Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

Editorial Introduction

To cite this article: (2020) Editorial Introduction, Journal of Cyber Policy, 5:1, 1-4, DOI: 10.1080/23738871.2020.1748080

To link to this article: https://doi.org/10.1080/23738871.2020.1748080

Published online: 05 May 2020.

JOURNAL OF CYBER POLICY
2020, VOL. 5, NO. 1, 1–4
https://doi.org/10.1080/23738871.2020.1748080

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

Editorial Introduction

> 'Since destruction of a small number of nodes in a de-centralized network can destroy communications, the properties, problems and hopes of building "distributed" communications networks are of paramount interest' Paul Baran, §: *I*, 1964, RAND

Paul Baran was a man with a vision. A researcher at RAND during the height of the Cold War, he described in a seminal series of papers a way of creating a communications network that was capable of surviving enemy attacks. Although Baran never obtained the funding to turn his theories into practice, his papers *On Distributed Communications* set out key concepts that were later reflected in the internet's foundational protocols invented by Vint Cerf and Bob Kahn. Those protocols enabled the rapid growth of a distributed network of private networks, over which no one exercised control, and delivered a reliable system built of heterogeneous and unreliable parts. Cerf and Kahn went on to found the Internet Society.

Despite the introduction of massive technological and commercial changes in the past 20 years, and despite the emergence of a handful of tech giants, the internet's architecture continued to retain its unique qualities. However, in recent years, it has become apparent that the internet's architecture is also experiencing consolidation. No matter where you look, whatever layer you examine, the same names keep popping up: Google, Amazon, Facebook, Apple, Microsoft. We are familiar with their applications, but increasingly the same companies are operating deep down in the infrastructure – resolving domain name queries, providing application programming interfaces, cloud hosting or computation.

Volume 5, No 1 of the *Journal of Cyber Policy* is a special issue on the Consolidation of the Internet. It is a collaboration between Chatham House and the Internet Society, whose 2019 paper 'Consolidation in the Internet Economy' called for deeper research to help understand the phenomenon. What comes across in the articles is that we are close to the point where the internet starts to lose its defining characteristics. Paul Baran's early experiments showed that decentralized networks retain their resiliency even when multiple nodes are disabled. Once they pass a certain point, however, the network can fail dramatically. If we want to avoid this happening to the internet, we need to take more interest and collective responsibility for ensuring that we push back against harmful consolidation trends. There is an urgent need for transparent governance and effective checks and balances, particularly of those firms which enjoy significant power over the network.

This open access special issue begins with a guest editorial by Andrew Sullivan, the Internet Society's President and Chief Executive Officer. The first article by security researchers Dan Geer and Éireann Leverett with Eric Jardine of Virginia Tech considers the consequences of market concentration on cybersecurity risk. Jari Arkko, former Chair of the Internet Engineering Task Force, offers a practitioner's point of view on the risks that the increasing centralization of the network presents. Roxana Radu of Oxford

University and Michael Hausding of the .ch domain registry SWITCH present a deep dive into the Domain Name System (DNS), finding that public DNS resolution is a highly concentrated market. Moreover, that consolidation is highly relevant to current controversies about encryption of DNS lookups through new protocols such as DNS over HTTPs.

Jennifer Cobbe, Chris Norval and Jatinder Singh of Cambridge University explore consolidation through the lens of run-time [Anything]-as-a-Service applications, and analyse the shortcomings of regulations (such as the General Data Protection Regulation) as tools to increase the transparency of online supply chains. Chris Riley, Mozilla's Director of Public Policy, argues that regulators are increasingly turning to the concept of interoperability as a way of combating distortions of competition arising from consolidation. Consolidation need not necessarily be a bad thing – Jesse Sowell of the Bush School in Texas shows how internet exchange points reduce costs and stimulate competition in local markets, while relying on the participation of big tech companies. Finally, Eva Claessen of the Leuven Global Governance Studies examines how regulatory interventions can also contribute to consolidation. The growing trend of securitization in both Russia and the EU and increased assertion of state sovereignty can result in regulation of the network in ways that undermine its fundamental characteristics.

On market concentration and cybersecurity risk

As the world becomes more reliant on a small number of digital service and infrastructure providers, the network as a whole is exposed to a growing level of risk. Dan Geer, Eric Jardine and Eireann Leverett argue that countering trends in market concentration will be essential for managing cyber risk on the internet. As market concentration can influence all three components of the cyber risk equation – threat, vulnerability and impact – ignoring trends in market concentration and not taking steps to build norms, diversify the ecosystem or create incentives to reduce concentration can exacerbate system-wide vulnerability, increasing the odds of a system-wide failure.

The influence of internet architecture on centralized versus distributed internet services

Architectural choices can affect the ability to deploy internet services within a distributed and competitive internet environment. In this practitioner paper, Jari Arkko, former Chair of the Internet Engineering Task Force, explores the impact of internet architecture on the competitive landscape with a particular focus on the evolution of internet technology. From a security perspective, Arkko suggests the need for greater awareness of the risks that a centralized system might pose, and advises the deployment of end-to-end protection for information passed via other parties, to minimize the passing of a control function to other parties, and careful consideration of the introduction of centralized resources.

Consolidation in the DNS resolver market – how much, how fast, how dangerous?

More than 35 years ago, the domain name system (DNS) was introduced in a highly decentralized manner, leaving Internet Service Providers (ISPs) to set up their own

DNS resolvers and to provide DNS resolution to their customers. However, this started to change from the early 2000s with the introduction of public resolver services. In a quantitative analysis of public resolvers vs resolvers run by ISPs, Roxana Radu and Michael Hausding find that more than 50 per cent of DNS queries are resolved by a small number of public resolver services. The authors argue this phenomenon risks greater centralization, higher costs and the deployment of new technical standards by leading public resolvers.

What lies beneath: transparency in online service supply chains

Large platform monopolies – such as Facebook, Google, Amazon and Netflix – have dominated public discussions on the impact that centralized networks can have on market competition. Beneath the highly visible application layer are questions around the growing concentration of online service supply chains such as cloud hosting and computation services, content distribution networks, software processing, advertising brokers, and analytics and data companies. Jennifer Cobbe, Chris Norval and Jatinder Singh argue that greater attention must be paid to these hidden supply chains, including greater transparency to uncover the nature and ownership of supply chain services. In an increasingly data-driven world, these questions have critical implications for market competition and power in the digital era.

Unpacking interoperability in competition

Chris Riley of Mozilla discusses the impact of consolidation on the ability of internet-connected technologies to remain interoperable. Currently, competition policymakers are aiming to regulate and promote interoperability. From a practitioner's perspective, Riley evaluates how interoperability, in the context of digital platforms, could fit within the landscape of competition law. This article shows how competition agencies need enhanced resources and new paradigms of enforcement to address internet-related competition challenges. Riley argues that interoperability and competition should be promoted in parallel within the internet economy.

Evaluating competition in the internet's infrastructure: a view of GAFAM from the internet exchanges

The dominance of a handful of large tech platforms (Google, Amazon, Facebook, Apple and Microsoft – or GAFAM) has received significant scholarly attention. Consolidation in most market environments tends to breed anticompetitive practices that stifle innovation from small- or medium-sized competitors. Despite these common frames, Jesse Sowell argues that a more nuanced understanding of the impact of large platforms on competition is needed. Sowell shows how, despite (or even because of) the involvement of the large platforms, Internet Exchanges can facilitate open markets for small- or medium-sized innovators by providing diverse content delivery, lowering barriers to development and enabling global deployment.

Reshaping the internet – the impact of the securitization of internet infrastructure on approaches to internet governance: the case of Russia and the EU

While the other articles in this special issue focus on consolidation issues at the technical layers of the internet, Eva Claessen shows how regulatory interventions can also have a consolidating impact on the internet's infrastructure. In response to a growing number of cyberattacks against government services and critical infrastructure, states are increasingly motivated to exert greater sovereignty over the internet. By comparing Russian and EU approaches to internet governance, Eva Claessen argues that cybersecurity has been used as a rhetorical tool to justify a greater role of the state in internet governance. While the Russian and EU approaches have fundamental differences, both cases show how countries' policy narratives are advocating for greater autonomy and control over cyberspace.

Acknowledgements

Thank you to our partners at the Internet Society who have worked with us over the past year to put together this special issue on the consolidation of the internet, especially Konstantinos Komaitis, Carl Gahnberg and Andrew Sullivan.