Georgia Tech

INTERNET GOVERNANCE PROJECT

R Street

Free markets. Real solutions.

R STREET POLICY STUDY NO. 121
November 2017

MARKETS VS. MANDATES: SOLUTIONS FOR SECURING THE INTERNET OF THINGS

Farzaneh Badiei, Ian Adams and Joe Kane

CONTENTS

EXECUTIVE SUMMARY

The internet of things (IoT) is "an array of connected objects with unique identifiers that have the ability to transfer data over a network."[1] IoT devices have diverse applications across disparate fields. For instance, transportation, agriculture and health care could all use connected devices to increase the quality and efficiency of their processes and products. However, introducing networked devices inevitably comes with new security risks. When everything from one's car to one's toaster[2] is connected to the internet, both the number of attack surfaces and their potential damage is multiplied.

Thus, in order to maximize the benefits of the IoT, we must develop a policy framework that is able to keep up with these evolving and expanding threats and that can address the damage caused when security measures fail. Accordingly, this paper examines different approaches to IoT security and argues that market-oriented solutions and incentives, rather than ex-ante[3] regulations and onerous liability rules are best suited to foster both security and innovation.

INTRODUCTION

It is now a common refrain that IoT security suffers from a market failure that necessitates regulation. For example, cybersecurity analyst Bruce Schneier argues that the IoT faces "a market failure that can't get fixed on its own," and that "government is the only solution."[4] Schneier is not alone in such a sentiment. Sen. Mark Warner (D-Va.) has also cited market failure as the driving force behind recently introduced IoT legislation:

> This legislation would establish thorough, yet flexible, guidelines for Federal Government procurements of connected devices. My hope is that this legislation will remedy the obvious market failure that has occurred

1. Anne Hobson, "Aligning cybersecurity incentives in an interconnected world," R Street Policy Study No. 86, February 2017, 2. https://goo.gl/aoYX4P.

2. Hans Scharler, "Social Networking for My Toaster," Thinking About Things, Dec. 8, 2008. http://nothans.com/social-networking-for-my-toaster.

3. Ex-ante regulations are those that attempt to address cybersecurity before attacks occur. Such measures can be undertaken by both the government and the private sector. They are distinguished from ex-post measures, which address damage or liability after an incident has occurred.

4. Bruce Schneier, "We Need to Save the Internet from the Internet of Things," Motherboard, Oct. 6, 2016. https://goo.gl/tHHFgG.

and encourage device manufacturers to compete on the security of their products.[5]

Despite such claims, critics have not yet made a compelling empirical case for the kind of market failure in IoT security that necessitates a regulatory solution. No matter how serious, anecdotal incidents alone do not prove that a systemic market failure exists or that private markets are unresponsive to cyber incidents.[6] Before we invite heavy-handed government interventions, we must have greater justification for why they would be effective and consider more deeply the costs they would impose. Even with today's security challenges in IoT, long term security may still be better provided by allowing markets to adjust rather than imposing prescriptive regulation that could stifle new innovation.

IOT CYBERSECURITY AND MARKET FAILURE

Strong security often has benefits and lacking security carries costs that spill over to third parties. On the consumer level, an unsecure device creates vulnerabilities not just for the device owner but also for other devices to which that device connects. Even when the transaction costs are high, market arrangements often result in private parties internalizing costs of security provision as opposed to leaving devices vulnerable.[7] Additionally, if the benefits to the parties of the transaction are greater than the costs of acquiring them, then the externality will be internalized irrespective of how large the spillover effects might have been.

As an example, consider the following scenario: Suppose the costs of failing to secure a device total $100,[8] but the costs to the rest of the IoT ecosystem from that insecure device total $100,000. We might expect that this externality would result in security being underprovided. But if the cost to secure the device is $50, then it is more likely that the device owner will secure it themselves since the expenditure is cheaper than the $100 expected loss. So even though the private costs are much lower than the external costs, the costs are still internalized by the private party when they are "inframarginal."[9] It should be noted that such an example does not mean that everyone will always take appropriate security precautions with their devices or that market failure can never exist in IoT security. In fact, there are almost certainly cases in which the specific costs and benefits do not result in those risks being internalized. The example merely shows that the presence of an externality does not necessarily entail market failure and thus more evidence is needed.

In order to assess the actual market conditions, we must look beyond the existence of particular security incidents to determine if a market failure exists. Only after a systematic evaluation can we discern whether or not government intervention is a plausible remedy. However, to analyze all the benefits and costs, including opportunity costs, is a challenging process, and it is difficult to measure how much cybersecurity and IoT security markets ought to provide in order to prove or disprove their failure. Given this difficulty, it is impossible to say for certain whether a market failure has occurred. For this reason, the debate should be instead focused on the efficacy of particular regulations and security measures, accounting for both their costs and benefits.

Despite the uncertainty surrounding claims of a market failure, one thing is certain: we should be wary about mandating costly regulatory measures, even if they might marginally increase security in the short term. For instance, home alarm systems provide some protection against burglary. However, they are also expensive to install, maintain and monitor, and they do not always work against knowledgeable and determined criminals. Accordingly, it is not obvious that government should mandate that all homeowners purchase and maintain such systems, especially since crime rates also vary across areas. Rather, it is likely that the cost of doing so would exceed the total losses associated with all burglaries. Likewise with the IoT: mandated security measures often have costs that exceed their benefits and do not account for variations among different use cases.

Government intervention in the name of IoT security should not, therefore, enjoy a presumption of success or harmlessness. It is not a given that regulation will strike an optimal balance of security and flexibility better than market driven options. Government regulatory failure may well prove as much or more of a problem as the market failure it seeks to forestall. Accordingly, the success of the status quo in the face of attacks can help inform a discussion of the present state of the market and the advisability of government reaction to security threats.

THE MIRAI BOTNET: THE CURRENT SYSTEM IN PRACTICE

In 2016, a high-profile incident involving a botnet named "Mirai" clearly demonstrated the difficulty of striking a sensible balance between security and innovation.[10] A botnet is composed of many IoT devices commandeered for the purpose of carrying out harmful activities, such as dedicated

5. Office of Senator Mark R. Warner, "Senators Introduce Bipartisan Legislation to Improve Cybersecurity of "Internet-of-Things" (IoT) Devices," Press Release, Aug. 1, 2017. https://goo.gl/QgpQ9w.

6. Eli Dourado, "Is There a Cybersecurity Market Failure?", *Mercatus Center Working Paper* No. 12-05, January 2012, 4. https://goo.gl/TQESmx.

7. Ibid., 9-12. https://goo.gl/TQESmx.

8. This figure should be read as net expected costs, controlling for the probability of the event happening; e.g. a $200 attack with a 50 percent chance of occurring has a $100 expected cost.

9. Dourado, 4-18. https://goo.gl/TQESmx.

10. In Japanese, "mirai" means "the future."

denial of service (DDoS) attacks. The Mirai botnet was created by pooling together compromised devices—like routers and cameras—that used the factory default username and password. Once brought online, it was able to conduct DDoS attacks that temporarily brought down several major websites.[11]

While those that argue the case for a market failure and government intervention in IoT cybersecurity point to this incident as proof that manufacturing companies do not take appropriate security measures—even after attacks—the data are ambiguous on this account. For example, one study conducted after the Mirai botnet incident indicated that 49.3 percent of IoT device manufacturers already have a process for changing the default password on their devices.[12] Moreover, at least some portion of the market took action in the wake of Mirai. For instance, the Chinese company XiongMai Technologies, whose cameras were compromised, recalled 10,000 of its infected devices,[13] asked all of its customers to perform the necessary updates and resolved the vulnerability for its future products.[14] Further, another manufacturing company attacked by Mirai, Axis Communications, reported its device vulnerabilities to customers and provided instructions for upgrading the firmware needed to fix them.[15] And, as Jim Hunter explains for *TechCrunch*, IoT consortiums (IOTC) have also increased their attentiveness to the security of their products:

> On a more hopeful note, the industry is not just sitting idly waiting for [the proliferation of vulnerable devices] to happen. [...] The IOTC's key directive is to raise awareness among all stakeholders in IoT regarding the relatively simple steps we can adhere to as an industry to protect consumers, devices and the internet community at large. There are similar efforts afoot globally.[16]

Indeed, other IoT device-makers that were victimized by Mirai, such as Hikvision, Samsung and Panasonic have changed their protocols to require unique and complex passwords by default.[17] After the attack, Microsoft also launched the "Azure" security initiative that helped its customers to evaluate the safety of their devices,[18] while companies like Nexusgard provided IoT security products designed to detect and block IoT DDoS attacks.[19]

This suggests that as security weaknesses become more noticeable, markets will, in fact, respond and industry groups will help to develop new norms and standards. Whether the steps taken by private firms in the wake of the Mirai attack were sufficient is still unclear. However, what is clear is that the market is taking steps to provide IoT security on its own. In this respect, it is also critical to remember that this particular marketplace is still quite young and thus developments may start off weak and then grow stronger as manufacturers better understand threats and how to respond to them.[20] This was the also this case with other emerging technologies, such as PC security and cell phones. Likewise, the IoT security market should be allowed to grow rather than be replaced with regulation.

After all, not only do government regulators not possess special foresight that allows them to respond more quickly to attacks, but legislative and bureaucratic processes are notoriously slow. Government regulation should therefore be viewed as only one of multiple alternatives—and as inferior to less restrictive, market-driven ones.

GOVERNMENT REGULATION

Despite existing legal frameworks, expanded government regulation of IoT security has been proposed in a variety of forms, including mandatory registration and pre-market approval. At first glance, these proposed measures may have some appeal, but ultimately their shortcomings outweigh their benefits.

Public registration

One proposed avenue of additional government intervention is mandatory device registration. Such an approach allows new devices to be authenticated and provides an opportunity for the entity with which a device is registered to maintain ongoing oversight of its security measures. For instance, registrars may require that the devices meet certain security standards or best practices before they are included in the registry or allowed to connect to other devices on the registrar's network. The result of such an approach is a universe of trusted devices that can safely and easily "talk" to each

11. Manos Antonakakis, Tim April, et al., "Understanding the Mirai Botnet," 26th USENIX Security Symposium, August, 2017, 1093. https://goo.gl/UhBwLb.

12. "IOT Security Survey," Lieberman Software, 2017, 6. https://goo.gl/RNbvTv.

13. Sija Jian and Jim Finkle "China's Xiongmai to recall up to 10,000 webcams after hack," *Reuters*, Oct. 25, 2016. https://goo.gl/Jj8p5w.

14. Michael Kan, "Chinese firm admits its hacked products were behind Friday's DDOS attack," *Computerworld*, Oct. 23, 2016. https://goo.gl/vWUxw5.

15. "Axis recommends firmware upgrade to address security vulnerability," Axis Communications, July 6, 2016. https://goo.gl/mjvJrH.

16. Jim Hunter, "IoT redux... this time, it's personal," *TechCrunch*, Dec. 28, 2016. https://goo.gl/gwvzK6.

17. Brian Krebs, "Did the Mirai Botnet Really Take Liberia Offline?," *Krebs on Security*, Nov. 4, 2016. https://goo.gl/hvJZUM.

18. "Securing the internet of things: Introducing the Security Program for Azure IoT," *Microsoft Secure*, Oct. 26, 2016. https://goo.gl/4PbAM1.

19. "Patching DNS Vulnerabilities Protect Mission-critical Online Services," Nexusguard, https://goo.gl/27sgie.

20. See, e.g., Jack Wallen, "iOS and Android security: A timeline of the highlights and the lowlights," *TechRepublic*, June 26, 2017. https://goo.gl/UgFrbX; and David Emm, "Changing threats, changing solutions: A history of viruses and antivirus," Securelist, April 14, 2008. https://goo.gl/YyXRyH.

other. When security problems do arise, registration allows compromised devices to be quickly identified and diagnosed. Registered devices can also be cross-referenced with known threats on an ongoing basis, so vulnerable devices can be identified and repaired. Proponents of this form of ex-ante regulation argue that it will bolster security throughout the IoT.

The main advantage of a government-run registry is that it can be made mandatory via statute or regulation, as device owners may opt out of registration if they are allowed. However, in a public registry, all devices within the jurisdiction of a government must meet the registration requirements and thus for the government of a large population, mandatory registration can create a large pool in which, theoretically, all devices meet the required standards. A single, mandatory system may also ensure better interoperability between devices because they all use the same standards and protocols.

However, this feature can also be considered a "bug" because a flaw in the system would be coterminous with the universe of registered devices. In other words, compromising one device in a jurisdiction with a single mandatory registration standard would result in many more being compromised, as well.

Other drawbacks to mandatory, public registries pertain to the operational signals and incentives that surround the creation and maintenance of the registration standards. One fundamental limitation of the public sector is the inability of governments to rely on profit and loss signals to the same extent that private markets do. Governments are not disciplined by profit and loss because their revenue is a function of taxation rather than voluntary trade. The solution for a government program that lacks the resources to continue its activities is not to go out of business, but rather to petition for more funding. Because governments do not have access to the market signals to which private actors must respond, it is more difficult for governmental decision-makers to gauge whether their choices have yielded a productive outcome. To be sure, security can always be marginally increased by expending more resources on it, but whether that cost is worthwhile given the alternative uses of those resources is hard to calculate without using market prices and calculations of profit and loss.

Furthermore, the incentives created by government-mandated registration schemes do not work in favor of consumers. If we view bureaucrats as individuals just as self-interested as any other individuals,[21] it is potentially problematic that those who will make decisions about registration standards do not directly benefit from creating the optimal registration system. Nor do they benefit from consistently updating the standards in response to threats. Rather, they benefit by prolonging their own necessity and increasing their own budgets.[22] Further, that their budgets depend on the political process means that IoT security has the potential to become merely a political "football."

Government agencies are also vulnerable to capture by the industries they seek to regulate because a single set of standards may function to choose winners and losers among competing manufacturers with different security techniques. These developments would compromise the strength and consistency of the security apparatus.

By their very nature, governments are also slower to respond, which makes them ill-suited to respond to cyber threats that occur in real time. Unlike private industry, the government is obligated to adhere to various processes of public participation. To use the United States as an example, the legislative process requires bicameralism and presentment, whereby standards are promulgated through both houses of the legislature and then signed into law by the executive. In the regulatory context, then, the Administrative Procedures Act[23] functions as a de facto brake on the development and updating of standards because doing so would likely require a notice, comment and publication process that must take place over months.[24]

Moreover, government registration programs are not as universal as they might seem because they are limited by the capacity of the government that implements them. Not all governments have the technical expertise to run a registry or control a large area. While the United States, for example, could require registration of all devices within its borders, it cannot (without tremendous geopolitical and pecuniary cost) force European or Chinese devices to meet the same standards. This will be a recurring problem for security measures purveyed and enforced by national governments because the internet and threats against it are global and generally not limited to the boundaries of nation-states. Here, private industry—in the form of multinational corporations—has an advantage: because they operate in many nation-states, they have the potential to unify standards across national borders.

Pre-market approval

Another IoT security regulation that is currently being considered is for government regulators to approve all connect-

21. James M. Buchanan, "Public Choice: Politics Without Romance," *Policy*, Spring 2003, 16. https://goo.gl/3N6zdY.

22. William A. Niskanen, "The Peculiar Economics of Bureaucracy," *The American Economic Review* 58:2, (May 1968), 303. https://goo.gl/BR66aA.

23. 5 U.S.C. §§ 500-596. The 1946 Administrative Procedures Act specifies the process for U.S. administrative agencies to make regulations, including timelines for notice and comment on proposed rules. Agencies that regulate IoT security would be subject to this statute.

24. 5 U.S.C. § 553.

ed devices before they are available on the market. Proponents of this form argue that pre-market approval can apply to the design of the device itself, to its software and to subsequent software updates. However, such claims rest on the false assumption that security vulnerabilities not addressed by manufacturers can be easily discovered by regulators. This is not necessarily the case and even if these potential weaknesses could be determined by the government, the process would be costly and cause unnecessary delays that would ultimately diminish, rather than bolster cybersecurity measures.

Particularly with IoT security, delays are not just inconveniences, as updates to devices and software are essential to repair vulnerabilities or respond to attacks. Thus to require these updates to be approved by a government entity before rollout could mean that attacks and their subsequent damage will multiply while bureaucratic deliberations grind on. Pre-market approval systems in other device markets show that the delays they cause are no trivial concern. For example, some medical devices spend more than 20 months in similar processes.[25]

Additionally, the perverse incentives predicted in the context of government registration are even more salient for pre-market approval. For instance, if the government approves a device that is later compromised, the costs are easily seen and the approving agency will be blamed for its failure to spot the vulnerability and prohibit the device from entering the market. On the other hand, if the responsible agency denies approval for a device that would have been reasonably secure and could have provided benefits to users, those lost benefits are unseen and few will notice. Thus, regulators will tend to be overly precautionary. To focus too much on potential failures and neglect the opportunity costs of caution will lead to under-approval of new devices. Worse, it may also lead to a decline in innovation, as time and resources that could otherwise be devoted to designing more useful, more secure devices will need to be expended on navigating the approval process.

MARKET-DRIVEN MEASURES

In light of the often-counterproductive issues caused by these various regulatory approaches, the creation of an innovation-friendly framework can best be accomplished by deferring to market-driven mechanisms. Accordingly, private registration, cyber insurance and ex-post contractual arrangements have significant advantages over the more interventionist options.

25. Ariel Dora Stern, "Innovation under Regulatory Uncertainty: Evidence from Medical Technology," *Harvard Business School Working Paper* No. 16-005, September 30, 2016, 23-24. https://goo.gl/ofPsau. This figure is an implication of Stern's findings that pioneer devices spend 7.2 months longer in the approval process than similar devices that develop later and that this represents a 34 percent delay.

Private Registration

The lack of market signals and territorial boundaries faced by government registration requirements mean that those regimes will not find the right standards to maximize the net benefits of the IoT. However, the alternative, private registration, overcomes these obstacles by making use of profit and loss feedback and operating internationally.

What's more, private systems are already in use. For example, Microsoft's Azure Registry provides secure storage of device identities and security keys.[26] It facilitates the creation of "allow" or "block" lists in order to enable network operators to control how their devices connect and communicate with others on the network. Likewise, Amazon Web Services' (AWS) registers devices with certificates signed with public-private keys in order to securely identify which devices can be trusted. It also uses identity and access management (IAM) to allow for control of different groups of devices and users.[27] Although still in beta testing, Google's Cloud IoT Core similarly seeks to apply IAM roles to device registries in order to control access to devices and data.[28]

These private services have incentives better aligned with secure and productive use of IoT devices than those of governments because they benefit when they maximize value to their customers, which entails balancing costs and benefits. Companies like Amazon, Microsoft and Google have a strong incentive to ensure security, if only to protect their own networks that interface with their customers' IoT devices. They are incentivized to register as many devices as possible since doing so increases the number of devices in their ecosystem and, therefore, increases their revenue. All the while, however, they must maintain a secure system to protect their reputation and future revenue streams. While it is possible that firms could connect many more devices if they had looser security procedures for their registries, doing so could increase their vulnerability to attacks. This would not only cause direct harm to the company but to its reputation. After all, few will want to use a network known for glaring vulnerabilities. Unlike governments, too lax security standards by a private firm are directly linked to that firm's profit. Put simply, private firms will reap losses if they cannot reach enough customers or if they fail to secure the devices of their existing ones. Conversely, they will reap profits if they are able to gain customers and secure their devices well. Thus, market incentives will tend to produce a closer-to-optimal mix of security, accessibility and easy to use.

26. "Overview of the Azure IoT Hub service," Microsoft Azure, Sept. 14, 2017. https://goo.gl/ID1QcP.

27. See, e.g., "How the AWS IoT Platform Works," Amazon Web Services, 2017. https://goo.gl/VOjTzc; "Create and Register an AWS IoT Device Certificate," Amazon Web Services, 2017. https://goo.gl/8HtfkD; and "AWS IAM FAQs," Amazon Web Services, 2017. https://goo.gl/5MNgQt.

28. "Cloud IoT Core: A fully managed service to easily and securely connect, manage, and ingest data from globally dispersed devices," Google Cloud Platform, 2017. https://goo.gl/eCh2nP.

Private registries also combat free riders — those who might not secure their own devices, instead relying on connections with devices that have already been secured. Registries create an ecosystem of devices from which those who do not meet the requirements are excluded. Security, thus, becomes a club good, rather than a public good, and can be provided by the market.[29]

Governments and other bodies need not be completely divorced from private registration schemes. They can participate in and contribute to the process of standards development, and they have done so productively. For example, the U.S. Federal Communications Commission has worked with internet service providers on a framework of best practices to address the scourge of botnets.[30] The framework, published by the National Institute of Standards and Technology (NIST),[31] is positively viewed around the world and can serve as a model for others seeking to build registration systems.[32] Another set of guidance comes from collaboration by industry players through the Institute of Electrical and Electronics Engineers (IEEE) which publishes best practices for IoT security.[33] Group standards such as these help facilitate wide adoption of interoperable rules, which will lead to greater productivity and security for the whole IoT ecosystem.

Cyber insurance

Another option for private IoT cybersecurity is cyber insurance. While not a panacea, insurance creates an incentive structure that can be used within a larger cybersecurity strategy to improve security before attacks occur.

Since even the most sophisticated security is not absolute, the goal of cyber insurance is to limit exposure to cyber risks and to ensure resiliency in the face of security failure. Using insurance to guard against the consequences of breaches before they happen is more cost effective than reacting after the fact because it frees up capital for other business purposes that would otherwise be held indefinitely in reserve in contemplation of a possible incident.

The security benefits of cyber insurance begin with the underwriting process, which serves as a mechanism of private assessment of a potential client's cyber-risk profile. Once written and effective, the insurance policy requires ongoing adherence to the policy's terms, which often include security measures the insured must follow in order to maintain coverage. In so doing, the insurer provides ongoing compliance oversight. Annual renewal procedures provide a recurrent opportunity for both insurer and insured to reassess the risk profile and preparedness.

The cyber insurance system should, however, not include a government backstop. Backstops create a moral hazard[34] that enable firms to rely upon the government — and ultimately taxpayers — to step in and bail out companies rather than securing and funding their own risks. These perverse incentives also weaken the private insurance market for entities that do want to purchase insurance on their own.

The negative effects of government backstops on insurance markets are evident in the analogous market for terrorism insurance. It is conceptually possible that a thoughtfully and meaningfully circumscribed government insurance entity could be used to encourage the cultivation of private risk transfer, rather than the implicit guarantee of U.S. taxpayers. However, this has not been the case with the Terrorism Risk Insurance Act ("TRIA"),[35] which is often cited as a model for a cybersecurity insurance backstop. For one, the renewal of the terrorism risk insurance program ("TRIP")[36] is contingent upon the need for the program to stabilize the market for an entirely different type of insurance. Thus, if TRIP expires as it should, when the market for terrorism insurance has stabilized, the cyber-insurance provisions would be put at risk. Conversely, in the event of rapid growth in cyber insurance, a scenario could unfold in which a cyber backstop outlives its usefulness and actually hampers the growth of that market through moral hazard.

The latter scenario is likely to occur because the market for private cyber insurance is young but growing quickly.[37] Government actions that hamper its development, like the creation of a backstop, will therefore be harmful to security and resiliency to cyber-attacks. In view of this, governments should instead seek to facilitate a private market in cyber insurance rather than to establish backstops and regulation.

29. See, e.g., James M. Buchanan, "An Economic Theory of Clubs," *Economica* 32:125 (February 1965), 1-14. https://goo.gl/4Rdj5K.

30. Working Group Seven, "Final Report: U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs)," Communications Security, Reliability, and Interoperability Council, March 2012. https://goo.gl/kvwQrw.

31. The NIST provides voluntary guidance and best practices for managing cyber risk.

32. "Framework for Improving Critical Infrastructure Cybersecurity," *National Institute of Standards and Technology*, Jan. 10, 2017. https://goo.gl/x7vcoj.

33. "Internet of Things Security Best Practices," Institute of Electrical and Electronics Engineers, 2017. https://goo.gl/Gk5QoV.

34. A moral hazard exists when an insured entity increases their exposure to risk precisely because their insurance decreases the potential consequences to which they may directly be subjected.

35. "Terrorism Risk Insurance Program Act of 2002," H.R. 3210, 107th Congress. https://goo.gl/AUdU3C.

36. "Terrorism Risk Insurance Program," U.S. Dept. of the Treasury, May 3, 2017. https://goo.gl/MxW5mH.

37. "Cyber the fastest growing peril, will require reinsurance & ILS capital" *Artemis*, Aug. 25, 2016. https://goo.gl/yjnNaZ.

Ex-post contractual liability

Contractual liability arrangements are those in which the distribution of risk and liability is agreed upon beforehand by the buyer and seller.[38] The contract of sale defines who is liable for what potential damages. Ideally, these contracts would solve all problems of ex-post liability, however, in practice, complications arise. When a large firm is selling many of the same product to thousands of customers, contracts can become a mere formality in which the buyer has no say. This disparate bargaining power means that buyers may not even read the "fine print" and, therefore, not account for the risk to which their purchase exposes them. A privately developed and widely adopted code for contracts, akin to the Uniform Commercial Code (UCC) for business law[39] could also address this imbalance in bargaining power. When these contracts are negotiable, or at least transparent, they are preferable to regulation because they allow the buyer and seller to judge the benefits and costs for themselves and voluntarily incur the risks with which they are comfortable.

HYBRID APPROACHES

There are also options between prescriptive government regulation of IoT security and the above market-driven measures and such proposals have their own pros and cons that are worth considering.

Ex-post remedies: tort law

Legal systems must assign liability somehow, as setting the "rules of the game" is necessary for private approaches to cybersecurity to take hold. But governments should take care not to create arrangements that impose costs that could reduce net innovation and security.

Governments may seek to facilitate de facto regulation through the setting of liability rules using national and subnational political and legal systems.[40] There are a wide variety of approaches governments can take to civil liability and rules often vary between jurisdictions. For example, in the United States, available remedies can differ widely from state to state. Some approaches, like a negligence standard, involve an inquiry into the reasonability of the behavior in question. Others, like strict product liability,[41] are more onerous. In the context of the IoT, under a strict liability system, a device manufacturer may be found responsible for damage from cyber incidents regardless of the behavior of other actors. Such strict liability discourages innovation without improving security because device-makers can face costly liability claims for actions that were beyond their control or ones that they took reasonable precautions to prevent.

Further, a recent European Commission report proposes a risk-generating approach in which liability is assigned to "actors generating a major risk for others and benefiting from the relevant device, product or service," and a risk-management approach in which liability is assigned to "the market actor which is best placed to minimize or avoid the realisation of the risk or to amortize the costs in relation to those risks."[42] In short, if the manufacturer can cheaply mitigate risk, it is liable if it does not do so, but if other actors in the supply chain are better positioned to mitigate risk, liability lies with them. In one sense, this arrangement may be preferable to strict product liability because it seeks to evaluate the particulars of various circumstances and to find the lowest-cost way of dealing with risk. However, it is difficult to practically enact such a method in the context of the IoT where causal links between security measures, consumer behavior and damage is often difficult or impossible to establish.[43]

Ex-post liability regimes also must contend with lost benefits that may result from their implementation. For example, creating too onerous liability standards can stifle the development and deployment of new technology and can also lead to innovation arbitrage in which the best entrepreneurs leave the country and do business elsewhere.[44] What's more, lopsided liability rules can also distort the market by making manufacturers less willing to open their systems to third-party applications and/or modifications that could benefit consumers. Ultimately, although reducing access may increase security, it does so at the cost of core benefits of connected devices. For these reasons, while the legislative and judicial systems must clearly assign liability, they should conceive of it as a way of maximizing net benefits rather than simply maximizing security at any and all cost.

38. "Commission Staff Working Document on the free flow of data and emerging issues of the European data economy Accompanying the document Communication: Building a European data economy," *European Commission*, Jan. 10, 2017, 40. https://goo.gl/z8wCJj.

39. The UCC is a privately developed set of rules "governing commercial transactions that has been adopted in some form by every state as well as by the District of Columbia." See, e.g., "Uniform Commercial Code," Legal Information Institute, 2017. https://goo.gl/98S5P9.

40. "Commission Staff Working Document on the free flow of data and emerging issues of the European data economy—Accompanying the document Communication: Building a European data economy," European Commission, Jan. 10, 2017, 40. https://goo.gl/z8wCJj.

41. "Products Liability," Legal Information Institute, 2017. https://goo.gl/uUAbEz. These regimes are also common in Europe. See Jamie Cartwright, "Product liability and the internet of things," Charles Russell Speechlys, Apr. 21, 2017. https://goo.gl/ixDfPY.

42. "Commission Staff Working Document," 45. https://goo.gl/z8wCJj.

43. See, e.g., Cartwright. https://goo.gl/ixDfPY.

44. Adam Thierer, "Innovation Arbitrage, Technological Civil Disobedience & Spontaneous Deregulation," *Technology Liberation Front*, December 5, 2016. https://goo.gl/XAadSx.

Recent legislative proposals

Concrete policies aimed at enhancing IoT security have been proposed by several U.S. legislators. The IoT Cybersecurity Improvement (IoTCI) Act[45] and the Cybershield Act[46] are two such examples.

The IoTCI Act seeks to use the government's power as a larger purchaser of connected devices to push responsible security measures. Accordingly, it would require devices procured in federal government contracts not to have any known vulnerabilities that have been highlighted by the NIST, to be able to accept updates, to use industry-standard communications, connection and encryption protocols, and not to have fixed credentials for remote access. This bill could be a positive step toward improving government security, as it could provide a model for private producers of security and insurance products and also attract early customers that will bolster the market for such products.

The Cybershield Act would use existing standards, like the NIST framework, to establish a system for rating device security that is akin to the way the EnergyStar program certifies energy efficiency.[47] Devices that meet these benchmarks could then mark their products with the certification, which would signal to customers that it has industry-standard security. Voluntary standards like this one are an improvement compared to prescriptive, technology-specific mandates. There are, however, some potential pitfalls to relying too heavily on the rating process as a primary indicator of security.

First, IoT devices comprise a broad, heterogeneous category and adequate security can have different meanings for different devices. Second, security is not necessarily an objective or binary quality. Different aspects of a device's security may be more or less important depending on the particular use. Certifications and ratings also risk giving users a false sense of security, as they may think a device that was highly rated when they bought it will always be secure. A binary rating, or even a system of five stars as the bill proposes, may also incentivize manufacturers to target the certification, perhaps doing only the bare minimum, rather than seeking to incorporate or innovate new security measures. For these reasons, insofar as government becomes involved in the rating and certification process, a model that incorporates grades along various dimensions of security would provide more useful information to consumers. Even so, the competition promoted by the existence of many, competing private standards and rating systems for security rather than a single, government operated one may also contribute both to overall quality and to the expeditious updating that is necessary to keep pace with evolving threats.

45. Introduced by Sens. Mark Warner (D-Va.), Ron Wyden (D-Ore.), Cory Gardner (R-Colo.) and Steve Daines, (R-Mont.).

46. Introduced by Sen. Edward Markey (D-Mass.)

47. See, e.g., "Energy Star Overview," Energy Star of the U.S. Environmental Protection Agency, 2017. https://goo.gl/Dk36Tb.

Disclosure mandates

An additional or alternative measure in the middle ground between heavy-handed regulation and private measures is to require companies to inform affected parties when they are breached in order to identify harmed parties and allow the legal system to assign liability. The U.S. Securities and Exchange Commission requires a certain degree of disclosure for public companies when risks or incidents are relevant to shareholders.[48] Europe's General Data Protection Regulation (GDPR) also includes reporting requirements for incidents that could cause damage to Europeans' rights.[49] The GDPR rules are notable for their expansive scope, as they apply to non-EU companies that process the data of EU citizens, and assign hefty penalties of up to 4 percent of a firm's annual revenue.[50]

Disclosure mandates could be a reasonable regulatory middle ground, but they also come with some trade-offs and potentially adverse unintended consequences. First, by revealing that it has been the victim of an attack, a company identifies itself and others that may use similar security measures as easy targets. Second, if a firm is forced to disclose security vulnerabilities or failures when they are discovered, then it has an incentive simply not to discover them. These side effects of disclosure mandates may result in diminished security. Accordingly, enforceable anti-fraud measures must accompany disclosure mandates for them to have their intended effect.

NTIA's multistakeholder process

Another governmental approach is the National Telecommunications and Information Administration's (NTIA) public-private process,[51] which was convened to work on IoT security in a transparent, multistakeholder forum.[52] The NTIA defines the goal of the process as "to develop a broad, shared definition or set of definitions around security upgradability for consumer IoT, as well as strategies for communicating the security features of IoT devices to consumers."[53]

48. Jay Clayton, "Statement on Cyber Security," U.S. Securities and Exchange Commission, Sept. 20, 2017. https://goo.gl/qrNsTn.

49. "GDPR Key Changes," EU General Data Protection Regulation, 2017. https://goo.gl/HhqT4Y.

50. Ibid.

51. Angela Simpson, "Increasing the Potential of IoT through Security and Transparency," National Telecommunications and Information Administration, Aug. 2, 2016. https://goo.gl/5JIq1Z.

52. National Telecommunications and Information Administration, "Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching," U.S. Dept. of Commerce, Oct. 11, 2017. https://goo.gl/veoxPS.

53. Ibid.

The NTIA process is designed to create methods to avoid and detect vulnerabilities in IoT devices for the prevention of security incidents. The multistakeholder nature of the IoT security process differentiates it from other government-led ones. This is because although the NTIA was convened by the government, it did so at the request of the stakeholders. Thus, it is being shaped by various groups, rather than the government alone. It is also an open and inclusive process with no need to seek permission or get accredited in order to attend the meetings and participate in its working groups. This distinguishes the process from certain international ones, such as the International Telecommunication Union (ITU)-led process on cybersecurity, which is a less-open system.[54]

The effectiveness of NTIA's multistakeholder process is still unknown. While the members of the working groups are prominent industry players, governments and NGOs,[55] the outcomes have no binding effects. But industry's participation is a clear signal that the market has recognized IoT security as an important field and that it is working toward solutions.[56]

CONCLUSION

IoT governance is gradually taking shape through individual actions and the interaction of networks, governments and markets. Currently, it is not clear how the landscape will evolve or which actors will gain prominence in the governance of IoT security. There are, however, significant reasons to be skeptical of efforts to impose a restrictive regulatory regime on the rapidly-evolving IoT ecosystem. There is already a diverse landscape of IoT security measures that includes many market mechanisms that can succeed where government action—with its structural limitations—would not. Recognizing that it would be ill-advised to impose a one-size-fits-all regulatory regime, policymakers should not only allow but should also encourage these mechanisms and should simultaneously allow private and multistakeholder standards to develop.[57]

This is not to say that government cannot take any productive actions in the near term that affect the broader landscape. For instance, it would be entirely appropriate to clarify existing rules to remove barriers to vulnerability research.[58] But before any additional intervention is undertaken, we should allow security standards to develop spontaneously rather than imposing prescriptive regulation. Doing so will maximize innovative use cases for IoT technology, while allowing security practices to be flexible and responsive. While this approach may mean tolerating some near-term failures, in the long run it is the most likely to maximize the scope of the technology's benefits.

ABOUT THE AUTHORS

Farzaneh Badiei is a research associate at the Georgia Institute of Technology, School of Public Policy, and the Executive Director of internet Governance Project (IGP).

For the past six years, Farzaneh has been a part of internet governance research and professional community where she has carried out research projects at the Humboldt Institute for Internet and Society (HIIG) and the Syracuse School of Information Studies. She received her Ph.D. from the University of Hamburg, Institute of Law and Economics. Her dissertation focused on online private justice systems, institutional design and online market intermediaries. Farzaneh also worked at the United Nations Internet Governance Forum Secretariat. Currently, she is the chair of Noncommercial Stakeholdergroup at ICANN, which focuses on noncommercial rights in domain names.

Farzaneh's current research interests revolve around online private justice systems, internet governance and accountability of internet governance institutions, internet and jurisdiction, online intermediaries and dispute resolution, as well as cybersecurity and digital trade.

Ian Adams is associate vice president of state affairs with the R Street Institute, responsible for coordinating R Street's outreach and engagement at the state and local level. He also is involved in the Institute's insurance research, matters related to next-generation transportation and is a frequent commentator on the disruptive impact of burgeoning technologies on law and regulation.

Ian is a graduate of Seattle University, with bachelor's degrees in history and philosophy. He also received his law degree from the University of Oregon, and is a member of the California and Illinois bars.

Joe Kane is a technology policy associate with the R Street Institute, where he works primarily on telecommunications, antitrust and intellectual property issues to push for regulatory frameworks that will promote long term innovation.

Joe has a bachelor's degree in political science from Grove City College and a master's degree in economics from George Mason University.

54. See e.g. "Study Group 17: Security," International Telecommunication Union, 2017. https://goo.gl/PuUvyp.

55. A partial list of participants in the various working groups includes Consumer Technology Association, Device Authority, Ice Miller LLP, National Telecommunications and Information Administration, The Niskanen Center, Online Trust Alliance, OutSecure Inc., SAP, The Providence Group, Trusource Labs, Venable LLP, and Microsoft. For a complete list of companies and individuals who filed public comments see National Telecommunications and Information Administration, "Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things," U.S. Dept. of Commerce, June 6, 2016. https://goo.gl/NF7TRh.

56. See e.g., "Communicating IoT Device Security Update Capability to Improve Transparency for Consumers," NTIA Communicating Upgradability and Improving Transparency Working Group, July 18, 2017. https://goo.gl/oBcf9N; "Catalog of Existing IoT Security Standards" NTIA Existing Standards, Tools and Initiatives Working Group, Sept. 12, 2017. https://goo.gl/XGRc9q; and "Internet of Things (IoT) Security Upgradability and Patching," NTIA: Incentives and Barriers to Adoption Working Group, Sept. 12, 2017. https://goo.gl/7pKn94.

57. For example, it is obvious that a medical device likely does not have the same security needs as a connected toaster.

58. Alexander Gamero-Garrido, Stefan Savage, et al., "Quantifying the Pressure of Legal Risks on Third-party Vulnerability Research," ACM SIGSAC Conference on Computer and Communications Security, September 2017. https://goo.gl/js9934.