International Review of Law, Computers & Technology

ISSN: 1360-0869 (Print) 1364-6885 (Online) Journal homepage: https://www.tandfonline.com/loi/cirl20

Regulating security on the Internet: control versus trust

Bibi van den Berg & Esther Keymolen

To cite this article: Bibi van den Berg & Esther Keymolen (2017) Regulating security on the Internet: control versus trust, International Review of Law, Computers & Technology, 31:2, 188-205, DOI: 10.1080/13600869.2017.1298504

To link to this article: https://doi.org/10.1080/13600869.2017.1298504

© 2017 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

Published online: 19 Mar 2017.

Submit your article to this journal

Article views: 4928

View related articles

View Crossmark data

Citing articles: 8 View citing articles

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=cirl20

INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY, 2017
VOL. 31, NO. 2, 188–205
http://dx.doi.org/10.1080/13600869.2017.1298504

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

Regulating security on the Internet: control versus trust

Bibi van den Berg[a] and Esther Keymolen[b]

[a]Institute for Security & Global Affairs (ISGA), Faculty of Governance & Global Affairs, Leiden University, The Hague, The Netherlands; [b]eLaw (Center for Law & Digital Technologies), Faculty of Law, Leiden University, Leiden, The Netherlands

ABSTRACT
This article focuses on the role of government in relation to cybersecurity. Traditionally, cybersecurity was primarily seen as a technical issue. In recent years, governments have realised that they, too, have a stake in securing the Internet. In their attempts to grapple with cybersecurity, governments often turn to technical solutions to 'code away' illegal or undesired behaviours. 'Techno-regulation' has become popular because it may seem to be an effective and cheap way of increasing control over end users' behaviours and increasing cybersecurity. In this article, we will explain why using techno-regulation has significant downsides and, therefore, why it may be unwise to use it as a dominant regulatory strategy for securing the Internet. We argue that other regulatory strategies ought to be considered as well, most importantly: trust. The second part of this article explains that trust can be used as an implicit strategy to increase cybersecurity or as an explicit mechanism for the same goal.

KEYWORDS
Cybersecurity; techno-regulation; trust

1. Introduction

Over the past decades, the Internet has become an indispensable element of our social, professional, and economic lives. Some would even argue that it should be labelled a critical infrastructure (cf. Latham 2003). The Internet has brought a significant segment of the world's population more and better possibilities to connect. It has led to an increase in efficiency in accessing and sharing information. And it has been a boost for global trade, facilitating a new online economy and digitising traditional economies. At the same time, it has become increasingly clear that the Internet can also be used to create harms of many kinds, ranging from cybercrimes (hacking, identity theft, and other forms of fraud) to cyber-espionage, cyber-terrorism, and cyber-warfare. Due to the centrality of the Internet in the global economy and in our personal and professional lives, moreover, the impact of cybersecurity risks can potentially be very severe. This is why, over the past decade, cybersecurity – keeping the Internet and the networked digital technologies connected to that network safe and secure – has become an increasingly important topic. But how do we realise cybersecurity?

CONTACT Bibi van den Berg b.van.den.berg@fgga.leidenuniv.nl

© 2017 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (http://creativecommons.org/licenses/by-nc-nd/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

One of the answers that is often given by governments and regulators is that we can make the Internet safer and more secure by gaining more *control* over it. If we can keep a tighter rein on the behaviours of actors online – be they individuals, communities, organisations, businesses, or public parties – then this will increase security in cyberspace. More security is essential, governments argue. Not only does it ensure effective and uninterrupted network operations, but it also strengthens users' trust in the system. This bolsters the innovative potential that the Internet offers and will make it flourish even more in years to come.

In this article, we will look at one of the key strategies that governments and regulators have embraced in the past decade or so in the name of increasing security in cyberspace. This strategy is called 'techno-regulation': 'influencing […] individuals' behaviours by building legal norms into technological devices' (Van den Berg and Leenes 2013, 68). Techno-regulation means that we build barriers into technological artefacts or systems, so that individuals using them cannot commit undesired or illegal actions anymore. The key element of techno-regulation is that, by implementing norms and (legal) rules into technological artefacts, these artefacts become the enforcer of the rule or the norm.

It is easy to see why techno-regulation might be a popular regulatory strategy for governments.[1] If the technological systems offered only allow end users a clearly circumscribed set of actions, and if deviating from that set of actions is made impossible because systems simply do not offer the possibility to do so, then the level of control increases. When techno-regulation is deployed to increase security the outcome is easy to predict: such systems will, in fact, be more secure. There are numerous examples of cases where techno-regulation is used, both in the offline and in the online world, for a wide variety of purposes. Increasing security is one of them, and it turns out that this strategy is, in fact, very effective in raising security levels. However, at the same time using techno-regulation also has significant shortcomings. Over the years, these have been discussed in various scientific publications (Yeung 2008; Brownsword and Yeung 2008b; Hildebrandt 2009; Leenes 2011), and we will touch upon them in this article in Section 3.2 as well (see below).

The main contribution of this article lies in asking the question that *precedes* the deployment of techno-regulation. It takes a critical stance towards the silent assumption that more cybersecurity must mean *more control*? Can we not use regulatory strategies to increase cybersecurity that do *not* require, or lead to, more control? In our view, the answer is a wholehearted 'yes, we can'. Yes, we can make cyberspace more secure, and yes, we can do this, for instance, by using another interpersonal strategy that we commonly use in our everyday, offline lives: trust. In this article, we will show that rather than viewing control as the only, or even the most important path to cybersecurity, we should expand our view on the means and ends of securing cyberspace and allow for other key mechanisms as well.

We will start the article with a brief discussion on cybersecurity: what it is, why it matters and why governments feel they have a responsibility in (contributing to) cybersecurity. This is followed by a discussion of techno-regulation, explaining its strengths and weaknesses. It is these weaknesses, and the drive for control that leads to increased adoption of techno-regulatory interventions, that are at the heart of this article. We will argue that rather than focusing on increased control for cybersecurity, we can also use other mechanisms to increase security, most importantly trust. The second part of this article discusses

what trust is and how we can put it to good use for cybersecurity. We will explain that trust as a regulatory strategy for a more secure Internet can take different forms: we can use trust as an implicit strategy, or as an explicit mechanism for improved cybersecurity. We conclude that reliance on techno-regulation as a dominant strategy for improving cybersecurity has serious shortcomings, and that it is vital that we broaden our views on how to make the Internet more safe and secure. Using trust as a regulatory strategy could be a good candidate.

2. Cybersecurity: a very short introduction

For decades, concerns over the security of networked technologies were originally largely left to the technical community. Under the banner of 'information security', research and development in this area focused predominantly on three domains: protecting the *confidentiality* of data, keeping the *integrity* of data safe and secure, and ensuring the *availability* of systems, networks, and data (cf. Schneier 2004; Nissenbaum 2005; Hansen and Nissenbaum 2009; Singer and Friedman 2013; Appazov 2014). Over the years, much progress has been made on these three topics in the technical sciences.

In recent years, however, researchers and stakeholders outside the technical domain have started pointing out that to create adequate protection levels for security on/off the Internet a purely technical focus is too limited. 'Cybersecurity' became a novel term for a much broader understanding of security in relation to the Internet, emphasising not only the role of technologies and systems themselves, but also those of human beings that use these systems. Understanding cybersecurity risks, and findings ways to reduce these to acceptable levels (whatever we define these to be), can, only be done effectively when both the human and the technological component are taken into consideration (cf. Van den Berg et al. 2014). Cybersecurity issues not only require technical remedies and solutions, but also demand responses and interventions by governments, by regulators and policy-makers, by businesses and organisations, and even by end users themselves. Consequently, many Western countries now consider cybersecurity an element of their national security strategy (cf. Nissenbaum 2005). These countries have started developing regulatory mechanisms to improve cybersecurity. But many of them wonder whether they can, and should, do more. One of the strategies they increasingly turn to is implementing rules and norms into technical systems, also known as 'techno-regulation' or 'code as law' (Lessig 2006).

3. Techno-regulation or 'code as law'

The foundations for the notion of techno-regulation were developed by Lawrence Lessig in his landmark book *Code 2.0* (Lessig 2006; also see Lessig 1999). In this book, Lessig pointed out that legal scholars tend to be predisposed to use legal rules as a remedy to any societal problem they encounter. But there are, in fact, a number of other regulatory forces that may shape individuals' actions as well. For example, individuals' actions may be influenced by market forces, such as price mechanisms or taxation. Or they may be steered in their choices and behaviours by social norms. And finally – and most importantly for this article – Lessig pointed out that individuals behaviours are shaped by architectures (Lessig 2006, 123). This is so in both a literal and a more figurative meaning of the word

'architecture'. Architecture as in buildings, the physical organisation of our public and private spaces, affects what people can and cannot do. We are contained in, and constrained by, the shape and size of the spaces we work and live in, or travel through. But architecture also has a more figurative meaning. Software and hardware also qualify as forms of architecture: they shape what we can and cannot do when using digital technologies. They are regulatory forces, steering, guiding and influencing behaviours, and actions of end users. Lessig (2006) used the terms 'code as law' and 'regulation by design' to illustrate the idea that architectures can be used to regulate behaviours of individuals. Over the years this idea has come to be called 'techno-regulation' (Wu 2003; Kesan and Shah 2006; Brownsword and Yeung 2008a; Kerr 2010; Hildebrandt 2011; Leenes 2011; Yeung 2011; Van den Berg and Leenes 2013; Van den Berg 2014).

3.1. Limiting and enabling actions through design

Techno-regulation refers to the implementation of (legal) rules or norms into artefacts or systems, with the goal of shaping, steering, or influencing end user's actions. Note that techno-regulation has both a *limiting* and an *enabling* function. On the one hand, the design of software and hardware provides a limited action space for users: they can only use an artefact or system in the way it was intended by the designers. Other functionalities or options are simply not open to them (except maybe to a very small minority of very tech-savvy end users or hackers). In this way, techno-regulation enables designers (or regulators) to keep end users away from undesired or illegal actions. Such actions are literally coded away. But techno-regulation does not only offer limitations. Techno-regulation also means that we build specific incentives into artefacts or systems to encourage users towards desired or desirable actions.

One key characteristic of techno-regulation is that end users are often entirely unaware of the fact that their actions are being regulated in the first place. Techno-regulation invokes such implicit, almost automatic responses, that end users do not realise that their action space is limited by the artefacts' offerings. Thus, when (legal) rules or norms are implemented into artefacts or systems, it becomes difficult, if not outright impossible, to disobey these rules or norms. These artefacts and systems become implicit managers and enforcers of rules: they automatically, and oftentimes even unconsciously, steer or guide users' actions in specific directions – towards preferred (set of) actions and away from undesirable or inappropriate ones.

3.2. Benefits and drawbacks of using techno-regulation

For regulators, this last point is considered one of the key benefits of using techno-regulation. Using techno-regulation is efficient, easy, and very effective. It leads to very high levels of compliance. Because disobeying the rule that is implemented into an artefact or system is (nearly) impossible, techno-regulatory interventions are among some of the most effective forms of regulation. Moreover, techno-regulation is one of the most cost-effective ways of regulating. The enforcement of the rule for example is delegated to the artefact or system, which means there is no need for expensive law enforcement personnel. And since end users are much less likely to break the rule, costs for enforcement are expected to be reduced.

These two benefits play a key role in the increasing popularity of using this regulatory strategy. This combination is a regulator's dream: a regulatory strategy that will lead to substantial, if not complete, compliance at a fraction of the cost of many other types of regulatory interventions, including but not limited to laws that need enforcement or norms that do not have the same level of effectiveness. What's more, when regulators push for the use of techno-regulation on the Internet, for example, to increase security, in the process this automatically leads to significantly more control: more end users will 'colour within the lines' thus leading to a higher sense of command over the safe and secure use of cyberspace.

Having said that, over the years, several lines of critique have been launched against the use of techno-regulation. For one, this form of regulation is incredibly opaque (cf. Leenes 2011; Yeung 2011). When rules and norms get implemented into a technological artefact often end users who are confronted with such a device are not aware of the fact that they are being regulated. Sometimes instances of techno-regulation can be labelled as illegitimate, precisely because end users do not know if, and when, they are being regulated (cf. Yeung 2011). Under the rule of law, transparency and accountability are key values to uphold for governments when they seek to regulate the behaviours of citizens. Citizens need to know under which rule (laws, standards, institutional frameworks) they live and need to be able to hold government accountable for the proper implementation of laws and law enforcement that government executes on their behalf. When techno-regulatory interventions take place outside the awareness of citizens, the requirement of transparency is not met. Moreover, techno-regulation runs the risk of being undemocratic (cf. Benoliel 2004). If end users do not know that their actions are regulated by specific architectures, they have no possibility to question, appeal or object to this.

Despite these reservations, techno-regulation is an increasingly popular regulatory strategy for both public and private parties on the Internet. Why is this the case? We explain the rising popularity of techno-regulation by pointing to an underlying assumption. When techno-regulation is deployed on the Internet, especially to increase cybersecurity, regulators assume that when end users have less room for manoeuvring, there will be less risks to security. If end users 'cannot be bad' anymore, cybersecurity increases. Deploying techno-regulatory interventions entails that the regulator increases the level of control, because the action space of regulatees is more clearly defined and has sharp boundaries. Hence, when using techno-regulation regulators may, to borrow an idiom, strike two birds with one stone: it makes the Internet more secure, and it increases the level of control. Especially for an environment that is so valuable yet also appears to be so 'untameable' as cyberspace, reaching these dual goals through a single type of intervention may be very alluring for governments.

The question we need to ask ourselves, though, is: Is there really a relationship between control over the Internet and cybersecurity, and what role does techno-regulation play in this? Does an increase in control over the Internet, brought about by using techno-regulation, make the Internet a safer place?

4. More control equals more (cyber)security?

Answering that question is difficult for several reasons. First, there is the issue of how we would qualify 'making the Internet a safer place'. For whom would the Internet become

safer? And at what price? As we have seen there are significant drawbacks to using techno-regulation. End users carry the burden of the costs, while regulators (both from private and public parties) stand to gain: more efficiency and effectiveness, more compliance, a cheap implementation, and so on.

Second, it is debatable whether techno-regulatory interventions target the right audience if they are designed to increase cybersecurity. As we have seen, it is likely that techno-regulatory interventions lead to high levels of compliance, since end users will almost always automatically follow the implemented rule or norm. Hence, fewer end users will engage in 'risky behaviours', whatever these may be in a given context. While it is true that techno-regulation may prevent end users from making mistakes that can have a negative effect on their own cybersecurity or that of others, using this strategy will not weed out the biggest threat to security: that of intentional attackers. Hackers, cybercriminals, and those who engage in acts of cyber-espionage or cyber-terrorism go to great lengths to find weaknesses in systems and services and to exploit these to their benefit. Currently, the risks posed by these intentional attackers are considered to be far greater (both in terms of probability of occurrence and in terms of impact) than those created by genuine errors that random end users will make. Techno-regulatory interventions, or more generally the idea that a system's design will delineate the action space of end users, have no effect on those who intentionally seek to exploit vulnerabilities in it. This argument casts severe doubts on the assumption that more control (through techno-regulation) will also lead to more cybersecurity.

While techno-regulation as a strategy has clear and admitted benefits, we argue that the increasing tendency to seek to 'solve' cyber risks through techno-regulation is in need of reconsideration. Should we not also look at other strategies as well? In the rest of this article, we will contrast techno-regulation with another regulatory strategy, which up until this point in time has received little attention in the field of cybersecurity: using trust.

5. An alternative on the horizon: trust

Without some basic sense of trust, we would not be able to get up in the morning. Overwhelmed by just thinking about all the possible turns fate might take, we would not dare to leave the warm safety of our beds. Trust is a strategy to deal with the complexities inherent in life. The fact that, to a certain extent, we are aware of the unpredictable character of the future and that we cannot foresee all the actions of others make that we need trust to set aside some of these uncertainties. To trust is to act as if we know for certain what tomorrow will bring, while in fact we are groping in the dark.

Although most people intuitively have some ideas on what trust is, this concept cannot be pinned down easily. In their review article, Seppanen, Blomqvist, and Sundqvist (2007) counted more than 70 different definitions of trust and this was only in the domain of inter-organizational trust. As Simon (2013, 1) rightly concludes: 'As pervasive trust appears as a phenomenon, as elusive it seems as a concept'.

5.1. What is trust?

While it is not feasible to provide an all-encompassing definition of trust, there are some characteristics that reoccur in inter-disciplinary scholarly discussions on trust. A proposed

starting point is that trust is closely connected to having *positive expectations about the actions of others*. When we trust someone, we assume that the other will not act opportunistically but take into account our interests (e.g. see the encapsulated-trust account of Hardin 2006). This also entails that when we speak of trust there must be at least two actors, often referred to as a *trustor* (who vests trust) and a *trustee* (who receives trust). The trustor and trustee do not interact in a vacuum. Trust is *contextual* in the sense that certain – often implicit – societal roles, institutions, norms, and values guide the expectations of actors involved. The notion of expectations assumes that the trustor is not completely sure of the actions of the trustee. The trustor does not possess all the information or does not have full control to determine the outcome of a certain event. Moreover, the trustor depends on the trustee and the trustee has the possibility to act in a way that was not expected by the trustor. To speak of trust, the trustee, therefore, has to have some kind of agency. In addition, for the trustor there has to be something at stake. Trust consists of at least three components: The trustor (A) trusts the trustee (B) to do something (X) (Hardin 2001, 2006). If the actions of the trustee do not make a difference to the position of the trustor, that is, if the trustor is not affected by the performance of the trustee, we cannot meaningfully speak of trust. Trust is inextricably connected to vulnerability (also see Baier 1986). The trustee may betray the trustor, who as a consequence runs the risk of getting hurt – physically, mentally, or otherwise. Vesting trust in another person is a risky business (Luhmann 1979).

Traditionally, trust is located in interpersonal relations and interactions (Good 1988; McLeod 2014). However, increasingly, due to – amongst others – a wide range of societal and technological developments, trust is not only being placed in persons but in systems as well, which is referred to as *system trust* or *confidence* (Luhmann 1979, 1988; Giddens 1990, 1991; Giddens and Pierson 1998). Recently, there also has been an increased interest in trust in and on the Internet – referred to as e-trust (cf. Lahno and Matzat 2004; Taddeo 2010; Taddeo and Floridi 2011; Keymolen 2016) and trust in Artificial Intelligence and robots (cf. Taddeo 2011; Coeckelbergh 2012). This trust in and through (technological) systems, such as the Internet, leads to inquiries in the specific shape trust takes because of the mediating workings of the technologies at hand. Focusing on the Internet, some scholars argue that interpersonal trust is nearly impossible online (cf. Pettit 2004). However, generally, it is concluded that trust is 'translated' in an online context by developing trust tools such as reputation schemes and other actor-identifying measures (de Laat 2005; Simpson 2011).

5.2. The function of trust

In order to be able to investigate if and how trust might be of value for regulating the cyber domain, we have to focus on the functionality of trust. Which problems trust solves that could be fruitful for cybersecurity measures as well?

Luhmann (1979, 1988) defines the function of trust as a strategy to reduce complexity. This complexity resides in the fact that, as human beings, we have to deal with uncertainty and the unpredictable actions of all other human beings with whom we share our world. As we often do not have full information at hand and cannot be sure about what tomorrow brings, trust is a 'blending of knowledge and ignorance' (Luhmann 1979, 25); it is acting *as if* the future is certain. Although we do not know for certain, we assume that an anticipated future will become reality based on the assumption that other actors will

act in a stable and predictable way. Trust, therefore, is not about diminishing uncertainty, but about accepting it. When trust is set in motion, vulnerabilities and uncertainties are not removed; they are suspended (Möllering 2006, 6). We could say that trust is a very productive fiction because 'certain dangers which cannot be removed but which should not disrupt action are neutralized' by it (Luhmann 1979, 25).

As a complexity-reducing strategy, trust is a very useful way to cope with the uncertainties of everyday life. For example, in economics, trust is generally recognised as an important mechanism to reduce transactional costs. Since people have to operate in situations characterised by uncertainty that may negatively impact their willingness to interact, investments have to be made in all sorts of safeguards and controls to reduce this uncertainty and to facilitate interaction. However, when there is (mutual) trust, this uncertainty is neutralised and risk management measures and costs of address damaging, opportunistic or hostile behaviour can be avoided (cf. Möllering 2006, 26–29).

Trust has also been seen as an important prerequisite for innovation practices (cf. Nooteboom 2013). Because innovation is inherently uncertain, it is more difficult to rely on complexity-reducing mechanisms such as contracts, which are focused on determining the process. Trust, however, is about holding positive expectations about the outcome without too much control over the course of action. Trust, therefore, is specifically needed in innovation processes where the process benefits from openness and the results are uncertain. Moreover, when it comes to adopting new goods or services trust is acknowledged as an important feature (McKnight and Chervany 2002; McKnight, Choudhury, and Kacmar 2002; Warkentin et al. 2002; Keymolen, Prins, and Raab 2012). Without some trust in the functioning of a good or a service, it becomes less likely that customers will move to purchase.

In summary, trust is valued as a fruitful strategy to cope with uncertainty because, amongst others, trusting actors can keep transactional costs low, foster innovation, and feel confident enough to adopt new services and goods.

5.3. The limits of trust

For trust to be a very fruitful and robust strategy in dealing with the uncertainties of everyday life, its limitations should not be underestimated. First, trust is never the sole strategy at work to reduce complexity. Rather, we should think of an amalgam of interdependent strategies that are used to reduce complexity. Tamanaha (2007), for example, explains how the rule of law enhances certainty, predictability, and security between citizens and government (vertical) and among citizens themselves (horizontal). The existence of rules and the fact that citizens know there is a safety net in the form of a legal system fosters trust. Möllering (2006, 111) explains how trust 'is an ongoing process of building on reason, routine, and reflexivity'. Estimating chances, relying on roles and norms in society, and step-by step building confidence in interactions provide meaningful grounds for the suspension of uncertainties characteristic for trust. Luhmann (1979) states that trust can only take place in a familiar world, an environment that is already known by its inhabitants to a certain extent. A world is familiar when shared norms and values are present; when people assume that others perceive the world in a similar way and certain aspects of everyday life are taken for granted. We can conclude that trust can be the dominant strategy to reduce complexity; but it is never the sole strategy.

Second, trust is not the preferred dominant strategy to reduce complexity in all situations. When it is of the utmost importance that a certain goal be reached or a, particularly, protocol be followed, other strategies may be more appropriate. For example, although trust is an important aspect in securing a nuclear plant, it is not the dominant strategy. Using control mechanisms such as security protocols that one cannot circumvent, or using security badges and biometric logging systems that control the access to different parts of the plant are better strategies to reduce the risks associated with a nuclear installation. To a certain extent, there still should be trust vested in the employees to follow the rules and in the technological systems in place. However, trust is not the dominant strategy in regulating the functioning of the nuclear plant.

6. Trust as a goal of cybersecurity

Trust is a fruitful strategy to deal with uncertainties. However, it is generally not recognised as an adequate regulatory strategy for cybersecurity. 'Trust is good, security is better', or so the saying goes (Keymolen, Corien, and Raab 2012, 24). Cybersecurity tends to focus on implementing rules and norms into systems to ensure the integrity of the communication and the stable functioning of the infrastructure. Rather than neutralising certain dangers, much work in the field of cybersecurity is focused on removing them. Although it is widely accepted by technicians and regulators alike that 100% security does not exist (Chandler 2009, 126–127; Singer and Friedman 2013, 70; Zedner 2003, 159), there still appears to be a tacit intention to come as close as possible to that goal. Consequently, in the relation 'trust-cybersecurity', security is seen as a *necessary condition* for trust but trust is not considered as *part* of cybersecurity. Security measures are put in place to enable a familiar world, necessary for trust to thrive. The Internet should have a taken-for-granted character to its users. To put it differently:

> If users had to decide every time they use an online service or make use of an application on their smartphone, whether or not to trust the underpinning infrastructure of the Internet, the costs would simply become too high. People would be overwhelmed by the uncertainty of such a complex and unstable environment and probably reject it as a valuable means of interaction. For trust to take place on the interpersonal level – or between a user and an organization –, the environment, whether or not online, should be familiar first, that is, stable and predictable. (Keymolen 2016, 108)

We also see this 'trust as a goal of cybersecurity perspective' reflected in policy documents (cf. Broeders 2015). For example, the Dutch National Cyber Security Agenda (NSCA) states that it is an explicit goal of cybersecurity to ensure a stable infrastructure to foster trust of users:

> [W]e cannot afford to let cyber criminals erode the trust we have – and need to have in the ICT infrastructure and the services it provides. Trust is a conditio sine qua non for normal economic transactions and inter-human communication. It is at the core of social order and economic prosperity, and in an increasingly ICT-dependent world, the security of ICT plays an ever more important role here (National Cyber Security Research Agenda II: 6–7)

In the academic literature, Nissenbaum (2001) has coined the perspective described above as 'trust through security'. She also recognises the strong emphasis on computer security as a means through which trust online can be established. Nissenbaum discerns three security mechanisms put in place to ensure trust online: *access control*, *transparency*

of identity, and *surveillance*. The first refers to passwords, firewalls, and other measures to ensure that only those actors who are allowed to enter – clients, citizens, members – do enter and those who are not allowed –hackers, spies, criminals – are blocked. The second mechanism is about making actors more identifiable. Even if a user does not willingly provide personal data, all sorts of cryptographic and profiling techniques are used to authenticate users. The basic idea is that if your identity is known you will think twice before acting malicious, as you can be held accountable for your deeds. The third mechanism is based on the idea that monitoring actions and behaviour online can prevent bad things from happening or at least could help to quickly and easily find the wrongdoers.

Nissenbaum is not against security. It is conspicuously clear that for specific online activities such as banking or e-commerce, high security is necessary. However, Nissenbaum (2004) warns against the seemingly self-evident move to strive for more security in all online domains and practices as it may endanger trust and the worthwhile practices trust facilitates. Reducing complexity and uncertainties should never become a permit to strive for overall security in a way that it narrows down freedom, which is nurtured by trust to develop (amongst others) innovative, creative, or political practices. She states:

> In a world that is complex and rich, the price of safety and certainty is limitation. Online as off, […] the cost of surety – certainty and security – is freedom and wide-ranging opportunity. (Nissenbaum 2004, 173–174)

7. Trust as an implicit part of a cybersecurity strategy

It is beyond doubt that trust is an important goal for cybersecurity. However, often under the radar, trust is also *part* of cybersecurity measures. Trust may be not the dominant strategy, but it certainly contributes to cybersecurity as a supporting, complexity-reducing strategy. In current regulatory strategies for cybersecurity, we discern at least three points where trust in fact plays a significant role: trust in human actors, trust in the functioning of technical systems, and trust as an attribute of risk assessment.

7.1. Trust in human actors

When taking a holistic approach in cyber security risk assessments (also see Section 2), not only the environmental and technical (hardware, software) aspects are considered. Human factors – defenders, users, and attackers – become part of the analysis as well. Including human factors in the risk assessment entails anticipating that certain expectations about human behaviour may not be fulfilled. Whereas in risk assessments it is a given that attackers act in unforeseen ways, it is sometimes overlooked that this also applies to defenders and users. They too may behave in deviant ways. For instance: defenders may circumvent protocols and users may be unable to detect risky situations due to information asymmetry. Notwithstanding their sometimes-precarious behaviour, defenders and users are expected to take on certain cybersecurity tasks and follow guidelines. For instance, defenders are supposed to have situational awareness and to be able to report and/or react to the information gathered; users are expected to take care of their passwords and other credentials to secure their interactions online.

The human actor in cybersecurity strategies, therefore, confronts regulators with a profound challenge: on the one hand, human actors with their specific roles and tasks are part

of the cybersecurity measures; on the other hand, their actions can only be steered and controlled by cybersecurity measures. To put it differently, in cybersecurity, defenders and users are *both risk and security enabler*.

Trust helps reconcile these conflicting roles. In the end, when cybersecurity assessments are developed and carried out, human actors are trusted to display certain behavioural responses based on which appropriate measures will be taken. Recently, Henshel et al. (2015) have taken a first step to make this implicit trust in human actors more tangible by developing a model that can be used to assess the trustworthiness of the human actors in cybersecurity.[2] Also from a policy perspective, the awareness grows that a mere cybersecurity strategy is not enough. Trust between the actors – often distributed over the public–private sphere – who have to put these strategies into practice is crucial as well (Heuvel and Baltink 2014).

7.2. Trust in systems

Techno-regulation is, as we have seen, an important regulatory strategy in the cybersecurity domain. Generally, the assumption is that inscribing rules into technology leads to high levels of compliance and thus is a very effective form of regulation.

While it is obviously true that technological control mechanisms such as cryptography, logging, and surveillance reduce complexity in the cybersecurity domain, we should not be blind for the new complexity these technologies at the same time also cause. First, where information and communication technology (ICT) systems generally are designed in such a way that they are easy to use, this does not necessarily imply they are also easy to understand (Keymolen 2016, 152). If defenders have no alternative means at their disposal to check if what the computer tells them is true; when they simply have to rely on the results the system displays. The system becomes what van den Hoven (1998) has coined an 'artificial authority' in which users have to put their trust. The fact that technology increasingly functions as a black box, increases dependence on *system trust* or *confidence in systems* (Luhmann 1988; Jalava 2003; Henshel et al. 2015). Second, as these systems themselves are often too complex to be completely understood, users not only have to trust the system but the experts who maintain the system as well (Luhmann 1979). Nowadays, parts of the system are delegated to experts. Experts may also function as 'facework commitments' (Giddens 1990). They mediate the interaction of the users and the systems. They become 'the face' of the system; making the system accessible to the user to a certain extent. However, the control of experts over the system also has its limits. Even computer experts acknowledge that the system sometimes can perform in a way that goes beyond their understanding (see for example Aupers 2002: who found that computer experts often experience these systems as autonomous forces). New systems are built upon old ones, continuous updates are needed and ICT systems always remain 'under construction'. All in all, this results in a technological knot only few are able to unravel.

7.3. Trust in risk assessment

Finally, trust is also implicitly part of the cybersecurity risk assessments, of the activity involved in defining which risks exist in cyberspace for a given party, what their probability and impact may be, and which measures and interventions ought to be taken to reduce

these risks to 'acceptable levels' (whatever we define these to be). Just as trust is a strategy to reduce complexity, a risk assessment is also a way of reducing complexity. More specifically, it reduces the complexity of a certain situation or event by translating it in risks and uncertainties. With risk we refer to an active and explicit engagement with future threats. When we talk about risks, we talk about the chance or probability that a certain – often undesirable – event will occur. When we refer to uncertainty, on the other hand, we face possible unpredictable outcomes (Knight 1921; Keymolen 2016, 69). Here, trust also implicitly enters the scene, as we have to trust that these unpredictable outcomes will not hinder our actions. These uncertainties cannot be removed, but only be neutralised. With trust these possible negative outcomes are moved to the background and the focus is turned to this one desired future state of affairs. However, risks and uncertainties cannot always be so easily discerned. So-called *systemic risks* – risks that are embedded in larger societal processes (Renn, Klinke, and van Asselt 2011, 235) – are highly complex in nature, making it more difficult to clearly detect chains of events. Moreover, the ambiguity surrounding these systemic risks often results in several viewpoints which all seem legitimate (Renn, Klinke, and van Asselt 2011, 235). Consequently, these systemic risks cannot easily be calculated as a function of probability and effects (Renn et al. 2011). In addition, the world does not only confront us with uncertainty because of the variability and indeterminacy of social processes, we are also aware that our knowledge of risk-determinacy, impact, and causal effect are limited. To put it differently, even when we talk about risks there is uncertainty because we might have doubts about our own risk perception. We may be more convinced about some risks than about others. Some authors, therefore, see uncertainty as an attribute of risk (Van Asselt 2000). To conclude, it becomes clear that risk assessments cannot eradicate complexity completely. Risk assessments provide regulators and defenders with models they can use to base their cybersecurity strategies on, but by default these models are never as rich as the empirical case they represent and therefore there is always the possibility of missing out on – what later turn out to be – important aspects. Consequently, while risk assessment is a dominant strategy in cybersecurity, it should not be neglected that in fact it functions in an amalgam of interdependent complexity-reducing strategies, of which trust is an important element.

8. Trust as an explicit part of a cybersecurity strategy

After establishing that trust is not merely a goal of cybersecurity but is also an *implicit part* of cybersecurity, we now want to go a step further and see if and how trust can also be an *explicit part* of cybersecurity.

That trust can also be an explicit part of security strategies is probably most evident in cases where security is 'outsourced'. Especially after 9/11, we witness an increase in what has been referred to as the introduction of *deputy sheriffs* (cf. Lahav and Guiraudon 2000; Torpey 2000). Organisations or people are asked to take on a role as deputy sheriff. They become the eyes and ears, as authorities cannot be everywhere. For example, when the public is actively asked to call if they see something suspicious, they become the deputy sheriffs of the police. Or when different organisations intensify their cooperation this can lead to the recruitment of professionals for assignments that lay beyond their initial field of expertise (e.g. in the domain of youth care: cf. Keymolen and Broeders 2013). On a similar note, Garland (2001) speaks of *responsibilisation*. People who are not

an actual expert or are not trained in a certain field are nevertheless giving responsibility to report to the police or other authorities.

Responsibilisation and the introduction of deputy sheriffs can be seen as a trust-based (cyber)security strategy.[3] For example, when governments call upon citizens to report suspicious situations, they trust citizens to be aware and react quickly by calling the number and report what they have seen. This strategy of course is not full-proof (if it was, it would not be a trust-based strategy). As the trustor, the government is vulnerable by relying on non-trained, perhaps not really interested citizens, because it might miss crucial information. This vulnerability, however, does not necessarily make it a bad strategy. Perhaps it is simply not possible because of capacity issues or costs involved to have ears and eyes everywhere and this trust-based approach might then be a good alternative. The trustor might not receive as much meaningful information as when there would be professionals on the ground, but still more information than when there would be no one paying attention.

When focusing on the domain of cybersecurity, we will now look into two examples in which security is being outsourced and a trust-based approach is being used to underpin the cybersecurity strategy. First, we will look into security reward programs as initiated by Google and Facebook. Second, we will look at peer-to-peer flagging of suspicious behaviour on the platform of Airbnb.

8.1. Security reward programs

As no software program or hardware device can be 100% full-proof safe, it is absolutely necessary – from a cybersecurity perspective – to continuously monitor and investigate the used technologies to discover bugs and weaknesses. As this is a very time-consuming task that, moreover, can only be carried out by people with sufficient expertise, it is not always feasible as a company to cover this in-house. Companies such as Facebook and Google have therefore captured this problem by calling upon the tech community to help them detect security issues in their services. In return for their efforts, people who find weaknesses and report them to the companies involved receive a reward.

Several reward programs are created to stimulate savvy people to engage in this security quest. Google, for example has installed a Google Vulnerability Reward Program to stimulate the detection of vulnerabilities in Google-owned websites and bugs in Google-developed apps and extensions. Rewards may range from $100 for finding information leakages to $20.000 for detecting bugs that give direct access to Google servers (e.g. sandbox escapes).[4] Other reward programs Google runs are a patch reward program, a Chrome reward program, and an Android reward program.[5]

Facebook has created the Facebook Bug Bounty program,[6] which is more or less similar to Google's. People who find security issues on Facebook or on another member of the Facebook imperium, can file a report, which Facebook will then investigate. If the bug is indeed a security risk the discoverer will be rewarded.

All in all, we can conclude that in the above-described cases, companies are trusting outsiders to be part of their cybersecurity strategy. On the one hand this makes companies vulnerable, as they come to depend on these outsiders, who they can (at best) nudge into participating by promising rewards but who are, in the end, out of their direct control. On the other hand, this trust-based approach may fill a blank in the cybersecurity strategy of a

company, as it would be too time-consuming or costly to keep these matters in their own hands.

8.2. Peer-to-peer security

Another example of security being outsourced on a trust-based manner is the reporting of suspicious behaviour of users by other peers. In the shared economy, which is characterized by cutting out the middle man and bottom-up regulation (Botsman and Rogers 2010; Botsman 2012), peer-to-peer security is an important part of the overall platform security.

The most obvious tool that is set in place to ensure peer-to-peer security is the possibility of rating the trustworthiness of other peers. By rating the interactions with other peers, it becomes clear for the whole community who is a secure partner to deal with and who is to be trusted less.

Some platforms, such as Airbnb, go a step further and enable their users to 'flag' other people. On any moment in the interaction on Airbnb, users have the possibility to click on a flag when they believe something is suspicious or inappropriate.[7] Airbnb investigates each flag on a case-by-case basis.

Alternatively, Airbnb could also choose to screen all users of their platform and monitor every interaction. And although they certainly do have some (technological) security measures set in place (Chesky 2011; Gannes 2013; Tanz 2014), by relying on their users to flag suspicious events, they make their users part of their cybersecurity strategies. Airbnb depends on their users to report fishy situations based on which they then take action. Controlling every interaction intensively would probably prevent dubious situations from happening at all, however, it would come at a price of losing freedom (cf. Nissenbaum 2001), which is key to the shared economy.

9. Conclusion

This article started from the assessment that cybersecurity is an increasingly important theme, and that, aside from the technical community, it also increasingly receives attention from governments as well. Governments in many Western countries are grappling with ways in which they can impact cybersecurity in a positive way, predominantly through the use of regulatory interventions. As we have argued in this article, we find it striking that certain regulatory strategies have gained widespread implementation, while others have largely been ignored. We have discussed techno-regulation as a prime example of the former, and trust of the latter. Underneath the reliance on techno-regulation, we have argued, is a deep-seated – though probably false – assumption that using techno-regulation leads to more control, and more control equals more cybersecurity. Since the most important threat to cybersecurity comes from intentional, highly savvy attackers that seek to exploit systems and find vulnerabilities, the use of a strategy such as techno-regulation in all likelihood has very little effect with respect to increasing security. After all, these kinds of attackers make it their business to break into *any* system, regardless of its design and the values or rules or norms this design promotes. In contrast, techno-regulatory interventions may have negative effects for end users, because they limit and shape their action space. So while techno-regulatory interventions may promise more control and more cybersecurity, we suspect that oftentimes

these benefits will not materialise, while end users pay a price in terms of their freedom to act.

An overly strong reliance on techno-regulation as the dominant solution for cybersecurity issues might be unwise, therefore, and this is why it makes sense to also turn to other regulatory strategies. In this article, we have focused on trust as a key candidate. While trust is currently considered a key *goal* for cybersecurity, up until this point in time it is not explicitly considered to be a potential candidate to help improve cybersecurity as well. We have shown, however, that trust is already a key, albeit implicit, element of many cybersecurity strategies (both technical and non-technical). We have also shown that it can be used very effectively as an explicit element of cybersecurity strategies, for companies and potentially also for governments themselves.

Notes

1. Or businesses or any other party who wishes to increase control over (an element of) cyberspace. In this article, we focus only on governments. But much of what is said here is applicable to any party seeking to regulate the behaviour of others.
2. It is evident that 'trustworthiness' is deemed crucial when one considers to put trust to use as an explicit regulatory strategy in the cybersecurity domain. Questions such as: 'which design choices foster trustworthiness – both on the psychological and technical level?' or 'how can trustworthiness be measured and become a part of risk-assessments?' then come in to play. To understand trustworthiness, one has to take a contextual approach and analyse the intertwining of the different complexity-reducing strategies that are active in a specific case. For example, a comprehensive legal framework may presort the action of actors enhancing their trustworthiness, consequently lowering the barrier to place trust. However, as this article focuses on the choices of regulatory strategies and not so much on the implementation of these strategies, nor takes a contextual approach by delving into a specific case, 'trustworthiness' unfortunately falls out of its scope.
3. Responsibilisation and the introduction of deputy sheriffs do not necessarily take the shape of a trust-based strategy. Responsibilisation can also be enforced, for example, by inscribing it in the system or by holding employers accountable if they do not fulfil their deputy sheriff function.
4. https://www.google.com/about/appsecurity/reward-program/index.html, Accessed 10 July 2016.
5. https://www.google.com/about/appsecurity/programs-home/, Accessed 10 July 2016.
6. https://www.facebook.com/BugBounty/info?tab=page_info, Accessed 10 July 2016.
7. https://www.airbnb.nl/help/article/4/how-does-airbnb-help-build-trust-between-hosts-and-guests, Accessed 10 July 2016.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Appazov, Artur. 2014. *Legal Aspects of Cybersecurity*. Copenhagen: Justitsministeriet. 70 p.

Asselt, van Marjolein. 2000. *Perspectives on Uncertainty and Risk*. Dordrecht: Kluwer.

Aupers, Stef. 2002. "The Revenge of the Machines: On Modernity, Digital Technology and Animism." *Asian Journal of Social Science* 30 (2): 199–220.

Baier, Annette. 1986. "Trust and Antitrust." *Ethics* 96 (2): 231–260.

Benoliel, Daniel. 2004. "Technological Standards, Inc.: Rethinking Cyberspace Regulatory Epistemology." *California Law Review* 92: 1069–1117.

Botsman, Rachel. 2012. *The Currency of the New Economy is Trust*. Ted Talk, 09-24-2012.
Botsman, Rachel, and Roo Rogers. 2010. *What's Mine is Yours: The Rise of Collaborative Consumption*. New York, NY: Harper Business.
Broeders, D.W.J. 2015. *The Public Core of the Internet. An international Agenda for Internet Governance*. Amsterdam: Amsterdam University Press.
Brownsword, Roger, and Karen Yeung. 2008a. *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*. Portland, OR: Hart.
Brownsword, Roger, and Karen Yeung. 2008b. "Regulating Technologies: Tools, Targets and Thematics." In *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, edited by Roger Brownsword, and Karin Yeung, 3–23. Oxford: Hart.
Chandler, Jennifer. 2009. "Privacy Versus National Security: Clarifying the Trade-Off." In *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, edited by Ian R. Kerr, C. Lucock, and V. Steeves, 121–138. Oxford: Oxford University Press.
Chesky, B. 2011. "On Safety: A Word From Airbnb." *Techcrunch*. Accessed 12 December 2015. http://techcrunch.com/2011/07/27/on-safety-a-word-from-airbnb/.
Coeckelbergh, Mark. 2012. "Can we Trust Robots?" *Ethics and Information Technology* 14: 53–60. doi: 10.1007/s10676-011-9279-1
Gannes, Liz. 2013. "After Home-In Trashing Incident, Airbnb Builds an In-House Enforcer Team." *AllThingsD* Accessed 24 July 2015. http://allthingsd.com/20130716/after-home-trashing-incident-airbnb-builds-an-in-house-enforcer-team/.
Garland, David. 2001. *The Culture of Control. Crime and Social Order in Contemporary Society*. Chicago, IL: The University of Chicago Press.
Giddens, Anthony. 1990. *The Consequences of Modernity*. Cambridge: Polity Press in association with Basil Blackwell, Oxford, UK.
Giddens, Anthony. 1991. *Modernity and Self-Identity. Self and Society in the Late Modern Age*. Stanford, CA: Stanford University Press.
Giddens, Anthony, and Christopher Pierson. 1998. *Conversations with Anthony Giddens: Making Sense of Modernity*. Stanford, CA: Stanford University Press.
Good, David. 1988. "Individuals, Interpersonal Relations, and Trust." In *Trust: Making and Breaking Cooperative Relations*, edited by D. Gambetta, 31–48. Oxford: Basil Blackwell.
Hansen, Lene, and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Security Studies Quarterly* 53 (4): 1155–1175.
Hardin, Russell. 2001. "Conceptions and Explanations of Trust." In *Trust in Society*, edited by K.S. Cook, 3–39. New York, NY: Russel Sage Foundation.
Hardin, Russell. 2006. *Trust*. Cambridge: Polity Press.
Henshel, D., M.G. Cains, B. Hoffman, and T. Kelley. 2015. "Trust as a Human Factor in Holistic Cyber Security Risk Assessment." *Procedia Manufacturing* 3: 1117–1124.
Heuvel, Elly Van Den, and Gerben Klein Baltink. 2014. "Coordination and Cooperation in Cyber Network Defense: the Dutch Efforts to Prevent and Respond." In *Best Practices in Computer Network Defense: Incident Detection and Response. NATO Science for Peace and Security Series D: Information and Communication Security*, edited by M. Hathaway, 118–130. Amsterdam: IOS Press.
Hildebrandt, Mireille. 2009. "Technology and the End of Law." In *Facing the Limits of the Law*, edited by Erik Claes, Wouter Devroe, and Bert Keirsbilck, 443–465. Heidelberg: Springer.
Hildebrandt, Mireille. 2011. "Legal Protection by Design: Objections and Refutations." *Legisprudence* 5 (2): 223–249.
van den Hoven, Jeroen. 1998. "Moral Responsibilty, Public Office and Information Technology." In *Public Administration in an Information Age*, edited by I. Snellen, and W. van de Donk, 97–112. Amsterdam: IOS Press.
Jalava, Janne. 2003. "From Norms to Trust: The Luhmannian Connections Between Trust and System." *European Journal of Social Theory* 6 (2): 173–190.
Kerr, Ian R., ed. 2010. "Digital Locks and the Automation of Virtue." In *From 'Radical Extremism' to 'Balanced Copyright': Canadian Copyright and the Digital Agenda*, edited by Michael Geist, 247–303. Toronto: Irwin Law. https://ssrn.com/abstract=2115655

Kesan, Jay P., and Rajiv C. Shah. 2006. "Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics." *Notre Dame Law Review* 82 (2): 583–634.
Keymolen, Esther. 2016. *Trust on the Line. A Philosophical Exploration of Trust in the Networked Era*. Den Hague: Wolf Legal Publishers.
Keymolen, Esther, and Dennis Broeders. 2013. "Innocence Lost: Care and Control in Dutch Digital Youth Care." *British Journal of Social Work* 43 (1): 41–63.
Keymolen, Esther, J.E.J. Prins Corien, and Charles Raab. 2012. "Trust and ICT: New Challenges for Public Administration." In *The Coming of Age of ICT in Public Administration*, edited by Wim van de Donk, and Mark Thaens, 21–35. Amsterdam: IOS Press.
Knight, Frank H. 1921. *Risk, Uncertainty and Profit*. Boston, MA: Houghton Mifflin Company.
de Laat, Paul. 2005. "Trusting Virtual Trust." *Ethics and Information Technology* 7: 167–180.
Lahav, G., and V. Guiraudon. 2000. "Comparative Perspectives on Border Control: Away From the Border and Outside the State." In *The Wall Around the West. State Borders and Immigration Controls in North America and Europe*, edited by Andreas, P., and T. Snyder, 55–77. Lanham: Rowman and Littlefield publishers.
Lahno, Bernd, and Uwe Matzat. 2004. "From the Editors. Trust and Community on the Internet. Opportunities and Restrictions for Online Cooperation." *Analyse & Kritik. Zeitschrift für Sozialtheorie* 26 (1): 1–6.
Latham, Robert. 2003. *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*. New York, NY: The New Press.
Leenes, Ronald. 2011. "Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology." *Legisprudence* 5 (2): 143–169.
Lessig, Lawrence. 1999. "The Law of the Horse: What Cyberlaw Might Teach." *Harvard Law Review* 113 (501): 501–549.
Lessig, Lawrence. 2006. *Code: Version 2.0*. 2nd ed. New York, NY: Basic Books.
Luhmann, Niklas. 1979. *Trust and Power. Two Works by Niklas Luhmann. Translated by Howard Davis*. New York, NY: John Wiley & Sons.
Luhmann, Niklas. 1988. "Familiarity, Confidence, Trust: Problems and Alternatives." In *Trust: Making and Breaking Cooperative Relations*, edited by D. Gambetta, 94–107. Oxford: Blackwell Publishers.
McKnight, D. H., and N. L. Chervany. 2002. "What Trust Means in e-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology." *International Journal of Electronic Commerce* 6: 35–60.
McKnight, D. H., V. Choudhury, and C. Kacmar. 2002. "Developing and Validating Trust Measures for e-Commerce: An Integrative Typology." *Information Systems Research* 13 (3): 334–359.
McLeod, C. 2014. "Trust." In *Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta. https://plato.stanford.edu
Möllering, G. 2006. *Trust: Reason, Routine, Reflexivity*. Amsterdam: Elsevier.
Nissenbaum, Helen. 2001. "Securing Trust Online: Wisdom or Oxymoron?" *Boston University Law Review* 81: 101–131.
Nissenbaum, Helen. 2004. "Will Security Enhance Trust Online, or Supplant It?" In *Trust and Distrust in Organizations: Dilemmas and Approaches*, edited by Roderick M. Kramer, and Karen S. Cook, 155–188. New York, NY: Russell Sage Foundation.
Nissenbaum, Helen. 2005. "Where Computer Security Meets National Security." *Ethics and Information Technology* 7 (2): 61–73. Kluwer Academic Publishers.
Nooteboom, Bart. 2013. "Trust and Innovation." In *Handbook of Advances in Trust Research*, edited by R. Bachmann, and A. Zaheer, 106–125. Northampton, MA: Edward Elgar.
Pettit, Philip. 2004. "Trust, Reliance and the Internet." *Analyse & Kritik* 26: 108–121.
Renn, Ortwin, Andreas Klinke, and Marjolein van Asselt. 2011. "Coping with Complexity, Uncertainty and Ambiguity in Risk Governance: A Synthesis." *AMBIO: A Journal of the Human Environment* 40 (2): 231–246. doi:10.1007/s13280-010-0134-0
Schneier, Bruce. 2004. *Secrets & Lies: Digital Security in a Networked World*. 2nd ed. Indianapolis, IN: Wiley Publishers.

Seppanen, Risto, Kirsimarja Blomqvist, and Sanna Sundqvist. 2007. "Measuring Inter-Organisational Trust: A Critical Review of the Emperical Research in 1990-2003." *Industrial Marketing Management* 36 (2): 453–486.

Simon, Judith. 2013. "Trust." In *Oxford Bibliographies in Philosophy*, edited by D. Pritchard. New York, NY: Oxford University Press. http://www.itas.kit.edu/pub/v/2013/simo13a.pdf

Simpson, Thomas W. 2011. "e-Trust and Reputation." *Ethics and Information Technology* 13 (1): 29–38.

Singer, Peter W., and Allan Friedman. 2013. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford, NY: Oxford University Press.

Taddeo, Mariarosaria. 2010. "Trust in Technology: A Distinctive and a Problematic Relation." *Knowledge, Technology & Policy* 23 (3): 283–286.

Taddeo, Mariarosaria. 2011. "The Role of e-Trust in Distributed Artificial Systems." In *Trust and Virtual Worlds*, edited by Charles Ess, and May Thorseth, 75–88. New York, NY: Peter Lang.

Taddeo, Mariarosaria, and Luciano Floridi. 2011. "The Case for e-Trust." *Ethics and Information Technology* 13 (1): 1–3.

Tamanaha, Brian Z. 2007. "A Concise Guide to the Rule of Law". *Florence Workshop on the Rule of Law*, edited by Neil Walker and Gianluigi Palombella, Hart Publishing Company, 2007; St. John's Legal Studies Research Paper No. 07-0082. Available at SSRN: http://ssrn.com/abstract=1012051.

Tanz, Jason. 2014. "How Airbnb and Lyft finally got Americans to trust each other." *Wired* Accessed 26 April. http://www.wired.com/2014/04/trust-in-the-share-economy/

Torpey, John. 2000. *The Invention of the Passport: Surveillance, Citizenship, and the State*. Cambridge: Cambridge University Press.

Van den Berg, Bibi. 2014. "Colouring Inside the Lines: Using Technology to Regulate Children's Behaviour Online." In *Minding Minors Wandering the Web: Regulating Online Child Safety*, edited by Simone Van der Hof, Bibi Van den Berg, and Bart Schermer, 67–90. The Hague: TCM Asser Press.

Van den Berg, Bibi, and Ronald Leenes. 2013. "Abort, Retry, Fail: Scoping Techno-Regulation and Other Techno-Effects." In *Human Law and Computer Law: Comparative Perspectives*, edited by Mireille Hildebrandt, and Jeanne Gaakeer, 67–89. Dordrecht: Springer.

Van den Berg, Jan, Jacqueline Van Zoggel, Mireille Snels, Mark Van Leeuwen, Sergei Boeke, Leo Van Koppen, Jan Van der Lubbe, Bibi Van den Berg, and Tony De Bos. 2014. 'On (the Emergence of) Cyber Security Science and Its Challenges for Cyber Security Education'. *NATO STO/IST-122 Symposium in Tallin*, 1–10.

Warkentin, Merrill, David Gefen, Paul A. Pavlou, and Gregory M. Rose. 2002. "Encouraging Citizen Adoption of e-Government by Building Trust." *Electronic Markets* 12 (3): 157–162.

Wu, Tim. 2003. "When Code Isn't Law." *Virginia Law Review* 89 (4): 679–751.

Yeung, Karen. 2008. "Towards an Understanding of Design-Based Instruments." In *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, edited by Roger Brownsword, and Karin Yeung, 79–109. Oxford: Hart.

Yeung, Karen. 2011. "Can We Employ Design-Based Regulation While Avoiding Brave New World?" *Law, Innovation and Technology* 3 (1): 1–29.

Zedner, Lucia. 2003. "Too Much Security?" *International Journal of the Sociology of Law* 31 (3): 155–184. doi:10.1016/j.ijsl.2003.09.002