Silicon Flatirons

KNOW WHAT'S NEXT.

Rountable Series on Entreprenuership, Innovation, and Public Policy

Flatirons Report

Future of the Internet of Things in Mission Critical Applications

Jeffrey Westling

November 2016

Silicon Flatirons is a center for innovation at the University of Colorado Boulder to serve students, entrepreneurs, policymakers, and professionals at the intersection of law, policy, and technology.

Flatirons Reports capture thoughtful analysis of various issues in law, technology, and entrepreneurship. These reports are derived from research conducted by Silicon Flatirons faculty, fellows, and research assistants, as well as from thoughtful conference and roundtable conversations hosted by Silicon Flatirons that include academia, policymakers, legal professionals, entrepreneurs, and students sharing their knowledge and best practices on specific topics.

Flatirons Reports are published at siliconflatirons.org.

Executive Summary

The "Internet of Things" (IoT) promises many benefits to improve efficiency and quality of life for consumers and society as a whole. As IoT devices develop and proliferate, new vulnerabilities open up to bad actors, and the wide range of devices present heightened risk that some will interfere with others, risking potentially catastrophic failures. The Silicon Flatirons Center for Law, Technology, and Entrepreneurship held a roundtable in Washington, D.C. on June 22, 2016 to discuss the promise of IoT technology and what role, if any, the government can play in the oversight of security and spectrum interference concerns. This report captures the insights from that discussion and supplements them with relevant research.

For those developing IoT technology, addressing security concerns is a core challenge. For innovators and regulators, security is also a timing challenge, as they must determine how secure these devices must be before going to market. Where a product is already in the market, another challenge is to address security vulnerabilities to prevent or limit harm once a vulnerability is discovered.

Many IoT devices use wireless spectrum to send and receive data, so manufacturers also need to ensure that their devices operate reliably, even when potential jammers and spoofers seek to do harm. Moreover, because the spectrum used is frequently unlicensed, it is important to ask whether and how mission-critical IoT should operate without interference protection. In short, a key part of the challenge comes down to ensuring that manufacturers understand the risks of interference and share this information with end users so that they can prevent, mitigate, or manage potential harms.

As IoT devices become more popular, policymakers are considering the role, if any, the federal government should play in this area. Because IoT technology is at a nascent stage, federal agencies need to be working closely with industry to ensure that regulations are flexible and do not limit innovation, thereby preventing deployment of these technologies. Two basic questions for policymakers emerge: how can they help consumers understand the relevant risks and encourage information sharing to identify and resolve issues as they arise.

Table of Contents

Introduction

The world is becoming increasingly interconnected. Today, devices, systems, and people are connecting to the internet or to internet technology (via private networks), in ever greater numbers, making devices "smarter." This connectivity powers services that are more personalized, more efficient, more intelligent and thus more valuable to consumers. By 2020, 50 billion "smart" devices will be interconnected.[1] In the same timeframe, global spending on these devices and associated services is expected to grow by $3 trillion.[2] Collectively, this family of rapidly expanding technologies is known as the Internet of Things (or IoT, for short).

IoT devices promise benefits that can significantly improve the quality of life for consumers.[3] Consumer-facing products such as insulin pumps and blood-pressure cuffs enable people to record, track, and monitor their own vital signs.[4] Homeowners can use smart meters

[1] FTC STAFF, INTERNET OF THINGS, PRIVACY AND SECURITY IN A CONNECTED WORLD 1 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf. ("FTC Staff Report").

[2] *Id.*

[3] DANIEL CASTRO & JOSHUA NEW, 10 POLICY PRINCIPLES FOR UNLOCKING THE POTENTIAL OF THE INTERNET OF THINGS 1-3 (Center for Data Innovation, 2014), http://www2.datainnovation.org/2014-iot-policy-principles.pdf.

[4] Alex Scroxton, *Startup Insulin Angel Uses Internet of Things in Healthcare by 2020*, FORBES (Apr. 09, 2015), http://www.computerweekly.com/news/4500244001/Startup-Insulin-Angel-uses-internet-of-things-to-help-diabetics.

to analyze energy use and detect problems with their power systems.[5] Connected cars may be able to reduce automobile deaths to a fraction of the current numbers.[6] On a grander level, large-scale aggregation of data can lead to significant innovations.[7]

The future of IoT remains uncertain and even defining IoT is a challenge. To begin with, the contours of IoT remains uncertain. The IoT is not a network or even a network of networks. As Ellen Goodman, a Professor at Rutgers Law School, explained, there is a heterogeneity of architectures and standards used for IoT products and connectivity. What is considered part of the IoT ranges widely in terms of data sensitivity, security, public or private deployment, and the data that is being collected and acted upon.[8] As IoT technology proliferates, more of these devices and systems are connecting with one another and utilizing these connections, allowing them to share data and information.[9] With the increased proliferation of this technology, interference and security issues come to the forefront.[10]

Many "mission-critical" devices and supporting infrastructure—from those used in health care facilities to those used in electricity networks—now utilize IoT systems to facilitate essential operations.[11] Such mission-critical devices are ones where a failure would create a serious risk of loss of life, injury, or a considerable economic loss. These devices face potential threats to their operation that should be addressed and mitigated.[12]

To address the questions surrounding how policymakers should approach IoT technology, the Silicon Flatirons Center hosted a roundtable discussion on June 22, 2016 in

---

[5] BUILD GREENER ENERGY SOLUTIONS WITH SMART METER TECHNOLOGY, SIERRA WIRELESS (last visited Oct. 30, 2016), https://www.sierrawireless.com/applications/energy-and-industrial/smart-metering/.

[6] *See* Michael Bongartz et al., *IT Security for the Connected Car: Intelligent Mobility by IBM and G&D*, Giesecke & Devrient 3 (Mar. 2016), https://www.gi-de.com/gd_media/media/documents/brochures/mobile_security_2/IT_Security_for_the_Connected_Car.pdf.

[7] *See* James Manyika et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity,* MCKINSEY GLOBAL INSTITUTE (May 2011), http://www.mckinsey.com/business-functions/business-technology/our-insights/big-data-the-next-frontier-for-innovation.

[8] In some cases, service providers will offer supported IoT services, where they install and manage a service using IoT devices. In such cases, the service provider manages the device and any relevant security issues. As those cases are distinct and different from ones where consumers buy and install devices themselves, we discuss only the latter set of issues in this report, leaving any questions around IoT services to one side.

[9] Notice, Request for Public Comment, The Benefits, Challenges, and Potential Roles for Government in Fostering the Advancement of the Internet of Things, 81 Fed. Reg. 19956 (April 06, 2016), https://www.federalregister.gov/articles/2016/04/06/2016-07892/the-benefits-challenges-and-potential-roles-for-the-government-in-fostering-the-advancement-of-the.

[10] THE PRESIDENT'S NATIONAL SECURITY ADVISORY COMMITTEE, NSTAC REPORT TO THE PRESIDENT ON THE INTERNET OF THINGS ES-1 (Nov. 14, 2014), https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf; *see also* Drew Fitzgerald, Hackers Infect Army of Cameras, DVRs for Massive Internet Attacks, The Wall Street Journal (Sept. 30, 2016), http://www.wsj.com/articles/hackers-infect-army-of-cameras-dvrs-for-massive-internet-attacks-1475179428.

[11] *See, e.g,* TJ McCue, *$ 117 Billion Market for Internet of Things in Healthcare by 2020,* FORBES (April 22, 2015), http://www.forbes.com/sites/tjmccue/2015/04/22/117-billion-market-for-internet-of-things-in-healthcare-by-2020/#13a5513f2471.

[12] *See generally* Daniel Halperin et al., *Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses*, IEEE SYMPOSIUM ON SECURITY AND PRIVACY (2008).

Washington, D.C. with experts from a wide array of backgrounds to discuss how government should oversee the use of mission-critical IoT devices. The participants in the roundtable discussion are listed in Appendix A. The roundtable followed Chatam House Rules, meaning no participant was quoted without his or her permission. The goal of the discussion was for participants to engage in an open-minded effort to explore potential problems, concerns, and solutions. This report captures the essence of the discussion and supplements it with relevant research, recommending that government agencies explore ways (1) to provide simple and transparent messages to consumers; (2) incentivize reporting; and (3) enable information sharing among IoT vendors.

This report proceeds in four parts. After this Introduction, Part I explains the security concerns associated with mission-critical IoT devices and provides some suggestions for addressing these issues. Part II discusses the need for reliable operations and potential spectrum interference concerns associated with IoT devices using wireless spectrum. Finally, Part III examines the role that regulators could play in addressing these issues.

I. Security Challenges Associated with Mission-critical IoT Devices

With the increased proliferation of mission-critical IoT technology, security vulnerabilities present a serious concern.[13] As more developers design products that connect with one another, including mission-critical devices and systems, the risks associated with these devices increases dramatically.[14] Roundtable participants noted that these security risks are increasing due to a variety of factors. First, the number of devices in the marketplace is rapidly increasing.[15] With more devices, hackers have more targets and attack vectors, increasing the likelihood of security breaches.[16]

Second, connected devices are occasionally shipped with out-of-date software that could contain known vulnerabilities.[17] In some cases, these devices may not allow for real-time updates (or "patching"), or alternatively, the software patches may not be automatically downloadable or secure.[18] Likewise, customers may not adequately manage the security updates and even if companies develop fixes for the devices, many users will never upgrade or replace their equipment or software despite the known vulnerabilities. For example, Jason Livingood, Vice President, Technology Policy & Standards at Comcast, explained that some brand name home

---

[13] GARY MATUSZAK ET. AL., SECURITY AND THE IOT ECOSYSTEM (KPMG International, 2015), https://www.kpmg.com/CO/es/IssuesAndInsights/ArticlesPublications/Documents/Security%20and%20the%20IoT%20Ecosystem.pdf.

[14] For example, an IoT botnet was recently used to to send a massive number of requests to DYN's DNS service, causing outages at services across the internet. Sean Gallagher, *Double-dip Internet-of-Things Botnet Attack Felt Across the Internet*, ARSTECHNICA (Oct. 21, 2016), http://arstechnica.com/security/2016/10/double-dip-internet-of-things-botnet-attack-felt-across-the-internet/.

[15] FTC Staff Report, *supra* note 1, at 1.

[16] Attack vectors are avenues through which an attacker can gain access to data. Jane Kim & David Zakson, *Health Information and Data Security Safeguards*, 32 J. Marshall J. Info. Tech. & Privacy L. 133, 145 (2016).

[17] Kate Cox, *Your Home Router Was Probably Out-Of-Date and Insecure before You Even Plugged It In*, CONSUMERIST (January 19, 2016), https://consumerist.com/2016/01/19/your-home-router-was-probably-out-of-date-and-insecure-before-you-even-plugged-it-in/.

[18] *Id.*

routers have a well-known DNS bug that will start sending thousands of queries per second to look like a distributed denial of service (DDoS) attack, but many customers never actually took steps to fix the bug. These problems grow more pronounced when corners are cut in limiting device capacity to add more battery life, lower cost, or some other reason. In short, simply identifying and developing fixes for security vulnerabilities does not necessarily mean that the devices or systems will be secure.

Third, device manufacturers do not necessarily have expertise in security matters. As Jason Livingood pointed out, a manufacturer may ship devices or technology with problems such as weak authentication or other basic security issues in part because they do not necessarily know the harms associated with these practices or have not internalized the risks (often because there is no incentive for them to do so). For example, manufacturers that use weak authentication allow bad actors to search for other devices connected to the network such as webcams and, using factory default passwords to break into the device, gain access to the user's camera and take advantage of this vulnerability.[19]

Finally, participants noted that even if manufacturers of mission-critical devices take security concerns seriously and ensure that their devices are well protected, many consumers may not necessarily use the devices as they are intended to be used. If a device is used for a mission-critical purpose (for example, in managing a transportation system), then it essentially becomes mission-critical. But the manufacturer of a device might not take the same security precautions they would if designing a mission-critical application or device. Likewise, the manufacturer could simply fail to anticipate the mission-critical application for the device.

The above scenarios all involve situations where potential harms can arise. For example, participants discussed the ability for hackers to enable unauthorized access to a device and misuse the personal information stored within it.[20] Target learned this lesson the hard way when a breach of its air conditioning system enabled a hacker to obtain 40 million credit card numbers.[21] Similarly, even non-mission-critical devices such as Wi-Fi cameras can act as a backdoor to breach a company's network or other vital infrastructure.[22] Hackers can attack devices, such as insulin pumps, that ultimately create significant risks to personal safety.[23] Most recently, a number of devices like Wi-Fi routers and IP video cameras were used to send a massive number

[19] John Leyden, *Webcam Hacker Pervs in Mass Home Invasion*, THE REGISTER (Nov. 20, 2014), http://www.theregister.co.uk/2014/11/20/insecure_webcam_peeping_tom_threat/.

[20] *See generally* Gary Matuszak et.al. *supra* note 13.

[21] Michael Riley, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG (Mar. 17, 2014), http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data; *IoT Devices Easily Hacked to be Backdoors: Experiment*, SECUIRTYWEEK (Jan. 13, 2016), http://www.securityweek.com/iot-devices-easily-hacked-be-backdoors-experiment.

[22] *Id.*

[23] Eric Basu, *Hacking Insulin Pumps and Other Medical Devices From Black Hat*, FORBES (Aug. 3, 2013), http://www.forbes.com/sites/ericbasu/2013/08/03/hacking-insulin-pumps-and-other-medical-devices-reality-not-fiction/#3ca2eab34327.

of requests to DYN's DNS service.[24] These attacks resulted in outages at services across the internet.[25]

A. Discovering Security Vulnerabilities

Manufacturers cannot develop patches for security vulnerabilities if they do not know that the vulnerabilities exist. Thus, manufacturers must first find and identify a security vulnerability before any remedial action can take place.

The first way companies can identify issues with their products is to share information with one another about known security vulnerabilities and mitigation strategies to address them.[26] However, this may not always occur or occur in time to address the harm. Participants suggested that companies may conceal security concerns because of the fear that, as a result of disclosing the issue, customers will select other products.[27] Thus, some participants noted that one overarching challenge is to create an ecosystem that enables appropriate and secure sharing of threat information and also supports companies in handling the influx of new security issues as they arise.

Second, companies can incentivize third party researchers to come forward with discoveries.[28] As Blake Reid, Assistant Clinical Professor at the University of Colorado Law School, noted, many researchers do not know how their discoveries will be received by the companies. While some companies may offer programs such as "bug bounties," participants noted that others may instead send a cease and desist letter to those identifying vulnerabilities. Instead of preventing hackers from accessing their security systems, these companies should look to the myriad of success stories in facilitating researchers to discover and disclose security issues.[29]

White hat hackers (hackers who search for vulnerabilities and report their findings), for example, approach new products with the same mindset as the actual bad actors, and can therefore reach deeper into the states of web application than traditional security scanners.[30] Perhaps more importantly, a large and diverse group of potential white hat hackers exist and can provide different perspectives on the same problems.[31] To facilitate these investigations,

---

[24] Sean Gallagher, *Double-dip Internet-of-Things Botnet Attack Felt Across the Internet*, ARSTECHNICA (Oct. 21, 2016), http://arstechnica.com/security/2016/10/double-dip-internet-of-things-botnet-attack-felt-across-the-internet/.

[25] *Id.*

[26] Bruce Schneier, *Disclosing vs. Hoarding Vulnerabilities*, SCHNEIER ON SECURITY (May 22, 2014), https://www.schneier.com/blog/archives/2014/05/disclosing_vs_h.html.

[27] *See, e.g.*, DAVID CLARK ET AL., AT THE NEXUS OF CYBERSECURITY AND PUBLIC POLICY: SOMBE BASIC CONCEPTS AND ISSUES 101 (The National Academies Press, 2014) ("NRC Report").

[28] Mingyi Zhao et al., *An Empirical Study of Web Vulnerability Discovery Ecosystems*, CSS '15 (2015), https://s2.ist.psu.edu/paper/An-Empirical-Study-of-Web-Vulnerability-Discovery-Ecosystems.pdf.

[29] Gregg Keizer, *Microsoft Trumpets Early Success in IE11 Bug Bounty*, COMPUTERWORLD (July 3, 2013), http://www.computerworld.com/article/2483541/malware-vulnerabilities/microsoft-trumpets-early-success-in-ie11-bug-bounty.html.

[30] Mingyi Zhao et al., *supra* note 27, at 1.

[31] *Id.*

organizations can offer rewards for hackers who come forward and disclose vulnerabilities.[32] In fact, such ecosystems have been growing rapidly and can play a helpful role in identifying security issues going forward.[33] In the open source world, this ethos is captured by the maxim that "with enough eyeballs, all bugs are shallow."[34]

B. The Tradeoffs Between Security and Functionality

Ultimately, identifying and fixing security vulnerabilities is useless if the device itself cannot support these fixes. In an effort to keep costs down, producers may rely on low power processors that are not powerful enough to encrypt information. Likewise, designers of battery powered devices may choose to avoid using encryption to increase the life of the device. Another major concern raised in the discussion is that many of these devices and systems may not have two-way capabilities that would allow for security upgrades once the device is already in the field.

Whether they realize it or not, consumers may be choosing to forego security for other qualities and functions that they want in a device (namely, lower cost). Regulations raising minimum security requirements for devices would raise their costs and limit the rate at which the device is adopted in the marketplace. Likewise, including more processing power to allow for increases in security may also come at the expense of limiting speed and portability as well as increasing the power consumption of these devices. All of these factors will affect the ultimate success and deployment of the devices in the marketplace. In short, participants noted that a core challenge is how to decide and who should decide whether a device is secure enough.

Some participants argued that, in appropriate circumstances, users should decide what levels of security they require and what functionalities the devices should include. To facilitate intelligent choices by consumers, it might be important to develop an independent and trusted certification process to evaluate and indicate the level of product security. On this point, Len Cali, Senior Vice President, Global Public of Policy at AT&T suggested that an industry product certification process could potentially inform consumers in meaningful and transparent ways of the level of security they are receiving with certain price points, form factors, etc., and the trade-offs associated with such decisions.

A certification process for IoT devices may well emerge, but participants raised a series of important questions regarding how such a process would work. Who will be the party certifying the devices? Will the certification process make a difference if other users install their own devices? How will consumers learn to trust and use certified products appropriately? Would the certification be lost in the sea of other certifications in the marketplace (many of which consumers don't understand)?

Participants also noted that there are incentives to disregard security and functionality to get the customer on a particular network before any other competitors. This incentive for speed in product deployment follows the concept of network effects: the more consumers that a

---

[32] Meghan Neal, *Government Bounties for All: White Hat Hacking is Big Business*, VICE (July 16, 2013), http://motherboard.vice.com/blog/government-bounties-for-all-white-hat-hacking-is-big-business.

[33] *See generally* Mingyi Zhao et al., *supra* note 27.

[34] Eric Raymond, *The Cathedral and the Bazaar*, THYRSUS ENTERPRISES (1999), http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/.

company can get onto its network, the more beneficial it is to join that specific network.[35] Therefore, to get the benefits of the new connected devices, consumers may not be given a real opportunity to make the security decision for themselves.

Other participants noted that companies also have incentives to take security and functionality into consideration when designing and manufacturing devices and systems: customers expect that their devices will be reliable and secure. As Alex Reynolds, former Director of Regulatory Affairs at the Consumer Technology Association, explained, manufacturers who implement better security practices will continue to face consumer scrutiny if other manufacturers fail to implement similarly good security or act in ways that consumers do not expect; the challenge for manufacturers implementing security measures will be to differentiate the enhanced security in consumers' eyes.

C. Addressing Security

To address these issues, it can be helpful to think in terms of several dimensions. On the product dimension, a basic question is whether the security fix must be made before the device goes into the market or can be added later (say, through a software update).[36] Such updates could be either voluntary or mandated, but by automatically updating a device, a company can ensure that user devices contain the most up-to-date security protections regardless of whether the security of the device is maintained by the consumer. As noted earlier, this might depend on the type of product.

A second dimension is the time dimension. How long will a product be supported? Particpants noted that one option is to provide an expiration date on the device after which users cannot update, or to notify consumers that will not be supported after a certain period of time. In such cases, a consumer would be able to see the product end date and return it to the manufacturer to be replaced or updated. As Joseph Lorenzo Hall, Chief Technologist for the Center for Democracy & Technology, noted, kill switches could be utilized to automatically shut down a device that is out of date. As Jason Livingood pointed out, however, this creates a new attack point for hackers to target. In a similar vein to the kill switch suggestion, Hall raised the issue of whether an agency (say, the Federal Trade Commission) could oversee and manage product recalls in this space. Finally, there is the question of how to manage the likely situation of a manufacturer cutting off support for older devices.[37]

A third dimension is whether regulatory oversight occurs at the federal or state level. Whether or not federal regulators take an interest in this area, Rebecca Arbogast, Senior Vice President for Global Public Policy at Comcast, explained that state laws are likely to influence the security requirements for devices. This may develop as a "race to the top," where the most demanding state rules dictate the approach for all consumer-facing technology in the United

[35] *See generally* Michael Katz & Carl Shapiro, *Network Externalities, Competition, and Compatitibility*, 75 Am. Econ. Rev. 424 (1985).

[36] *See, e.g*, Dustin Childs, *Security Update Released to Address Recent Internet Explorer Vulnerability*, MICROSOFT (May 1, 2014), https://blogs.technet.microsoft.com/msrc/2014/05/01/security-update-released-to-address-recent-internet-explorer-vulnerability/.

[37] Gordon Kelly, *Mircrosoft Abandons Windows 8.1: Take Immediate Action or Be Cut Off Like Windows XP*, FORBES (Apr. 15, 2014), http://www.forbes.com/sites/gordonkelly/2014/04/15/microsoft-abandons-windows-8-1-take-immediate-action-or-be-cut-off-like-windows-xp/#54b6a5a142e5.

States. At the same time, state regulations may inhibit the development and deployment of IoT technology. Eric Schneider, Senior Vice President for Policy and Research at the Commonwealth Fund, noted that this concern about state laws and regulations has already affected the digital health arena, where prohibitions on telemedicine, for example, have had the effect of imposing prohibitive costs on innovation, as well as deterring product development and rollout. He noted that similar issues could emerge in the IoT space.

II. Improving Reliable Operation in Wireless Devices

Many IoT devices use wireless spectrum to send and receive data. As Silicon Flatirons Senior Fellow Dale Hatfield explained, for mission-critical devices, radio interference can be the difference between life and death. Just as with security concerns, the increased proliferation of wireless devices creates more radio transmitters and receivers, thereby increasing the chance of harmful interference. Worse, bad actors can use radio waves to maliciously cause damage to devices and systems.[38] Some simply choose to jam reception by transmitting radio noise in the area of the device. Others spoof signals, meaning that the hacker replicates a valid signal and can gain access to the device.[39]

Unfortunately, as Dale Hatfield explained, many factors are leading to an increased risk of intentional jamming and spoofing. First, much progress has been made in the field of software defined radios. These radios allow for less sophisticated users to more easily replicate valid signals.[40] For example, researchers demonstrated how software defined radios can be used to attack pacemakers and implantable cardiac defibrillators.[41] Moreover, participants explained that the devices and the components used to build them are rapidly decreasing in cost as digital technology develops. Taken together, an increasing number of potential bad actors can more easily access increasingly sophisticated IoT devices. At the same time, recent cutbacks to the Federal Communications Commission's Enforcement Bureau may exacerbate the challenge of identifying and stopping these bad actors.[42]

Second, participants discuseed that in modern networks, there is a trend towards separating the control plane of the network from the content plane of the network.[43] According to Dale Hatfield, the function of the content plane is to transfer the actual communications traffic (i.e., packets of data containing the content or payload). The function of the control plane is to control how those content or payload packets are routed. In emerging Software Defined Networks (SDNs), these two planes are separated in a way that allows traffic being transferred

---

[38] Nick Bilton, *Keeping Your Car Safe from Electronic Thieves*, THE NEW YORK TIMES (Apr. 15, 2015), http://www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html?_r=1.

[39] Travis Litman, *Cognitive Radio: Moving Toward a Workable Framework for Commercial Leasing of Public Safety Spectrum*, 4 J. on Telecomm. & High Tech. L. 249, 273-74 (2005).

[40] Patrick Devereaux, *Avoid this Wireless Alarm Hack*, SECURITY INFO WATCH (Mar. 13, 2015), http://www.securityinfowatch.com/article/12046272/avoid-this-wireless-alarm-hack.

[41] *See* Daniel Halperin et al., *supra* note 12.

[42] Michael Macagnone, *FCC Announces Enforcement Office Closures, Reforms*, Law360 (Sep. 4, 2015), http://www.law360.com/articles/699539/fcc-announces-enforcement-office-closures-reforms (In these cutbacks, the FCC did take steps to alleviate the potential shortcomings of the reduced field resources, such as complaint escalation processes and ensuring field office personal have electrical engineering backgrounds).

[43] Control Plane Attack, TELELINK (last visited Oct. 30, 2016), http://itsecurity.telelink.com/control-plane-attack/.

from node-to-node over the network to be routed or rerouted dynamically from a centralized location. For example, traffic that is very sensitive to delay (latency) but less so to bandwidth constraints can be routed one way while traffic that requires high bandwidth but is less sensitive to delay can be routed another. Making the network itself software programmable in this way can produce significant benefits in terms of network performance and resiliency. On the other hand, in comparison to more traditional decentralized network control systems, controlling how traffic is routed via multiple nodes from a centralized location may increase the extent of the damage caused if the control plane is successfully hacked. By disrupting the centralized controller and associated control plane, the flow of critical content, i.e., IoT messages, can be interrupted over a much wider area.

A third strategy discussed by participants that increases the risk of intentional jamming and spoofing is timing-based attacks. A spoofer or jammer might not necessarily have enough power to constantly interfere with a target operator, but the attacker can instead send out bursts of energy at increased power level. This is done by increasing the peak power, while lowering the average power. Furthermore, participants noted that attackers may not have the battery power for sustained broadcasting. By limiting the broadcasts to shorter bursts, the attacker can conserve battery life while still achieving the desired effect of interference that causes a critical failure in the device operation.

Furthermore, new attack vectors continue to open up and present new targets for the hacker or spoofer. For example, Jonathan Sackner-Bernstein, Former Associate Center Director for Technology and Innovation at the US Food and Drug Administration (FDA), shared an example of how the FDA would likely respond to different use cases. Specifically, for a mission-critical device such as an insulin pump, the regulatory approach would be to require tighter and stronger security assurances for a totally closed-loop control system---one that functions autonomously---than it would expect for an open-loop control system with trained user input.

Despite these concerns, there is always the question of incentives: why would bad actors choose to spoof or jam mission-critical devices? There will always be economic incentives such as using encrypting software to hold devices and data for ransom.[44] The larger concern for Hatfield is the really bad actors who are out to cause harm (e.g. terrorists or state actors). These attackers have more incentive to target mission-critical IoT technology and cause the largest amount of damage. In the face of such threats, it is therefore critical that these mission-critical devices can operate reliably, particularly with others working to disrupt them.

A. Ex Ante vs. Ex Post Enforcement

Some participants argued that one of the main issues with current enforcement of spectrum interference attacks is that enforcement of the rules generally occurs after the fact. Unfortunately, this usually means that the harm to the consumer has already occurred. While ex post, reactive enforcement can help prevent future interference issue from arising due to the deterrent effect. In the case of mission-critical devices, this can provide some deterrence value, but some participants were skeptical whether such deterrence could prevent serious harms from occurring. As Linda Kinney, Senior Advisor for Internet Policy at the National

[44] Danny Palmer, *Two-Thirds of Companies Pay Ransomware Demands: But not everyone gets their Data Back*, ZDNET (Sept. 7, 2016), http://www.zdnet.com/article/two-thirds-of-companies-pay-ransomware-demands-but-not-everyone-gets-their-data-back/.

Telecommunications and Information Administration (NTIA), explained, one formidable challenge is how to prevent the interference issue from happening in the first place.

Like most enforcement entities, the FCC's Enforcement Bureau has limited capability to prevent interference from occurring in the first place. Notably, the Enforcement Bureau only acts after an initial complaint and investigation to determine whether the alleged bad actor was the cause of harmful interference.[45] Therefore, as Blake Reid explained, these enforcement actions may not do enough to deter these actions. Consequently, other actors (including the developer and the consumer) may need to take greater care in preventing interference in mission-critical systems that rely on wireless communications.

A good example of preventing interference before the incident occurs raised in the discsussion is the partitioning of systems so that an attack on one system will not shut down the entire device or system. For example, cars use spectrum for a variety of functions and, as more mission-critical applications rely on spectrum, it is vital that the vehicle operates without interference.[46] In some cases, the connection between the IoT device and the vulnerability may be that the same network is used for multiple purposes and is not kept secure between the different uses.[47] To prevent an attack that could shut down the vehicle, as we have seen in the past, one possible solution is the partitioning of the system controlling infotainment and other, less critical features to ensure that an attack on that system would not be able to shut the entire vehicle down.[48]

Participants noted that developers of IoT devices that use wireless communications may take for granted that wireless connectivity will remain available, ignoring threats like the ones noted above. They may not have expertise related to spectrum use nor may they know all the potential hazards associated with using wireless networks. As such, while the new products may offer innovative and beneficial services, these devices could be prime targets for attackers seeking to do harm.

An important challenge will be to assure that innovators recognize these issues and plan accordingly. This could take many forms, whether it be multi-stakeholder processes, laws and regulations, or industry-led initiatives. Regardless of how any standards are set, participants argued that it will be important to address the knowledge gap between the state of best practice, the innovators developing the products, and those consumers using them.

B. Mission-Critical Devices on Unlicensed Spectrum

Spectrum is a limited resource. The FCC continually struggles to find more spectrum that can be made available. Unlicensed use, which operates under Part 15 of the Commission's

---

[45] *See* 47 C.F.R. § 0.111 (2015).

[46] *See generally* Chris Hobbs & Yi Zheng, *Protecting Software Components from Interference in an ISO 26262 System: Building Functional Safety into Complex Software Systems, Part IV*, QNX SOFTWARE SYSTEMS LIMITED (last visited Oct. 30, 2015), http://www.we-conect.com/cms/media/uploads/events/311/dokumente/QNX_-_Protecting_Software_Components_from_Interference_in_an_ISO_26262_System.pdf.

[47] Gerry Smith, *Massive Target Hack Traced Back to Phishing Email*, HUFFINGTON POST (Feb. 12, 2014), http://www.huffingtonpost.com/2014/02/12/target-hack_n_4775640.html.

[48] Hobbs & Zheng, *supra* note 46, at 4.

rules, is open to any user that wishes to use the spectrum.[49] As there is no bidding process or cost associated with acquiring the rights to use this spectrum, developers have generally used unlicensed spectrum when designing and manufacturing untested products for which buying a license would be too costly or risky.[50]

New, innovative technologies use unlicensed spectrum to different extents.[51] Significantly, unlicensed spectrum frequencies, unlike licensed frequencies, carry no interference protection for the devices that use the unlicensed spectrum.[52] Mission-critical devices using unlicensed spectrum could thus potentially face completely legal, and expected, interference. In such cases, there may be little that device operators can do to stop the interference from occurring.

In cases where the interference is willful and intentionally harmful, it is possible that the FCC will be able to address such concerns. The Communications Act bans intentional interference of licensed and authorized services, which the Commission has interpreted to include services using unlicensed devices.[53] Indeed, the FCC took action against such conduct in a case of intentional blocking by Marriott Hotels of competing Wi-Fi networks, requiring that hotel guests purchase Marriot's own Wi-Fi.[54] One participant noted, however, that as this case was settled, it is not clear how a court would interpret the rules. Therefore, there continues to be a lack of clarity about whether or when harmful interference on unlicensed devices might be permitted. For starters, not all intentional jamming and spoofing is malicious in nature, and as Michele Farquhar, Partner at Hogan Lovells US LLP, explained, jamming and spoofing has been be used as a tool to stop drones from flying over certain areas. Participants also noted that it remains to be seen whether the Computer Fraud and Abuse Act could provide a remedy in this context.[55]

The above discussion does not mean manufacturers should avoid designing and operating mission-critical devices that utilize unlicensed spectrum. Rather, it underscores the importance of equipment manufacturer awareness of the limitations of unlicensed spectrum and wireless spectrum more generally. For example, Phil Weiser, Executive Director and Founder of the Silicon Flatirons Center for Law, Technology, and Entrepreneurship at the University of Colorado, and Dale Hatfield suggested that unlicensed spectrum could be used to establish redundancies in a network so that even if one path experiences interference, other spectrum

---

[49] 47 C.F.R. §§ 15.1-15.717 (2015).

[50] Gerald R. Faulhaber, *The Digital Broadband Migration: Rewriting the Telecommunications Act: Spectrum Reform: The Question of Spectrum: Technology, Management, and Regime Change*, 4 J. on Telecomm. & High Tech. L. 123, 139 (2005).

[51] *See generally* FEDERAL COMMUNICATIONS COMMISSION SPECTRUM POLICY TASK FORCE, REPORT OF THE UNLICENSED DEVICES AND EXPERIMENTAL LICENSES WORKING GROUP (Nov. 14, 2002), http://transition.fcc.gov/sptf/files/E&UWGFinalReport.pdf.

[52] 47 C.F.R. 15.5(b) (2015).

[53] 47 U.S.C. § 333 (2012).

[54] *In the Matter of Marriot International, Inc. et al.*, Order, 14 FCC Rcd 11760 (Released October 3, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DA-14-1444A1_Rcd.pdf.

[55] 18 U.S.C. § 1030 (2012).

frequencies will be available and the device will still be able to operate.[56] This strategy could theoretically be all on unlicensed spectrum, but developers could also split up functions and use licensed spectrum for portions of the network and unlicensed spectrum for less critical functions or even backing up the licensed spectrum (as licensed spectrum isn't immune from interference, even though the licensee has legal the right to use that spectrum).

With the advent of the recent Spectrum Frontiers proceeding at the FCC and the use of some super high frequency and extremely high frequency bands for unlicensed use, it is also possible that physical boundaries can be employed to ensure that the interference doesn't occur.[57] While this approach cannot be used in all mission-critical devices and systems, as these limitations also apply to the devices and systems themselves, physical boundaries may prevent unwanted interference.

Another question is whether mission-critical devices can share the spectrum. Spectrum-sharing is an important strategy for maximizing spectrum for commercial use.[58] Spectrum can be shared in time, space, or frequency and thus, it is entirely possible that mission-critical IoT devices can share spectrum. However, sharing also opens up more potential interference to the devices.[59] In some instances, such as with autonomous vehicles, the automobile industry prefers to retain dedicated spectrum to protect future potential uses that could be vulnerable if interference occurs.

Some participants suggested that mission-critical devices should receive some interference protections while using unlicensed spectrum. This stems from the potentially life threatening consequences of not ensuring the device can operate without other operators using the same spectrum. However, others in the discussion disagreed, arguing that unlicensed spectrum is intended for innovation and the development of new products. If mission-critical devices need access to uninterrupted spectrum, then operators should either implement protections such as redundancies or purchase access to licensed spectrum to alleviate the interference concerns.

C. Information Sharing

As with security, one of the most critical components for identifying potential reliability issues is the sharing of information between private parties. Unfortunately, as Jonathan Sackner-Bernstein explained, it appears that many companies do not make potential interference instances known---as seems to be the case for other security issues---with such hesitancy potentially linked to the fear of revealing trade secret information and/or losing customer confidence. Therefore, any regulatory model would need to address these barriers with proper incentives to assure

---

[56] *See, e.g*, Milan Goldas, *Connectivity That Will Shape the Future of Mission Critical IoT Applications*, IOTNOW (July 06, 2015), http://www.iot-now.com/2015/07/06/34522-connectivity-that-will-shape-the-future-of-mission-critical-iot-applications/.

[57] *See In the matter of Use of Spectrum Bands Above 24 GHz for Mobile Radio Services et al.*, Report and Order and Further Notice of Proposed Rulemaking, GN Docket No. 14-177 ¶¶ 106-118 (released July 14, 2016), http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0728/FCC-16-89A1.pdf.

[58] *See Spectrum Management: Federal Government's Use of Spectrum and Preliminary Information on Spectrum Sharing*, GAO-12-1018T (Sept. 13, 2012).

[59] *Id.*

disclosure and correction of such vulnerabilities - incentives that will not excessively stifle innovation or affect commercial viability.

Part of the issue, which Jason Livingood noted, is that the current environment around reporting is penalty-oriented, and government regulators can actually discourage reporting with stringent liability standards that punish companies that are victims of cybercrimes rather than working with them to avoid and remediate. Instead of incentivizing the sharing of information, the companies may wish to avoid the potential negative consequences of disclosing the fact that an attack occurred. This can potentially lead to the compartmentalization of information, which prevents other companies from identifying and resolving the same or similar issues themselves. John Heitmann, Partner at Kelley Drye & Warren LLP, noted that part of the problem is that the twenty-four hour news cycle and current political climate demonize companies that have issues or breaches, in particular pointing out that these companies are not the criminals. Livingood also explained that as the development of technology has become so rapid, that it might make more sense to assume these instances will occur and it isn't a bad thing.

Another part of the equation is statistical data from the FCC about interference disputes. Dale Hatfield explained that one of his biggest disappointments is that we cannot get more transparency from the Commission regarding interference that is occurring today. While it is true that disputes leading to Commission orders are published on the FCC's webpage, there is no comprehensive database cataloging the categories of devices that are causing interference. Furthermore, when the Commission cannot reach a resolution, or the parties resolve the issue amongst themselves, other parties do not get information about the dispute or what steps were taken to resolve the issue. Dale Hatfield also noted that the FCC's Technological Advisory Council is beginning to get professional interference hunters to work together to get real time information on interference incidents, which may also aid in preventing attacks from the really bad actors as well.

Therefore, some participants noted that it is critical that manufacturers and operators are incentivized to report and share interference instances. For example, some participants suggested that one potential solution could be establishing safe-harbor or immunity for reporting interference events. These already exist in other areas of the law, such as regulation encouraging pilots reporting near to report near misses with other aircraft.[60] John Heitmann argued that by potentially mitigating the risks of disclosure, parties might be more open to actually sharing their own interference events.

Another solution could be to establish a multi-stakeholder process that incentivizes collaboration and reporting. This method would actually bring interested parties together to agree on a consensus approach. Linda Kinney noted that the multistakeholder process has been used in the past to establish consensus based best practices. To this point, the NTIA recently announced a new multistakeholder process concerning the Internet of Things Security Upgradability and Patching, with the first meeting taking place on October 19, 2016.[61]

---

[60] NEAR MISS REPORTING SYSTEMS (National Safety Council 2013), http://www.nsc.org/WorkplaceTrainingDocuments/Near-Miss-Reporting-Systems.pdf.

[61] Notice of Open Meeting, Multistakeholder Process on Internet of Things Security Upgradibility and Patching, National Telecommunications and Information Adminstration, 81 Fed. Reg. 64139 (Sep. 19, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-09-19/pdf/2016-22459.pdf.

III. Towards An Adaptive Model of Governmental Oversight

With the widespread proliferation of IoT devices and the increasing number of industry sectors using wireless spectrum to improve efficiency and innovation, mission-critical IoT devices are being examined by multiple regulatory bodies. While this sector specific regulation allows for expert agencies to address potential harms that relates to each agency's expertise, multiple sets of regulations can lead to inconsistent and inefficient outcomes in the marketplace. Therefore, participants suggested that it is critical to develop a national strategy for the internet of things.

A. Leadership

A main challenge identified by participants is the lack of coordination between agencies. If the Department of Transportation creates a regulation for the use of cell phones in automobiles that is inconsistent with FCC regulations that apply to the same device, there will be confusion in the marketplace and innovation may be harmed. Glenn Reynolds, Chief of Staff at the NTIA, explained that the challenges associated with many different agencies regulating a specific technology also stem from the fact that each agency has a different mandate.

Some participants also noted that when two agencies attempt to regulate the same sector, it can become increasingly difficult for one regulators to ensure that important data is shared with the other regulator. Trying to create interoperability requires data sharing on a business to business level. Eric Schneider suggested that a consumer mediated data exchange model, in which a consumer controls who has access to personal health data of all types, might influence how the regulators approach the problem. Likewise, he explained that the patient safety movement has encouraged the sharing of information between parties. As a result, agencies will need to ensure sharing of information, even amongst themselves.

Many agencies do already share information. Christine DeLorme, Attorney Advisor in the Office of FTC Commissioner Terrell McSweeny, explained that the FTC encourages information sharing among agencies. The FDA and the FTC, for example, have consulted on privacy issues related to consumer generated health data. Similar processes could be used for IoT to encourage data sharing among agencies.

Professor Reid suggested that, ultimately, one agency will need to play the role of the convener. If one agency can bring stakeholders together, the other agencies can participate in the process and work toward shared solutions. As Fernando Laguarda, Adjunct Associate Professor of Law at American University Washington College of Law, explained, even when no consensus can be reached amongst the parties, simply bringing the different interests together can bolster agency expertise, ultimately increasing the knowledge base about critical spectrum issues. Using this model, the NTIA and the White House have taken a thought leadership role in other areas such as drones.[62] In that case, however, many of the privacy groups dropped out of the best practices discussions in the NTIA's Unmanned Aircraft Systems Multi-Stakeholder

[62] *Multistakeholder Process: Unmanned Aircraft Systems*, NTIA (June 21, 2016), https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-unmanned-aircraft-systems; *see also* Lawrence E. Strickling, *Privacy and Facial Recognition Technology*, NTIA BLOG (Dec. 03, 2013), http://www.ntia.doc.gov/blog/2013/privacy-and-facial-recognition-technology.

Process (at least for now).[63] Nonetheless, participants suggested such discussions can lead to a series of best practices that industry can follow. Similarly, the White House announced a "Smart Cities" initiative in 2015 which included collaboration from a wide array of agencies.[64]

In the context of mission-critical IoT devices, an agency should be able to bring together interested parties with different backgrounds and different areas of focus. Ideally, this would encourage responsible behavior by manufacturers. Participants noted that one goal the government can promote is the interoperability and the use of industry-wide standards. The National Institute of Standards and Technology (NIST), a part of the Department of Commerce, promotes and maintains measurement standards and has active programs for encouraging and assisting industry and science to develop and use these standards.[65] Furthermore, the federal government can use its purchasing power to encourage development and deployment of secure or securable mission-critical IoT devices. For example, the Department of Transportation created a $160 million smart city grant program designed to facilitate the use of IoT devices in the critical infrastructure of cities.[66]

Finally, the government could take a more liability oriented approach. If one device fails due to faulty design or care, serious liability penalties would be imposed on the manufacturer. In principle, this could incentivize more companies to take appropriate security protections to ensure devices operate correctly. To that end, Jeff Blattner, President of Legal Policy Solutions, PLLC, suggested that it would be a useful exercise to consider what regulatory regime would evolve if the starting point was that innovators bore the risk if their innovations caused harm.

B. Managing Risk

Regardless of how regulators approach IoT, a key consideration will be the risks associated with particular regulatory bodies. Phil Verveer, Senior Counsel to Chairman Tom Wheeler at the FCC, explained that, in general, private actors are risk averse in traditional issues of liability instead of risk averse to the new threats of criminals, accidental problems, or state actors. Even the risk of potential catastrophic failure may not be enough to spur innovation or overcome the political gridlock. Instead, it may take the actual "boom"---the catastrophic event---to ultimately spurs innovation and reform.

Participants noted that we do a good job of identifying the problems, but not necessarily a good job of finding solutions. The problems are not going away, and there could come a point where a mission-critical device fails on a large scale. Some participants noted that trying to prevent the event could be a fruitless task. Instead, the goal should be to take steps to minimize the potential impact so that if a failure were to occur, only limited damage would result.

---

[63] *Letter From Privacy Groups to Participants in the NTIA Multi-Stakeholder Process on Unmanned Aircraft Systems*, ACLU (2016), https://www.aclu.org/letter/letter-privacy-groups-participants-ntia-multi-stakeholder-process-unmanned-aircraft-systems.

[64] Press Release, The White House, FACT SHEET: Administration Announces New "Smart Cities" Initiatives to Help Communities Tackle Local Challenges and Improve Cirt Services (Sept. 14, 2015), https://www.whitehouse.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help.

[65] 15 U.S.C. § 271.

[66] *Smart City Challenge*, DEPARTMENT OF TRANSPORTATION (last visited Oct. 30, 2016), https://www.transportation.gov/smartcity.

Even in the face of these potential challenges, it is important that regulators not overreact as IoT is still in the early stages of development. There are enormous potential benefits to society and consumers from IoT technology. By focusing on precautionary measures (and the precautionary principle), regulators run the risk of harming innovation.[67] Alternatively, the regulator could remain relatively hands off and allow for development, warn against potential concerns, and monitor the marketplace. As the FTC reported, self-regulatory programs designed for particular industries would be helpful as a means to encourage the adoption of privacy and security-sensitive practices.[68] This could include third party due diligence assessments as well, ideally ensuring that it is in the industry's best interest to self-regulate. As Blake Reid pointed out, however, risk is much harder to identify in the context of IoT, and even simple devices open up more risks as they create new attack surfaces and problems.

C. International Factors

A final concern that policymakers must be aware of is how any government action will affect market players on an international level. Innovation and the development of IoT will depend on international markets and adoption.

However, the current status of the development and deployment of IoT in the United States compared with international markets is debatable. Some argue that the United States is behind other countries in developing IoT policy frameworks. By contrast, Len Cali noted that the United States leads the world in actual marketplace deployment. In any event, an important policy priority will be to encourage the international adoption and implementation of IoT devices without an overly prescriptive regulatory approach that unnecessarily limits innovation.

Conclusion

As this report has shown, there are important reasons to be concerned with IoT security and privacy. While there are many paths policymakers can take, most participants suggested that, at this point in time, the government's primary role should be to foster innovation and promote industry generated solutions. A national strategy on IoT would help advance IoT deployment and monitor changing circumstances.[69] Such an effort could seek to enhance security on existing models, particularly through collaborative, standards-based approaches and industry-led certifications based on these standards. This would also involve crafting simple and transparent messages to consumers so that they can make better decisions when purchasing and operating mission-critical IoT devices. Moreover, policymakers can work on creating incentives that encourage reporting and enable information sharing rather than imposing penalties for near misses or attacking companies who make security and interference incidents public.

In the years ahead, IoT technology will facilitate a range of benefits, including in mission-critical environments. Because IoT is in its nascent stage, policymakers should be careful not to impede innovation and development. At the same time, the federal government should recognize

---

[67] Adam Thierer, *Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 Minn. J.L. Sci. & Tech. 309, 361-362 (2013).

[68] FTC Staff Report at vii.

[69] *See* Joshua New & Daniel Castro, Why Countries Need National Strategies for the Internet of Things (Center for Data Innovation, 2015), http://www2.datainnovation.org/2015-national-iot-strategies.pdf.

the potential for harm caused by security concerns and begin developing a broader strategy for governmental oversight.

Appendix A: Participants

Rebecca Arbogast, Senior Vice President, Global Public Policy, Comcast Corporation
Jeff Blattner, President, Legal Policy Solutions, PLLC
Len Cali, Senior Vice President, Global Public Policy, AT&T
Ryan Clough, General Counsel, Public Knowledge
Hap Connors, Member, Commonwealth Transportation Board
Christine DeLorme, Attorney Advisor Office of Commissioner, Terrell McSweeny, Federal Trade Commission
Jameson Dempsey, Associate, Kelley Drye & Warren LLP
Scott Deutchman, Deputy General Counsel and Vice President for Legal and External Affairs, NeuStar, Inc
Michele Farquhar, Partner, Hogan Lovells US LLP
Derik Goatson, Student, University of Colorado Law School
Ellen Goodman, Professor, Rutgers Law School
Joseph Lorenzo Hall, Chief Technologist, The Center for Democracy & Technology
Dale Hatfield, Senior Fellow, Silicon Flatirons Center for Law, Technology, and Entrepreneurship at the University of Colorado
John Heitmann, Partner, Kelley Drye & Warren LLP
Hank Kelly, Partner, Kelley Drye & Warren LLP
Robert (Bob) Kelly, Partner, Squire Patton Boggs
Linda Kinney, Senior Advisor, Internet Policy National Telecommunications and Information Administration
Fernando Laguarda, Adjunct Associate Professor of Law, American University Washington College of Law
Jason Livingood, Vice President, Technology Policy & Standards, Comcast
Koyulyn Miller, Associate, Squire Patton Boggs
Blake Reid, Assistant Clinical Professor, University of Colorado Law School
Alex Reynolds, Former Director, Regulatory Affairs, Consumer Technology Association
Glenn Reynolds, Chief of Staff, National Telecommunications and Information Administration
Jonathan Sackner-Bernstein, Former Associate, Center Director for Technology and Innovation, US Food and Drug Administration
Jon Sallet, General Counsel, Federal Communications Commission
Eric Schenider, Senior Vice President for Policy and Research, The Commonwealth Fund
Sara Schnittgrund, Director of Student Programs, Silicon Flatirons Center for Law, Technology, and Entrepreneurship at the University of Colorado
Roger Sherman, Principal, Waneta Strategies
Phil Verveer, Senior Counsel to the Chairman, Federal Communications Commission
Phil Weiser, Executive Director and Founder, Silicon Flatirons Center for Law, Technology, and Entrepreneurship at the University of Colorado
Jeff Westling, Student, University of Colorado Law School