

Jacobs, Andrew. 2013. "Over News of Clash, a Shroud of Silence in Xinjiang." *New York Times*. 26 August 2013.

Jacques, Martin. 2009. *When China Rules the World: The End of the Western World and the Birth of a New Global Order.* New York: Penguin Press.

"Jakarta Declaration for Meaningful Broadband." 14 April 2011. Indonesia International Infrastructure Conference and Exhibition 2011. http://media.wix.com/ugd/7efb06_047233dbf0814ada8fa9744ef6f97052.pdf; accessed 1 November 2015

Jinkings, Daniella. 2011. "Government presents the proposal of the Civil Marco Internet to Congress." *Agência Brasil*. 24 August 2011. http://memoria.ebc.com.br/agenciabrasil/noticia/2011-08-24/governo-apresenta-proposta-do-marco-civil-da-internet-ao-congresso-nacional; accessed 11 December 2015

Johnston, Raúl Pérez. 2016. "A Historical Evolution of Human Rights in Mexico as a form of understanding Mexico's commitment to Human Rights." Diplomatico Escritores. http://www.diplomaticosescritores.org/revistas/21_4.htm; accessed 4 January 2016

Joint Foreign Chambers. 2010. "Advocacy Paper: Arangkada Philippines 2010: A Business Perspective, Infrastructure: Telecommunications and Information Technology." December 2010. http://www.investphilippines.info/wp-content/uploads/2010/12/13.-Part-3-Seven-Big-Winner-Sectors-Infrastructure-Telecommunications1.pdf; accessed 16 January 2016

Jung, John. 2014. "Bridging the digital divide in Rio de Janeiro." *EconomicDevelopment.org.* http://economicdevelopment.org/2014/03/bridging-the-digital-divide-in-rio-de-janeiro/; accessed 30 November 2015

Kahler, Miles. 1997. "Inventing International Relations: International Relations Theory After 1945." in *New Thinking in International Relations Theory*. eds. Michael Doyle and John Ikenberry. Boulder, CO: Westview Press. 20-53.

Kang, Cecelia. 2010. "Google says no timetable to leave China; lawmakers tell firms to stand up to censors." *The Washington Post.* 2 March 2010. http://voices.washingtonpost.com/posttech/2010/03/google_says_no_timetable_to_le.html; accessed 10 July 2015.

Kaspar, Lea. 2015. "The Road to WSIS+10: Key Country Perspectives in the Ten-Year Review of the World Summit on the Information Society." *Global Partners Digital.* September 2015. http://www.gp-digital.org/wp-content/uploads/pubs/WSIS+10%20Country%20Mapping%20Complete%20Draft%20150904%20-%20final%20minus%20pg%207&13%20-%20altered%20layout%20fixed%20FINAL.pdf; accessed 18 March 2016

Keane, Jonathan. 2015. “Mexico: State intervention & the end of the digital divide.” *IDG Connect*. 12 August 2015. http://www.idgconnect.com/abstract/10270/mexico-state-intervention-digital-divide; accessed 15 December 2015

Keck, Margaret E and Kathryn Sikkink. 1998. *Activists Beyond Borders*. Ithaca: Cornell University Press.

Kelly, Sanja et al. 2014. “Freedom on the Net 2014.” *Freedom House.* https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf; accessed 23 February 2015

Kelly, Sanja, Madeline Earp, Laura Reed, Adrian Shahbaz, and Mai Truong. 2015. “Freedom on the Net 2015.” Freedom House. https://www.freedomhouse.org/sites/default/files/FOTN%202015%20Full%20Report.pdf; accessed 30 October 2015

Keohane, Robert O. and Joseph S. Nye, Jr. 1998. "Power and Interdependence in the Information Age." *Foreign Affairs*. Vol. 77.5

Kleibrink, Alexander. 2011. “The EU as Norm Entrepreneur: the Case of Lifelong Learning.” *European Journal of Education*. Vol. 46.1

Klotz, Audie and Cecelia Lynch. 2007. *Strategies for Research in Constructivist International Relations*. Armonk, NY: M.E. Sharp, Inc.

Knight, Peter T. 2014. *The Internet in Brazil: Origins, Strategy, Development, and Governance*. Bloomington, IN: Author House LLC.

Knight, Peter T. 2016. “Re: Brazilian Internet Culture.” Message to Heather Katz 22 January 2016. Email.

Knoll, Amy. 1996. “Any Which Way But Loose: Nations Regulate the Internet.” *Tulane Journal of International and Comparative Law*. Vol. 275.4

Krasner, Stephen D. 1982. “Structural Causes and Regime Consequences: Regimes as Intervening Variables.” *International Organization*. Vol. 36.2.

Krasner, Stephen D. 1983. *International Regimes*. Ithaca, NY: Cornell University Press.

Kratochwil, Friedrich. 2005. “Religion and (Inter-)National Politics: On the Heuristics of Identities, Structures, and Agents.” *Alternatives: Global, Local, Political*. Vol. 30.2.

Krook, Mona Lena and Jacqui True. 2010. “Rethinking the life cycles of international norms: The United Nations and the Promotion of gender equity.” *European Journal of International Relations*. Vol. 18.1.

Kull, Steven, Clay Ramsey, Stephen Weber, Evan Lewis, Melinda Brouwer, Melanie Ciolek, and Abe Medoff. 2008. “World Public Opinion on Freedom of the Media.” *WorldPublicOpinion.org*. 1 May 2008. http://www.worldpublicopinion.org/pipa/articles/btjusticehuman_rightsra/477.php?nid=&id=&pnt=477//www.worldpublicopinion.org/pipa/articles/btjusticehuman_rightsra/477.php?nid=&id=&pnt=477; accessed 29 January 2016

La Rue, Frank. 2011. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27.” *United Nations General Assembly—Human Rights Council*

Larano, Chris. 2015. “Internet Access in Indonesia Closer to Laos Than Thailand.” *Wall Street Journal*. 27 March 2015. http://blogs.wsj.com/indonesiarealtime/2015/03/27/internet-access-in-indonesia-closer-to-laos-than-thailand/; accessed 24 October 2015

Legro, Jeffrey W. 1997. “Which Norms Matter? Revisiting the Failure of ‘Internationalism.’” *International Organization*. Vol. 51.1.

Lei No. 12.965, 23.04.2014 (Marco Civil da Internet)

Lemos, Ronaldo. 2007. “Brazilian Internet needs civil regulatory framework.” *Universo Online*. 22 May 2007. http://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm; accessed 11 December 2015

Lerner, Melissa Y. 2010. “Connecting the Actual with the Virtual: The Internet and Social Movement Theory in the Muslim World—The Cases of Iran and Egypt.” *Journal of Muslim Minority Affairs*. Vol. 30.4.

Liang, June. 2010. “The Internet in China.” *People’s Daily Online*. 8 June 2010. http://en.people.cn/90001/90776/90785/7017204.html; accessed 30 October 2015.

Linklater, Andrew and Hidemi Suganami. 2002. *English School of International Relations: A Contemporary Reassessment*. West Nyack, NY: Cambridge University Press.

Llorente, Elizabeth. 2015. “Cuba's desire to open STI economy is stymied by refusal to yield control US Officials say.” *Fox News Latino*. http://latino.foxnews.com/latino/politics/2015/11/02/cuba-desire-to-open-its-economy-is-stymied-by-refusal-to-cede-control-us/&usg=ALkJrhi0kx5fIwlyD5OuGYgOEtK0bMrFOg; accessed 6 November 2015

Loo, Becky P.Y. 2004. “Telecommunications reforms in China: towards an analytical framework.” *Telecommunications Policy*. Vol. 28.

Lovegrove, Caitlin. 2015. “SSG’s Partnership to Advance Internet Connectivity Promotes Sustainable Fishing, Saves Lives, and Wins Prestigious Award.” *SSG Advisors*. 6 October 2015. http://ssg-advisors.com/tag/philippines/; accessed 15 January 2016

Lure, Emmanuel. 2015. “Telkom, Indosat Resume Rivalry in Palapa Ring II Fiber Optic Project.” Jakarta Globe. 3 August 2015. http://jakartaglobe.beritasatu.com/business/telkom-indosat-resume-rivalry-palapa-ring-ii-fiber-optic-project/; accessed 31 October 2015

Magkilat, Bernie. 2014. “Free Internet for 600 towns in 2015.” *Manila Bulletin*. 13 October 2014. http://www.mb.com.ph/free-internet-for-600-towns-in-2015/; accessed 15 January 2016

Manyika, James , Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, and Angela Hung Byers. 2011. “Big data: The next frontier for innovation, competition, and productivity.” *McKinsey Global Institute*. http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation; accessed 19 October 2015

Mari, Angelica. 2015. “Facebook to bring Internet.org to Brazil.” *ZDNet*. 14 April 2015. http://www.zdnet.com/article/facebook-to-bring-internet-org-to-brazil/#!; accessed 6 December 2015

McCoy, Alfred W. 1999. “Dark Legacy: Humane Rights Under the Marcos Regime." Conference Presentation at “Legacies of the Marcos Dictatorship.” Ateneo de Manila University 20 September

1999. on *Hartford Web Publishing*. http://www.hartford-hwp.com/archives/54a/062.html; accessed 17 January 2016

Mearsheimer, John. 2001. *The Tragedy of Great Power Politics.* New York: W.W. Norton & Co.

Mediatelecom Informative Agency. 2015. "Brazilian mobile broadband grows three times faster than the global average." Aetechno. 25 May 2015. http://tecno.americaeconomia.com/articulos/banda-ancha-movil-crece-tres-veces-mas-rapido-que-el-promedio-mundial; accessed 6 December 2015

Mehr News Agency. 2015a. "China to help Iran complete National Internet." 13 June 2015. http://en.mehrnews.com/news/107869/China-to-help-Iran-complete-National-Internet; accessed 10 November 2015

Mehr News Agency. 2015b. "Iran launches domestic search engine Yooz." 16 February 2015. http://en.mehrnews.com/news/105970/Iran-launches-domestic-search-engine-Yooz; accessed 10 November 2015

Mehr News Agency. 2015c. "Iran ranks 4th in world in web hosting." 9 November 2015. http://en.mehrnews.com/news/111799/Iran-ranks-4th-in-world-in-web-hosting; accessed 10 November 2015

Mehr News Agency. 2015d. "Leader issues 6th Development Plan general policies." 30 June 2015. http://en.mehrnews.com/news/108305/Leader-issues-6th-Development-Plan-general-policies; accessed 10 November 2015

Merritt, Humberto. 2011. "Information technologies and the evolution of the digital divide in Mexico: a public policy approach." *Análisis Económico*. Vol 26.62.

Merry, Sarah Engle. 2006. *Human Rights and Gender Violence: Translating International Law into Local Justice*. Chicago: University of Chicago Press.

Mesher, G., Briggs, R., Goodman, S, Press, L., and Snyder, J. 1992. "Cuba, Communism, and Computing," *Communications of the ACM*. November 1992

Mexico Conectado. 2015a. "Mexico Conectado is Awarded WSIS Prize 2015." 26 May 2015. http://mexicoconectado.gob.mx/notas.php?id=265&cat=79; accessed 3 January 2016

Mexico Conectado. 2015b. "Mexico asume le presidencia de eLAC 2018. " http://mexicoconectado.gob.mx/notas.php?id=281&cat=65; accessed 5 January 2016

Meyer, David S. 2004. "Protest and Political Opportunities." *Annual Review of Sociology*. Vol. 30.

Mill, John Stuart. 1863. *A System of Logic, Ratiocinative and Inductive: Being a Connected View of the Principles of Evidence and the Methods of Scientific Investigation, Volume 1*. Google Books. https://play.google.com/store/books/details?id=y4MEAAAAQAAJ&rdid=book-y4MEAAAAQAAJ&rdot=1; accessed 12 April 2015

Minárik, Tomáš. 2014. "New UN Resolution Amplifies Call for Right to Privacy in the Light of Mass Surveillance." NATO Cooperative Cyber Defence. 18 December 2014. https://ccdcoe.org/new-un-resolution-amplifies-call-right-privacy-light-mass-surveillance.html; accessed 13 December 2015

Ministério das Comunicações. 2014. "Programa Nacional de Banda Larga: Situação em junho de 2014." June 2014. balanco-pnbl-21072014.pdf; accessed 6 December 2015

Ministry of Communication and Information. 2012. “2012 Indonesia ICT White Paper.” http://sdppi.kominfo.go.id/info_view_c_26_p_2097.htm; accessed 24 October 2015

Ministry of Communication and Information. 2013. “Palapa Ring KTI Accelerate Development.” 13 May 2013. http://www.telkom.co.id/en/telkom-membangun-backbone-serat-optik-mataram-kupang-cable-system.html; accessed 30 October 2015

Ministry of Telecom and Mass Communications of the Russian Federation. 2014. “Nikolay Nikiforov Told about Development of ICT to the Students of International University in Moscow.” 25 September 2014. *Ministry of Telecom and Mass Communications of the Russian Federation*. http://minsvyaz.ru/en/events/31626/; accessed 10 September 2015

Mirandilla-Santos, Mary Grace P. 2011. “Chapter 5: Unleashing the Power of Competition: the Philippine Telecommunications Reform Story.” In *Built on Dreams, Ground in Reality: Economic Policy Reform in the Philippines*. Makati City: The Asia Foundation.

Mitra, Luzviminda S. and Charles Van T. Miraflores. “Chapter/sector: Accelerating Infrastructure Development.” Philippines Statistics Authority. 24 July 2015. http://www.nscb.gov.ph/stats/statdev/2014/ch4_infrastructure.asp; accessed 15 January 2016

Mohebali, Amir Hossein, Mohammad Shirazi, and Kaveh Bazargan. 2013. “ICT Measurement for Iran (IMI):A Progress Report.” 11th World Telecommunication/ICT Indicators Symposium. 6 December 2013. http://www.itu.int/en/ITU-D/Statistics/Documents/events/wtis2013/026_E_doc.pdf; accessed 15 November 2015

Montenegro, Lourdes O. and Eduardo Araral, Jr. “Shared Prosperity: An ICT Manifesto for the Philippines for 2016 and Beyond.” Lee Kuan Yew School of Public Policy and Microsoft. 25 November 2015. https://download.microsoft.com/documents/apac/IC-Manifesto-for-the-Philippines.pdf; accessed 15 January 2016.

Morozov, Evgeny. 2011. *The Net Delusion: The Dark Side of Internet Freedom.* New York: Public Affairs, Perseus Books Group.

Morris, Amanda. 2015. “Research shows Cuba's Internet issues.” Phys.org. 31 October 2015. http://phys.org/news/2015-10-cuba-internet-issues.html; accessed 6 November 2015

Morris, Frank. “Another First for Kansas City: Free Google Fiber For Low-Income Housing Residents.” *KCUR 89.3*. 4 February 2016. http://kcur.org/post/another-first-kansas-city-free-google-fiber-low-income-housing-residents#stream/0; accessed 9 February 2016

Morris, Justin. 2005. “Normative Innovation and Great Powers.” in *International Society and Its Critics.* NY: Oxford University Press.

Moskvitch, Katia. 2013. “Russia's anti-internet piracy law faces backlash.” *BBC*. http://www.bbc.com/news/technology-23510065; accessed 20 August 2015

Mueller, Milton. 2002. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: MIT Press.

Mulyana, Eueung. 2008. “Palapa Ring (1).” *Personal blog post.* 9 February 2008. http://soft-brain.blogspot.com/2008/02/palapa-ring-1.html; accessed 1 November 2015

National Autonomous University of Mexico. 2008. “Mexico Computing, Chronology, and Applications.” http://computo50.unam.mx/computoenmexico2.html; accessed 15 December 2015

National People's Congress. 2007. "People's Republic Antimonopoly Law." *NPC, Google Translate*; https://translate.googleusercontent.com/translate_c?act=url&depth=1&hl=en&ie=UTF8&prev=_t&rurl=translate.google.com&sl=zh-CN&tl=en&u=http://www.npc.gov.cn/wxzl/gongbao/2007-10/09/content_5374672.htm&usg=ALkJrhiRv7ieSPUTallyb2OC42LPSZZDzQ; accessed 18 October 2015

Nefedov, Pavel and Aleksander Boreiko. 2001. "Cabinet Approves E-Russia Plan." *The Moscow Times*. 10 July 2001. http://www-cf.themoscowtimes.com/news/article/tmt/252663.html; accessed 15 September 2015

NETmundial Initiative Secretariat. 2016. "NETmundial Initiative Inaugural Coordination Council Madrid, Spain, 26 February 2016 Communiqué." *NETMundial.org*. 26 February 2016. https://www.netmundial.org/blog/secretariat/netmundial-initiative-inaugural-coordination-council-madrid-spain-26-february-2016; accessed 5 March 2016

NETmundial. 2014. "NETmundial Multistakeholder Agreement." 24 April 2014. http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf; accessed 4 March 2016

Nevers, Renee de. 2007. "Imposing International Norms: Great Powers and Norm Enforcement." *International Studies Review*. Vol. 9.

New York Times Co. v. United States. 1971. 403 U.S. 713.

Newport, Frank. 2013. "Americans Disapprove of Government Surveillance Programs." *Gallup*. 12 June 2013. http://www.gallup.com/poll/163043/americans-disapprove-government-surveillance-programs.aspx; accessed 31 January 2016

Newth, Mette. 2002. "On Censorship: Russia." *Beacon for Freedom of Expression*. http://www.beaconforfreedom.org/liste.html?tid=415&art_id=555; accessed 21 August 2015

Newton, Harry. 2009. *Newton's Telecom Dictionary*. NY: Flatiron Publishing.

Nikiforov, Nikolay. 2015. "Nikolay Nikiforov Took Part in the Extended Session of Rossvyaz." *Ministry of Telecom and Mass Communications of the Russian Federation*. 14 May 2015. http://www.minsvyaz.ru/en/events/33210/; accessed 14 March 2016

Noam, Eli. 2011. "Let Them Eat Cellphones: Why Mobile Wireless is No Solution for Broadband." *Journal of Information Policy.* Vol. 1.

Novais, Andréa. 2011. "Social Classes in Brazil." *The Brazil Business.* 7 October 2011. http://thebrazilbusiness.com/article/social-classes-in-brazil; accessed 6 December 2015

Numbeo. 2016. "Cost of Living (by Country)." *Numbeo*. http://www.numbeo.com/cost-of-living/; accessed 27 February 2016.

Obama, Barack. 2009. "Remarks by President Barack Obama at Town Hall Meeting with Future Chinese Leaders." The White House, Office of the Press Secretary. https://www.whitehouse.gov/the-press-office/remarks-president-barack-obama-town-hall-meeting-with-future-chinese-leaders; accessed 31 July 2015

OECD. 2014. "OECD Fixed (wired) broadband subscriptions per 100 inhabitants, by technology, June 2014." OECD Broadband Portal. http://www.oecd.org/internet/broadband/oecdbroadbandportal.htm; accessed 18 June 2015

Olesen, Alexa. 2014. "Welcome to the Uighur Web." *Foreign Policy;* 21 April 2014. http://foreignpolicy.com/2014/04/21/welcome-to-the-uighur-web/; accessed 3 October 2015

Ong, Janet. 2008. "China Begins Revamp of Telecommunications Industry, Xinhua Says." *Bloomberg.* 23 May 2008. http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a_ryexF4S2NI&refer=home; accessed 18 October 2015

ONI. 2013. "United States and Canada Regional Profile." *Open Net Initiative.* https://opennet.net/research/regions/united-states-and-canada. Accessed 1 June 2013

Ookla. 2015. "Net Index United States." *Ookla Net Index*. http://www.netindex.com/download/2,1/United-States/; accessed 1 July 2015

OpenNet Initiative. 2009. "Iran." https://opennet.net/research/profiles/iran; accessed 15 November 2015

Ordinario, Cai U. 2016. "Millions of Filipinos suffer the social injustice of digital divide: World Bank report." *Business Mirror.* 14 January 2016. http://www.businessmirror.com.ph/millions-of-filipinos-suffer-the-social-injustice-of-digital-divide-world-bank-report/; accessed 15 January 2016

Pagliery, Jose. 2015. "OMG: 2.1 million people still use AOL dial-up." CNN Money. 8 May 2015. http://money.cnn.com/2015/05/08/technology/aol-dial-up/; accessed 10 March 2016

Pagulong, Charmie Joy and Louella Desiderio. 2015. "Facebook offers free internet access in Phl." *The Philippine Star*. 20 March 2015. http://www.philstar.com/headlines/2015/03/20/1435536/facebook-offers-free-internet-access-phl; accessed 16 January 2016

Paquette, Emmanuel. 2015. "Orange veut développer Internet à Cuba." *L'Express*. 21 January 2015. http://lexpansion.lexpress.fr/high-tech/orange-veut-developper-internet-a-cuba_1642932.html; accessed 9 November 2015

Park, Han Woo. 2003. "Hyperlink Network Analysis: A New Method for the Study of Social Structure on the Web." *Connections*. Vol. 25.1

Pars Online. 2015. "High Speed Internet in Iran ParsOnline." http://www.parsonline.com/old/en/services/adsl/adsl_iran; accessed 20 November 2015

Paul Budde Communication Pty Ltd. 2015. "Philippines - Major Telecommunications Operators." June 2015. *Report Linker.* http://www.reportlinker.com/p01658108-summary/Philippines-Major-Telecommunications-Operators.html; accessed 15 January 2016

Paz, Luis Rondon. 2015. "The Two Faces of Cuba's Wi-Fi Services." *Havana Times*. 21 October 2015. http://www.havanatimes.org/?p=114548; accessed 8 November 2015

PBS. 2010. "Timeline: A Modern History of Iran." *PBS Newshour*. 11 February 2010. http://www.pbs.org/newshour/updates/middle_east-jan-june10-timeline/; accessed 16 November 2015

Penn, Michael. 2015. "Views from Around the Globe: 2nd Annual Poll on How Personal Technology is Changing Our Lives." Microsoft Corporation. http://mscorp.blob.core.windows.net/mscorpmedia/2015/01/2015DavosPollFINAL.pdf; accessed 13 December 2015

Pensando o Direito. 2015a. "Marco Civil: The Debate by the Numbers" Ministério da Justiça. http://pensando.mj.gov.br/marcocivil/debate-em-numeros/; accessed 11 December 2015

Pensando o Direito. 2015b. "Society may make Decree of text proposed for the Civil Marco Internet." Ministério da Justiça. 6 May 2015. http://pensando.mj.gov.br/marcocivil/2015/05/sociedade-

podera-formular-proposta-de-texto-de-decreto-para-o-marco-civil-da-internet/; accessed 11 December 2015

Perrin, Andrew. 2015. "One-fifth of Americans report going online 'almost constantly.'" *Pew FactTank*. 8 December 2015. http://www.pewresearch.org/fact-tank/2015/12/08/one-fifth-of-americans-report-going-online-almost-constantly/; accessed 1 February 2016

Perritt, Henry H. Jr. 1998. "The Internet is Changing International Law." *Kent Law Review*. Vol. 73.

Pew Research Center. 2013a. "Broadband and Smartphone Adoption Demographics." Pew Research Center. 27 August 2013. http://www.pewinternet.org/2013/08/27/broadband-and-smartphone-adoption-demographics/; accessed 30 June 2015

Pew Research Center. 2013b. "Broadband vs. Dial-up Adoption Over Time." Pew Research Center. September 2013. http://www.pewinternet.org/data-trend/internet-use/connection-type/; accessed 30 June 2015

Pew Research Center. 2014a. "US feelings on the Internet: the Internet at 25." *Pew Internet*. http://www.pewinternet.org/files/2014/02/PIP_SurveyQuestions_Webat25.pdf; accessed 1 February 2016.

Pew Research Center. 2014b. "Emerging Developing States want Internet Freedom." http://www.pewglobal.org/2014/03/19/emerging-and-developing-nations-want-freedom-on-the-internet/; accessed 29 January 2016

Pew Research Center. 2015a. "US Smartphone Use in 2015." Pew Research Center. 1 April 2015. http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/; accessed 30 June 2015

Pew Research Center. 2015b. "Global Support for Principle of Free Expression, but Opposition to Some Forms of Speech." 18 November 2015. http://www.pewglobal.org/files/2015/11/Pew-Research-Center-Democracy-Report-FINAL-November-18-2015.pdf; accessed 23 February 2016

Pew Research Center. 2015c. "Brazilian Public Disapproving of Most of U.S. Spying Program." *Pew Research Center*. 29 June 2015. http://www.pewresearch.org/fact-tank/2015/06/29/brazilians-views-of-u-s-rebound-as-wounds-of-nsa-scandal-heal/brazill6-29-2015-11-13-55-am/; accessed 14 December 2015

PhilRights. 2014. "The Declaration of Cyber-Martial Law: Examining the Provisions of the Cybercrime Prevention Act from a Human Rights Perspective." *Philippine Human Rights Center*. 24 September 2014. http://philrights.org/the-declaration-of-cyber-martial-law-examining-the-provisions-of-the-cybercrime-prevention-act-from-a-human-rights-perspective/; accessed 30 January 2016

PhilSite. 2016. "Philippine History." 10 January 2016. http://www.philippine-history.org/; accessed 16 January 2016

Pinho, Larissa and Katitza Rodriguez. 2015. "The Devil in the Detail." *Electronic Frontier Foundation.* 25 February 2015. https://www.eff.org/deeplinks/2015/02/marco-civil-devil-detail; accessed 25 November 2015

Pinlac, Melanie Y. "Marcos and the Press." 1 September 2007. *Center for Media Freedom and Responsibility*. http://www.cmfr-phil.org/2007/09/01/marcos-and-the-press/; accessed 17 January 2016

PNA. 2015. “Using TV White Space for Internet Connectivity.” *Metro Cebu News*. 13 December 2015. http://metrocebu.com.ph/2015/12/using-tv-white-space-for-internet-connectivity/; accessed 15 January 2016

Pool, Ithiel de Sola. 1983. *Technologies of Freedom*. Harvard, CT: Belknap University Press.

Pourghadiri, Bahram. 2014. “The bewildering maze of Internet usage statistics in Iran.” *Netbina*. 8 August 2014. http://www.netbina.com/blog/2014/8/8/internet-usage-in-iran; accessed 22 November 2015.

PPP Knowledge Lab. 2014. “Public Private Partnerships: A Reference Guide, Version 2.0.” Asian Development Bank, International Bank for Reconstruction and Development, and World Bank Group.https://library.pppknowledgelab.org/Knowledge%20Lab/documents/2480/download; accessed 22 January 2016

Preimesberger, Chris. 2015. “FCC Adds Mobile Broadband to Net Neutrality Rules, Prepares for Litigation.” *E Week*. 12 March 2015. http://www.eweek.com/mobile/fcc-adds-mobile-broadband-to-net-neutrality-rules-prepares-for-litigation.html; accessed 26 February 2016

Press, Larry, Grey Burkhart, Will Foster, Seymour Goodman, Peter Wolcott, and Jon Woodard. 1998. “An Internet Diffusion Framework.” Communications of the ACM, Vol. 41.10. http://som.csudh.edu/fac/lpress/articles/acmfwk/acmfrwk.htm; accessed 6 November 2015

Press, Larry. 1991. “A Computer Network for Democracy and Development.” Self Published. http://www.ibiblio.org/pub/docs/about-the-net/Usenet/soviet.coup; accessed 30 August 2015

Press, Larry. 1998. “The Internet in Cuba.” in *The MOSAIC Group*, The Global Diffusion of the Internet Project, An Initial Inductive Study, pp 51-84, March 1998.

Press, Larry. 2011. “Cuba's first Internet connection.” *Personal Blog*. 27 February 2011. http://laredcubana.blogspot.com/2011/02/cubas-first-internet-connection.html; accessed 7 November 2015

Press, Larry. 2013. “The Internet in Cuba: Applications, implications and technology.” *Personal Blog*. 20 January 2013. http://laredcubana.blogspot.com/2013/01/first-traffic-on-alba-1-cable.html; accessed 6 November 2015

Pribadi, Sugeng. 2013. “Indonesia Most Slow [sic] Internet Speeds in Asia.” *Socyberty*. 7 February 2015. http://socyberty.com/economics/indonesia-most-slow-internet-speeds-in-asia/; accessed 1 November 2015

Project Loon, 2016. “As Project Loon looks to build a ring of connectivity around the world in 2016.” *Google Plus*. 25 February 2016 https://plus.google.com/+ProjectLoon/posts25; accessed 12 April 2016

Project Loon. 2016. “Loon for All.” *Project Loon*. https://www.google.com/loon/; accessed 12 April 2016

Purbo, Onno W. 2015. “Internet History of Indonesia.” *Institut Teknologi Bandung: Amateur Radio Club.* https://translate.google.com/translate?sl=id&tl=en&js=y&prev=_t&hl=en&ie=UTF-8&u=http%3A%2F%2Farc.itb.ac.id%2Ftentang-arc%2Fsejarah-internet-indonesia%2F&edit-text=&act=url; accessed 22 October 2015.

Raad, Morteza. 2015. “Iran Telecoms Q3 2015.” *Financial Tribune.* 3 October 2015. http://financialtribune.com/articles/sci-tech/27046/iran-telecoms-q3-2015; accessed 15 November 2015

Rahimi, Babak. 2003. “Cyber Dissent: The Internet in Revolutionary Iran.” *Middle East Review of International Affairs*. Vol. 7.3.

Rahimi, Babak. 2008. “The politics of the internet in Iran.” in *Media, Culture and Society in Iran: Living with Globalization and the Islamic State*. ed Mehdi Semati. NY: Routledge.

Rahimi, Babak. 2015. “Internet Censorship in Rouhani's Iran: The ‘Wooden Sword.’” *Asian Politics & Policy*. Vol. 7.2.

Rainie, Lee. 2015. “Digital Divides 2015.” *Pew Internet & Technology*. 22 September 2015. http://www.pewinternet.org/2015/09/22/digital-divides-2015/; accessed 1 February 2016

Ramos Shahani, Lila. 2015. “Why is Our Internet So Slow?” *PhilStar: Opinion*. 24 August 2015. http://www.philstar.com/opinion/2015/08/24/1491398/why-our-internet-so-slow; accessed 13 January 2016

Ramzy, Austin. 2011. “The Activist Artist of China.” *Time*. 25 April 2011.

Ranine, Lee and Mary Madden. 2015. “Americans’ Views on Government Surveillance Programs.” *Pew Research Center.* 16 March 2015. http://www.pewinternet.org/2015/03/16/americans-views-on-government-surveillance-programs/#americans-are-divided-in-their-concerns-about-government-surveillance-of-digital-communications; accessed 4 February 2016

Rapoza, Kenneth. 2013. “China Says Broadband Speeds of 20 Mbps by 2015.” *Forbes*. www.forbes.com/sites/kenrapoza/2013/08/18/china-says-broadband-speeds-of-20-Mbps-by-2015; accessed 14 October 2015

Rappler. 2014. “PLDT to finish P1-B fiber network project this year.” 12 August 2014. http://www.rappler.com/business/industries/215-tech-biz/66016-pldt-fiber-optic-network-project; accessed 17 January 2016

Rassool, Cyrus. 2014. “The United States Must Lead in Upholding Net Neutrality.” *Huffington Post: The Blog*. http://www.huffingtonpost.com/freedom-house/the-united-states-must-le_b_5681846.html; accessed 14 July 2015

Reidenberg, Joel R. 2005. “Technology and Internet Jurisdiction.” *University of Pennsylvania Law Review*. Vol. 153.

Reporters without Borders. 2011. “Internet Leaders Cooperate with Government Efforts to Reinforce Online Controls.” 9 November 2011. http://en.rsf.org/chine-respect-for-free-speech-continues-27-10-2011,41303.html; accessed 13 October 2015

Republic Act No. 7925. “An Act to Promote and Govern the Development of Philippine Telecommunications and the Delivery of Public Telecommunications Services.” 1995

Reuters. 1995. “International Briefs; Sprint's China Accord.” *New York Times*. 25 March 1995

Riasonovsky, Nicolas. 1993. *A History of Russia*. NY: Oxford

Riska, Merlinda. 2015. “Businessman carrying domestic domain.” Kontan.co.id. 23 April 2015. industri.kontan.co.id/news/pebisnis-dukung-domain-domestik; accessed 24 October 2015

Risse, Thomas and Kathyrn Sikkink. 1999. “The socialization of international human rights norms into domestic practices: introduction.” in *The Power of Human Rights: International Norms and Domestic Change.* Cambridge: Cambridge University Press.

Roetter, Martyn F. Global Broadband Benchmarking 2013: Best Practice Lessons for Governments. *Journal of Information Policy*. Vol. 3

Rosenau, James N. and J.P. Singh. 2002. *Information Technologies and Global Politics: The Changing Scope of Power and Governance*. New York: SUNY Press.

Rosenzweig, Roy. 1998. "Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet." *The American Historical Review*. Vol. 103.5

.

Rossotto, Carla Maria, Natalija Gelvanovska, Yuri Hohlov, Vaiva Mačiulė, and Sergei Shaposhnik. 2015. "A Sector Assessment: Broadband in Russia." January 2015. *World Bank*. http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2015/07/07/090224b082c25e88/1_0/Rendered/PDF/Russian0Federa00broadband0in0Russia.pdf; accessed 15 September 2015

Rostelecom. 2015. "Strategic Projects." *Rostelecom.* http://www.rostelecom.ru/en/projects/; accessed 3 September 2015

Ruggie, John, 1998. "What Makes the World Hang Together? Neo-Utilitarianism and the Social Constructivist Challenge." *International Organization*. Vol. 52.4.

Ruiz, Rebecca R. and Steve Loeb. 2015. "F.C.C. Approves Net Neutrality Rules, Classifying Broadband Internet Service as a Utility." *NY Times*. 26 February 2015.

Sánchez, Yonai. 2014. "And Google arrived in Havana!" *Personal Blog*. 28 June 2014. http://www.14ymedio.com/blogs/generacion_y/Google-llego-Habana_7_1586911294.html&usg=ALkJrhgRWhIXAjlBqMKlqfcacJjvofGl2Q; accessed 9 November 2015

Sandholtz, Wayne and Kendall Stiles. 2009. *International Norms and Cycles of Change*. New York: Oxford University Press.

Sarmiento, Tomas and Cyntia Barrera. "Mexico gives competitors access to Telmex phone networks." *WHTC News*. 30 June 2015. http://whtc.com/news/articles/2015/jun/30/mexico-gives-competitors-access-to-telmex-phone-networks/; accessed 1 January 2016

Satake, Minoru. 2015. "Pivot or Perish: Rivalry drives top Philippine telecom company's digital buildup." Nikkei Asian Review. 11 September 2015. http://asia.nikkei.com/Business/Companies/Rivalry-drives-top-Philippine-telecom-company-s-digital-buildup; accessed 15 January 2016

Savageau, John. "Indonesia's ICT Policy Provides a Success Story for Developing Countries." Personal Blog. 24 March 2010. http://john-savageau.com/2010/03/24/indonesia%E2%80%99s-ict-policy-provides-a-success-story-for-developing-countries/; accessed 26 October 2015

Schradie, Jen. 2014. "Bringing the Organization Back In: Social Media and Social Movements." *Berkley Journal of Sociology*. 3 November 2014. http://berkeleyjournal.org/2014/11/bringing-the-organization-back-in-social-media-and-social-movements/; accessed 10 April 2016

Scott, Ben and Frannie Wellings. 2005. "Telco Lies and the Truth about Municipal Broadband Networks." *FreePress.net.* http://www.freepress.net/sites/default/files/fp-legacy/mb_telco_lies.pdf; accessed 10 July 2015

Secretaría de Comunicaciones y Transportes. 2015. "Reforma en materia de Telecomunicaciones." 7 June 2015. http://www.gob.mx/sct/reformas/reforma-en-materia-de-telecomunicaciones-6314; accessed 7 January 2016

Sensorly. 2016. “Map of Telcel 4G coverage.” http://www.sensorly.com/map/4G/MX/Mexico/Telcel/lte_334020#|coverage; accessed 9 January 2016

Shanker, Amy and Len Rodman. 1996. “Public-private partnerships.” *Journal (American Water Works Association)*. Vol. 88.6.

Sidorenko, Alexey. 2010. “Russia: Mapping Broadband Internet Prices.” *Global Voices*. 14 March 2010. https://globalvoices.org/2010/03/14/russia-mapping-broadband-internet-prices/; accessed 10 September 2015

Small Media. 2014. “Iranian Internet Infrastructure and Policy Report.” March 2014. Smallmedia. http://smallmedia.org.uk/sites/default/files/u8/IIIP_March2014.pdf; accessed 10 November 2015

Smarr, Larry. 1983. “’The Black Proposal’: NSA Grant Application.” *NSCA Illinois.* http://www.ncsa.illinois.edu/20years/timeline/documents/blackproposal.pdf; accessed 27 June 2015.

Smith, Emerald. 2011. “Lord of the Files: International Secondary Liability for Internet Service Providers.” *Wash. & Lee Law Review*. Vol. 68.

Smith, Steve and Patricia Owens. 2008. “Alternative approaches to international theory,” in *The Globalization of World Politics: an Introduction to International Relations*. 4th Edition. Eds. Baylis, John, Steve Smith and Patricia Owens. New York: Oxford University Press.

Soldatov, Andrei and Irina Borogan. 2015. “Inside the Red Web: Russia's back door onto the internet – extract.” 8 September 2015. *The Guardian*. http://www.theguardian.com/world/2015/sep/08/red-web-book-russia-internet; accessed 10 September 2015

Soprana, Paula. 2016. “The CPI of Cybercrime "mutilate" the Civil Marco Internet?” *Epoca*. 1 April 2016. http://epoca.globo.com/vida/experiencias-digitais/noticia/2016/04/cpi-de-crimes-ciberneticos-quer-alterar-marco-civil-da-internet-no-brasil.html; accessed 14 April 2016

Sosa, Luis. 2014. “Fastest ISPs 2014: Mexico.” PCMag. 14 May 2014. http://www.pcmag.com/article2/0,2817,2457831,00.asp; accessed 2 January 2016

Sridharan, Vasudevan. 2015. “Iran launches own search engine Yooz to beat internet-related sanctions.” International Business Times. 16 February 2015. http://www.ibtimes.co.uk/iran-launches-own-search-engine-yooz-beat-internet-related-sanctions-1488112; accessed 22 November 2015

Stampler, Laura and Maya Rhodan. 2014. “USAID Denies ‘Cuban Twitter’ Was Meant To Subvert.” *Time*. 4 April 2014. http://time.com/53501/usaid-cuban-twitter-rajiv-shah/; accessed 9 November 2015

Stecklow, Steve. 2012. “Lawmakers ask State Department to Probe Huwei Business with Iran.” *Wall Street Journal*. 5 January 2012

Steelmay, Emily. 2015. “Broadband at the Center of Charter-Time Warner Cable Deal.” *NY Times*. 25 May 2015

Steiner, Nils D. 2012. “Testing for a Political Bias in Freedom House Democracy Scores: Are U.S. Friendly States Judged to be more Democratic?” *Journal of Comparative Policy Analysis*, Forthcoming.

Stengel, Rick. 2011. “Person of the Year: Introduction.” *Time*. 14 December 2011.

Subsea News. 2013. “ALBA-1 Cable Activated (Cuba).” Subsea News. 21 January 2013. http://subseaworldnews.com/2013/01/21/alba-1-cable-activated-cuba/; accessed 8 November 2015

Sujarwoto and Gindo Tampubolon. 2013. “Deepening Digital Divide and Widening Spatial Gaps in Indonesia 2005-2009.” *Social Science Research Network*.

Swaine, Jon. 2011. “Egypt Crisis: the young revolutionaries who sparked the protest.” *The Telegraph*. 11 February 2011. http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8317055/Egypt-crisis-the-young-revolutionaries-who-sparked-the-protests.html; accessed 11 June 2015

Sy, Marvin. “Senate OKs proposed Fair Competition Act.” *Philippine Star*. 16 December 2014.http://www.philstar.com/headlines/2014/12/16/1403199/senate-oks-proposed-fair-competition-act; accessed 18 January 2016

Tambasen, Eunice N. 2015. “The Countryside in Figures.” *Philippine Statistics Authority*. 26 November 2015. http://www.nscb.gov.ph/countryside/showperindicator.asp; accessed 15 January 2016

Taub, Geoffry. 1998. “A Not-So-Worldwide-Web: The Internet, China, and Challenges to Non-Democratic Rule.” *Political Communication*. Vol. 15.2.

Taylor, Adam. 2014. “This sad Facebook page may be all that remains of the ‘Cuban Twitter’ created by the U.S. to stir unrest.” The Washington Post. 3 April 2014. https://www.washingtonpost.com/news/worldviews/wp/2014/04/03/this-sad-facebook-page-may-be-all-that-remains-of-the-cuban-twitter-created-by-the-u-s-to-stir-unrest/; accessed 9 November 2015

Telecompaper. 2015. “Telmex ordered to offer rivals improved last mile terms.” 12 October 2015. http://www.telecompaper.com/news/telmex-ordered-to-offer-rivals-improved-last-mile-terms--1107197; accessed 7 January 2016

Telegeography. 2015. “Submarine Cable Map.” *Telegeography*. Dynamic. http://www.submarinecablemap.com/#/; accessed 1 November 2015.

Telekom. 2015. “Improve Infrastructure eastern Indonesia, Telkom wake Luwuk Tutuyan Cable System.” *Telekom*. 3 May 2015. http://www.telkom.co.id/tingkatkan-infrastruktur-kawasan-timur-indonesia-telkom-bangun-luwuk-tutuyan-cable-system.html; accessed 30 October 2015.

Testmy.net. 2016. “World Results Database.” *Testmy.net.* http://testmy.net/country; accessed 12 April 2016

Theberge, Leonard J. 1981. “U.N.E.S.C.O.’s ‘New World Information Order’: Colliding with First Amendment Values.” *American Bar Association Journal*. Vol. 67.

Thomasson, James, William Foster, and Laurence Press. 2003. “The Diffusion of the Internet in Mexico.” Latin American Information Network Center. http://www.lanic.utexas.edu/project/etext/mexico/thomasson/thomasson.pdf; accessed 15 December 2015

Tiezzi, Shannon. 2014. “China's 'Sovereign Internet:’ China is increasingly seeking not just domestic but international influence over cyberspace.” *The Diplomat*. 24 June 2014. http://thediplomat.com/2014/06/chinas-sovereign-internet/; accessed 30 October 2015

Tiglao, Rigoberto. 2014. “Supreme Court: PLDT mocks the Constitution.” *The Manila Times*. 25 March 2014. http://www.manilatimes.net/supreme-court-pldt-mocks-the-constitution/85412/; accessed 16 January 2016

Time Warner Cable. 2016. “Investor News: Press Release.” *Time Warner Cable*. 18 May 2016. http://ir.timewarnercable.com/investor-relations/investor-news/financial-release-details/2016/Charter-Communications-Time-Warner-Cable-and-Bright-House-Networks-Complete-Transactions/default.aspx; accessed 8 June 2016

Toh, Michelle. 2015. “How the Philippines plans to improve 'pathetic' Internet speed.” *Christian Science Monitor*. 30 June 2015. http://www.csmonitor.com/Technology/2015/0630/How-the-Philippines-plans-to-improve-pathetic-Internet-speed; accessed 15 January 2016

Tsai, Katherine. 2010. “How to Create International Law: The Case of Internet Freedom in China.” *Duke Journal of Comparative and International Law*. Vol. 21.

Tucekci, Zeynep. 2014. “Bay of Tweets.” *Politico*. 4 April 2014 http://www.politico.com/magazine/story/2014/04/cuba-twitter-bay-of-tweets-105382#ixzz3r2E3HQJ9; accessed 9 November 2015

Turner, Eric. 2013. “New Movements, Digital Revolution, and Social Movement Theory.” Peace Review: A Journal of Social Justice. Vol. 25.3.

Tuwo, Lukita Dinarsyah. 2013. “Presentation: Indonesia Broadband Plan.” Meaningful Broadband—Indonesia Congress. http://docslide.us/documents/broadband-plan-indonesia.html; accessed 2 November 2015

UN General Assembly. 2001. World Summit on the Information Society. A/56/183.

UN General Assembly. 2011. Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. A/66/359

UN General Assembly. 2013. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 30 July 2013. A/68/98

UN General Assembly. 2014.69/166l “The Right to Privacy in the Digital Age.” A/RES/69/166 (19 November 2014)

UN Human Rights Committee. 1994. Initial Reports of State Parties due in 1993: United States. CCPR/C/81/Add.4

UN Human Rights Committee. 2005. Third periodic reports of State parties due in 2003: United States. CCPR/C/USA/3

UN Human Rights Committee. 2011. Replies from the Government of the Islamic Republic of Iran to the list of issues (CCPR/C/IRN/Q/3) to be taken up in connection with the consideration of its third periodic report (CCPR/C/IRN/3). CCPR/C/IRN/Q/3/Add.1

UN Human Rights Committee. 2011. Third Periodic Report of States Parties: Iran. CCPR/C/IRN/3

UN Human Rights Committee 2011. List of issues to be taken up in connection with the consideration of the third periodic report of the Islamic Republic of Iran (CCPR/C/IRN/3) CCPR/C/IRN/Q/3

UN Human Rights Committee. 2012. Fourth periodic reports of State parties due in 2011: United States. CCPR/C/USA/4

UN Human Rights Committee. 2013. List of issues in relation to the fourth periodic report of the United States of America. CCPR/C/USA/Q/4

United Nations Human Rights Council. 2013. "Universal Periodic Review Second Cycle - China: National report submitted in accordance with paragraph 5 of the annex to Human Rights Council resolution 16/21." https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/169/58/PDF/G1316958.pdf?OpenElement

United Nations Human Rights Council. 2014. "Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development A/HRC/26/L.24." *UN General Assembly*.

United Nations General Assembly. 2014. Special Rapporteur Report on Situation of Human Rights in the Islamic Republic of Iran. A/69/356

Venzon, Cliff. 2015. "Conglomerate targets telecom duopoly." Nikkei Asian Review. 14 July 2015. http://asia.nikkei.com/Business/Deals/Conglomerate-targets-telecom-duopoly; accessed 15 January 2016

Verizon Communications Inc. v. Federal Communications Commission. 2014. 740 F.3d 623

Vicari, Stefania. 2014. "Networks of Contention: The Shape of Online Transnationalism in Early Twenty-First Century Social Movement Coalitions." *Social Movement Studies.* Vol. 13.1.

Villagran, Lauren. 2012. "Mexico's Digital Divide." *Mahindra Rise*. 4 January 2012. http://rise.mahindra.com/mexicos-digital-divide/; accessed 15 December 2015

Virtual Brazil. 2013. "History of Internet in Brazil." http://www.v-brazil.com/science/history-internet-brazil.html; accessed 25 November 2015

Von Drehle, David. 2013. "The Surveillance Society." *Time*. 1 August 2013

Von Twickel, Nikolaus. 2009. "Internet Provider Says It Blocks Sites." *The Moscow Times*. 8 December 2009. http://www.themoscowtimes.com/news/article/internet-provider-says-it-blocks-sites/391080.html; accessed 20 August 2015

Voss, Michael. 2008. "Cuba lifts ban on home computers." *BBC News.* http://news.bbc.co.uk/2/hi/americas/7381646.stm; accessed 6 November 2015

Vox Populi Pollling. 2015. "Results of Nationwide Open Internet Survey." *Internet Freedom Business Alliance.* 21 January 2015. http://www.netfreedom.us/wp-content/uploads/2015/01/Open-Internet-Polling-Memo-2-Jan-2015.pdf; accessed 5 February 2016

Wahid, Fathul, Neila Ramdhani and Wisnu Wirdhany. 2014. "More gaining less gaming? The internet use in Indonesia after one decade." in Recent *Trends in Social and Behavioral Sciences*. Eds. Ford Lumban Gaol, Seifedine Kadry, Marie Taylor, Pak Shen Li. CRC Press.

Waltz, Kenneth. 1979. *Theory of International Politics.* Reading, Mass: Addison-Wesley Pub. Co.

Watkins, Thayer and Silivia Gonzàlez. 2010. "The Economic History and Economy of Cuba." *San José State University.* http://www.sjsu.edu/faculty/watkins/cuba.htm; accessed 8 November 2015

Wei, Miao. 2015. "Miao Wei: big data, change in the world's key resources." *People's Daily*; Google Translate. 14 October 2015. http://www.miit.gov.cn/n11293472/n11293832/n11293907/n11368223/16863935.html&usg=ALkJrhgq4e45z1n5PJoiR1DLtRHWtY35jg; accessed 14 October 2015

Weiss, Mellissa L. 2014. "New media, new activism: trends and trajectories in Malaysia, Singapore and Indonesia." *International Development and Planning Review*. Vol. 36.1.

Wendt, Alexander. 1992. "Anarchy is What States Make of It." *International Organization.* Vol. 46.2.

Wheeler, Nicholas J. 2000. *Saving Strangers: Humanitarian Intervention in International Society*. New York: Oxford University Press.

Wheeler, Tom and Mignon Clyburn. 2016. "Broadband: A Lifeline for the 21st Century." *The Federal Communications Commission*. 8 March 2016. https://www.fcc.gov/news-events/blog/2016/03/08/broadband-lifeline-21st-century; accessed 8 March 2016

Whitney, Lance. 2015. "Why don't people use the Internet?" *CNet.com. 29* July 2015. http://www.cnet.com/news/why-dont-some-people-use-the-internet/#!; accessed 5 January 2016

Wigfield, Mark. 2015. "FCC Finds U.S. Broadband Deployment Not Keeping Pace." *Federal Communications Commission*. https://apps.fcc.gov/edocs_public/attachmatch/DOC-331760A1.pdf; accessed 1 July 2015

Wood, Charles H. and Rachel Reis Mourão. 2015. "The Digital Inequality in Brazil, 2004-2009: Evolution and Effects on Political Engagement." Journal of Latin American Communication Research. Vol. 5.1

Woodward, Colin. 2003. "Estonia, where being wired is a human right." *The Christian Science Monitor*. http://www.csmonitor.com/2003/0701/p07s01-woeu.html; accessed 1 July 2015

World Bank Group. 2016. "World Development Report 2016: Digital Dividends." International Bank for Reconstruction and Development / The World Bank. http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2016/01/13/090224b08405ea05/2_0/Rendered/PDF/World0developm0000digital0dividends.pdf; accessed 14 January 2016

World Economic Forum. 2011. "The New Internet World: A Global Perspective on Freedom of Expression, Privacy, Trust and Security Online." *World Economic Forum*. http://www3.weforum.org/docs/WEF_GITR_TheNewInternetWorld_Report_2011.pdf; accessed 7 June 2015

World Wide Web Foundation. 2016. "7 Predictions for Broadband Access in 2016." World Wide Web Foundation. 14 January 2016. http://webfoundation.org/2016/01/7-predictions-for-broadband-access-in-2016/; accessed 4 March 2016

WSIS. 2003. "Final Report of the Geneva Phase of the Summit, revision 1" *ITU.int*. http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0009!R1!PDF-E.pdf; accessed 5 June 2015

WSIS. 2005. "Tunis Agenda for the Information Society." *ITU.int* http://www.itu.int/wsis/docs2/tunis/off/6rev1.doc; accessed 5 June 2015

WSIS. 2014. "WSIS+10 Outcome Documents Geneva 2014." *ITU.int*; http://www.itu.int/wsis/implementation/2014/forum/inc/doc/outcome/362828V2E.pdf; 13 November 2014

Wu, Tim. n.d. “Network Neutrality FAQ.” http://www.timwu.org/network_neutrality.html; accessed 28 June 2016

Xiang, Tracey. 2013. “What Do The First Chinese Mobile Virtual Network Operators Plan to Offer?” *TechNode.* 31 December 2013. http://technode.com/2013/12/31/plans-of-the-first-chinese-mobile-virtual-network-operators/; accessed 18 October 2015

Xinhuanet. 2012. “China's legislature adopts online info rules to protect privacy.” *Xinhuanet English News*. 28 December 2012. http://big5.xinhuanet.com/gate/big5/news.xinhuanet.com/english/china/2012-12/28/c_132069320.htm; accessed 2 October 2015

Yardley, Matt. 2012. “Developing successful Public-Private Partnerships to foster investment in broadband networks.” *ITU.int*. http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/documents/GSR12_BBReport_Yardley_PPP_7.pdf; accessed 7 June 2015

Yin, Robert K. 1984. *Case Study Research: Design and Methods*. Newbury Park: Sage Publications.

Yu, Xioahui. 2013. “Introduction to ‘Broadband China’ Strategy.” China Academy of Telecommunication Research of MIIT. 5 September 2013. http://file.eu-chinapdsf.org/Internet/PUB/Activity4/Results%203/Broadband%20China%20introduction_Yu%20Xiaohui.pdf; accessed 17 October 2015

Zakaria, Fareed. 2012. *The Post-American World: Release 2.0*. New York: W.W. Norton.

Zakharov, Roman. 2016. “Glasnost defence foundation digest No. 739.” *Glasnost Defense Foundation*. 22 January 2016. http://www.gdf.ru/digest/item/1/1347; accessed 29 January 2016

Zuckerberg, Mark. 2013. “Is Connectivity a Human Right?” 21 August 2013. https://scontent-lga3-1.xx.fbcdn.net/hphotos-xpa1/t39.2365-6/12057105_1001874746531417_622371037_n.pdf; accessed 21 February 2016

Zuckerberg, Mark. 2015. Facebook post. 26 March 2015.