MERCATUS CENTER
George Mason University

Bridging the gap between academic ideas and real-world problems

PUBLIC INTEREST COMMENT

LIFTING BARRIERS TO ENTREPRENEURSHIP: A "PERMISSIONLESS INNOVATION" APPROACH TO COMPETITION AND CONSUMER PROTECTION POLICIES

ADAM THIERER
Senior Research Fellow, Technology Policy Program, Mercatus Center at George Mason University

MICHAEL KOTROUS
Program Associate, Technology Policy Program, Mercatus Center at George Mason University

JENNIFER HUDDLESTON SKEES
Legal Research Associate, Technology Policy Program, Mercatus Center at George Mason University

ANNE HOBSON
Program Manager, Academic & Student Programs, Mercatus Center at George Mason University

Hearings on Competition and Consumer Protection in the 21st Century
Agency: Federal Trade Commission
Comment Period Opens: June 20, 2018
Comment Period Closes: August 20, 2018
Submitted: August 16, 2018
Document No. 2018-16608

The attached submission is written in response to the request by the Federal Trade Commission (FTC) for comments regarding the upcoming public hearings on competition and consumer protection in the 21st century.

These hearings come as the United States and European Union (EU) have significantly diverged on the questions of antitrust enforcement and consumer protection regulations concerning the digital economy. While proposals for reforming US competition and consumer protection policies to more closely match those of the EU have gained support in recent years,[1] we and other Mercatus Center scholars have written extensively on the damaging effects adopting an EU-style regulatory framework would have on innovation, competition, and consumer welfare.

[1] A policy paper recently produced by the office of Senator Mark Warner (D-VA) outlines 20 proposals for revising, among other things, consumer protection and competition policy regarding social media platforms and large tech companies. See David McCabe, "Scoop: 20 Ways Democrats Could Crack Down on Big Tech," *Axios*, July 30, 2018.

For more information, contact
Mercatus Outreach
Mercatus Center at George Mason University
3434 Washington Blvd., 4th Floor, Arlington, VA 22201

The ideas presented in this document do not represent official positions of the Mercatus Center or George Mason University.

The burdens that the EU's regulatory actions have imposed on innovation in the technology sector raise concerns the FTC should heed. The EU's sweeping General Data Protection Regulation (GDPR) could actually increase the market power of large tech companies like Facebook and Google in digital advertising, and GDPR is likely to raise compliance costs to businesses and individuals across the globe so much that many firms will drop out of the industry, leaving consumers with even fewer options in digital goods and services.[2] Meanwhile, the EU's antitrust actions against tech firms, such as its recent Android ruling, have done little to promote competition or increase consumer welfare.[3]

The EU's heavy-handed regulatory approach to competition and consumer protection directly opposes two decades of light-touch regulation in the United States and threatens the openness under which internet services have flourished.[4] Under the American light-touch regulatory regime—anchored in the principles of "permissionless innovation"—information technology companies experiment with different business models and deliver innovative and novel products and services to consumers without prior regulatory approval and with limited red tape.[5] The result of getting innovation policy right is seen in the large gap between the United States and Europe in attracting capital to tech ventures. Of the 274 privately held tech companies to reach a one-billion-dollar valuation since 2003, over half (148) of these so-called unicorns are based in the United States, while only 33 were started in Europe.[6]

Observing the success that permissionless innovation has given American technology companies, we offer the following principles to guide competition and consumer protection policy:

1. Antitrust policy should focus on the effects of a firm's practices on consumer welfare, not the firm's market power *per se*, the size of its network of users,[7] or supposed advantages of "big data."[8]
2. Review of vertical mergers and acquisitions ought not to be treated differently for firms in the "information economy."[9]

---

[2] Adam Thierer, "How Well-Intentioned Privacy Regulation Could Boost Market Power of Facebook & Google," *Technology Liberation Front*, April 25, 2018; Alice Calder and Anne Hobson, "Data Privacy at a Price," *Plain Text*, May 25, 2018; Andrea O'Sullivan, "The EU's New Privacy Rules Are Already Causing International Headaches," *Reason*, June 12, 2018.
[3] Andrea O'Sullivan and Veronique de Rugy, "Major Sanctions on Android Are the Latest EU Trade Barrier," *The Bridge*, July 26, 2018.
[4] Brent Skorup and Jennifer Huddleston Skees, "It's Not about Facebook; It's about the Next Facebook," *Real Clear Policy*, June 1, 2018.
[5] Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (Arlington, VA: Mercatus Center at George Mason University, 2016).
[6] François Candelon, Martin Reeves, and Daniel Wu, "18 of the Top 20 Tech Companies Are in the Western U.S. and Eastern China. Can Anywhere Else Catch Up?," *Harvard Business Review*, May 3, 2018.
[7] Christopher Koopman and Michael Kotrous, "AIM's Demise Illustrates the Fluidity of the Tech Market," *The Hill*, October 16, 2017.
[8] Michael Kotrous, "Antitrust and Tech: One Network to Rule Them All?," *Plain Text*, February 19, 2018.
[9] Adam Thierer and Brent Skorup, "Uncreative Destruction: The Misguided War on Vertical Integration in the Information Economy," *Federal Communications Law Journal* 65, no. 2 (2013): 157–201; Adam Thierer, "The Perils of Classifying Social Media Platforms as Public Utilities," *CommLaw Conspectus* 21, no. 2 (2013): 249–97.

3. Definitions of harm should be narrowly tailored to reflect only truly cognizable harms to the consumer or competition, not speculative harms like, for instance, the effects of a proposed merger or acquisition on "potential competition."[10]
4. Regulations regarding privacy and market power must be examined in the context of tradeoffs.[11]
5. A key role for regulatory agencies is to educate and empower consumers.[12]

We commend the FTC for its intention to hold hearings on the topic of competition and consumer protection. The growth in market concentration and declines in business startups and labor market mobility observed in the United States since the 1970s are troubling trends.[13] Thus, public policies and regulatory approaches that will encourage entrepreneurialism and competition in the marketplace ought to be examined and debated.

The digital economy has been the most productive and dynamic sector in the 21st century and created digital goods and services that have been a boon for consumers in the United States and across the globe.[14] This dynamism could not have been possible without the United States' light-touch regulatory regime. We therefore find proposals for US regulators to tighten the rules for the sake of taking action against today's leading technology firms to be misguided.[15] Indeed, the EU's ongoing regulatory interventions in the digital economy show that this approach comes to the detriment of both competition and consumer protection. To advance the ends of competition and consumer protection, the FTC would do better to continue the work of the Economic Liberty Task Force, a project that seeks to identify and reverse onerous rules and regulations that suppress entrepreneurial activity and consumer choice across many industries.[16]

In addition to the general comments and citations provided above, we are pleased to submit for the record the attached documents. We hope these comments and the attached documents are of assistance to the FTC as it begins to consider these important issues.

---

[10] Christopher Koopman et al., "Informational Injury in FTC Privacy and Data Security Cases" (Public Interest Comment, Mercatus Center at George Mason University, Arlington, VA, October 27, 2017).
[11] Skorup and Huddleston Skees, "It's Not about Facebook; It's about the Next Facebook."
[12] Adam Thierer, Jennifer Huddleston Skees, and Anne Hobson, "The Internet of Things and Consumer Product Hazards" (Public Interest Comment, Mercatus Center at George Mason University, Arlington, VA, June 14, 2018).
[13] White House Council of Economic Advisers, *Benefits of Competition and Indicators of Market Power*, April 2016.
[14] "From 2000 to 2015, the digital industries generated productivity growth of 2.7% per year, compared to just 0.7% for physical industries" See Michael Mandel and Bret Swanson, *The Coming Productivity Boom: Transforming the Physical Economy with Information* (Washington, DC: Technology CEO Council, 2017), 5.
[15] See, for example, Lina M. Khan, "Amazon's Antitrust Paradox," *Yale Law Journal* 126, no. 3 (2017): 710–805. The Institute for Technology Law & Policy hosted a symposium featuring panels such as "Governance of and by Platforms" and "Problems of Access and Entry" (the articles submitted for the symposium were published in the spring issue of the *Georgetown Law Technology Review*).
[16] Christopher Koopman and Adam Thierer, "FTC's New Economic Liberty Task Force Is a Step in Right Direction," *The Hill*, April 5, 2017.

ATTACHMENTS (4)

Christopher Koopman et al., "Informational Injury in FTC Privacy and Data Security Cases" (Mercatus Public Interest Comment)

Adam Thierer, Jennifer Huddleston Skees, and Anne Hobson, "The Internet of Things and Consumer Product Hazards" (Mercatus Public Interest Comment)

Anne Hobson, *R Street Institute Comments to the National Telecommunications and Information Administration Regarding the "Internet-of-Things"* (Washington, DC: R Street Institute, 2017).

Anne Hobson, "Aligning Cybersecurity Incentives in an Interconnected World" (Policy Study No. 86, R Street Institute, Washington, DC, February 2017).

MERCATUS CENTER
George Mason University

Bridging the gap between academic ideas and real-world problems

PUBLIC INTEREST COMMENT

INFORMATIONAL INJURY IN FTC PRIVACY AND DATA SECURITY CASES

CHRISTOPHER KOOPMAN
Director, Technology Policy Program, Mercatus Center at George Mason University

ADAM THIERER
Senior Research Fellow, Mercatus Center at George Mason University

ANDREA CASTILLO O'SULLIVAN
Program Manager, Technology Policy Program, Mercatus Center at George Mason University

JENNIFER HUDDLESTON SKEES
Legal Research Associate, Mercatus Center at George Mason University

Informational Injury Workshop P17-5413
Notice of Workshop and Opportunity for Comment
Agency: Federal Trade Commission
Proposed: September 29, 2017
Comment period closes: October 27, 2017
Submitted: October 27, 2017

INTRODUCTION

The Technology Policy Program of the Mercatus Center at George Mason University is dedicated to advancing knowledge about the effects of regulation on society. As part of its mission, the program conducts independent analyses to assess agency rulemakings and proposals from the perspective of consumers and the public. Therefore, this reply comment does not represent the views of any particular affected party but is designed to assist the agency as it explores these issues.

We appreciate the opportunity to submit reply comments regarding the Federal Trade Commission's (FTC) Workshop on Informational Injury. In her comments to the Federal Communications Bar Association on September 19, Chairwoman Maureen Ohlhausen defined the three goals of the workshop: (1) to "better identify the qualitatively different types of injury to consumers and businesses from privacy and data security incidents," (2) to "better explore frameworks for how we might approach quantitatively measuring such injuries and estimate the risk of their occurrence,"

For more information, contact
Canyon Brimhall, Outreach Associate, Technology Policy Program

Mercatus Center at George Mason University
3434 Washington Boulevard., 4th Floor, Arlington, VA 22201

The ideas presented in this document do not represent official positions of the Mercatus Center or George Mason University.

and (3) to "better understand how consumers and businesses weigh these injuries and risks when evaluating the tradeoffs to sharing, collecting, storing, and using information."[1]

The workshop raises important and timely questions about the FTC's role in investigating cases relating to data breach and privacy incidents that fall within the commission's statutory unfairness and deception authorities.[2] Our comments will focus on developing a framework that appropriately addresses the ongoing challenges with data security without imposing on society an ineffective, all-encompassing theory of "harm" that may undermine the freedom to innovate in data use.

We begin with a discussion of data and security issues at the FTC. We then outline our vision for the future of FTC oversight of data breach cases, drawing heavily from the iterative process of common law. We then discuss why rigid theories of harm are inappropriate for meeting data security challenges. Finally, we provide a roadmap for how the commission can move closer to the ideal.

A BRIEF HISTORY OF THE FTC AND CYBERSECURITY

The United States currently lacks a dedicated regulator for data and security issues, allowing a number of agencies to become involved in cybersecurity issues relating to incidents in their primary jurisdictions. For example, the Securities and Exchange Commission issues guidance for financial institutions to safeguard their data, while the Food and Drug Administration has investigated device manufacturers for selling insecure medical devices. The FTC, however, is more involved than any other federal agency in data security oversight and adjudication.[3]

This was a development more of necessity than of design. As the internet revolution took hold in the 1990s and companies began grappling with new questions of data collection and storage, there was no regulatory framework to guide industry and establish legal certainty. The FTC, with its relatively broad Section 5 authority to protect consumers from deceptive or unfair acts or practices,[4] was well poised to fill the void.[5]

The commission initially promoted self-regulation as the primary policy for data and security issues,[6] a policy that would be supplemented by promotion of "fair information practice principles" as adequate standards to guide groups. However, the FTC quickly pivoted to more active measures in an attempt to promote internet security and thereby ensure its future functioning.[7] Specifically, the FTC first began pursuing potential privacy violations—where websites did not provide the level

---

[1] Maureen K. Ohlhausen, "Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases" (Speech before the Federal Communications Bar Association, Washington, DC, September 19, 2017).

[2] For a description of these authorities, see the FTC website at https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

[3] Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress* (May 2000).

[4] 15 U.S.C. § 45 (2017).

[5] Woodrow Hartzog and Daniel J. Solove, "The Scope and Potential of FTC Data Protection," *George Washington Law Review* 83 (2015): 2230–2300.

[6] Federal Trade Commission, *Self-Regulation and Privacy Online: A Report to Congress* (July 1999).

[7] In 2000, the commission called upon Congress to pass comprehensive legislation expanding the government's role in controlling online privacy and data standards. This approach was ultimately unsuccessful, and several commissioners dissented against the recommendations provided to Congress. Michael D. Scott, "The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?," *Administrative Law Review* 60, no. 1 (2008): 127–83.

of privacy promised in their stated privacy policies[8]—using a claim of "deception."[9] Later, the FTC became involved in matters relating to data breaches and security, applying its authority to investigate "unfairness" as a basis for such cases.[10] This approach has become controversial within academic and policy circles,[11] and it has spawned two notable legal battles.[12]

Despite lacking a specific congressional charge to oversee data and privacy issues, the FTC has persevered as the primary watchdog for consumer cybersecurity challenges.[13] Notably, as we discuss in more detail later, the FTC has largely eschewed an approach characterized by substantive rulemaking, favoring instead a quasi-common law method facilitated mainly by consent orders and administrative adjudication.[14] Furthermore, the FTC lacks a clear set of guidelines[15] to guide private actors who wish to both maintain good security and remain compliant with FTC best practices[16]—a situation that the commission admirably wishes to rectify with this very workshop.

While we applaud the FTC for its commitment to flexibility and its distaste for onerous, top-down regulation, we believe that the FTC should strive to get closer to a true common law approach rather than attempt to develop rigid, all-encompassing theories of harm that might keep lawyers busy but bring us no closer to better security and privacy. We outline a model path for the FTC to pursue in the following section.

THE COMMON LAW IDEAL

Concerns about existing tort law's ability to handle perceived intrusions into privacy are not new in the digital age. In fact, an 1890 *Harvard Law Review* article established the jurisprudence for privacy torts. Its authors—one of them, Louis D. Brandeis, would later become the famed associate justice of the Supreme Court—thought the rising power of newspapers and new technologies such as photography presented threats to individual privacy.[17]

---

[8] For example, the first of such FTC actions was *In re Geocities*, Docket No. C-3850 (F.T.C. February 5, 1999), where Geocities allegedly used user data in a way contrary to the guidelines laid out in Geocities's privacy policy.
[9] Steven Hetcher, "The FTC as Internet Privacy Norm Entrepreneur," *Vanderbilt Law Review* 53 (2000): 2041–61.
[10] Alden Abbott, "The Federal Trade Commission's Role in Online Security: Data Protector or Dictator?," The Heritage Foundation, September 10, 2014.
[11] Scott, "The FTC, the Unfairness Doctrine, and Data Security Breach Litigation."
[12] FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015); LabMD, Inc. v. Federal Trade Commission, No. 1:1 4 -CV-81o-WSD, 2014 WL 198716 (N.D. Ga. May 7, 2014).
[13] The FTC has undertaken at least 40 general privacy cases and 60 cases related to data security since 2002. Federal Trade Commission, *Privacy and Data Security—Update: 2016*, 2016.
[14] Gus Hurwitz, "Data Security and the FTC's UnCommon Law," *Iowa Law Review* 101 (2016): 955–1022.
[15] The FTC's public guidelines, called "Protecting Personal Information: A Guide for Business," provide general security tips, but no specific requirements for companies to follow. Rather, FTC officials have argued that parties must keep abreast of a byzantine maze of consent decrees to determine the extent to which their security practices are in line with FTC requirements. Federal Trade Commission, "Protecting Personal Information: A Guide for Business," October 2016.
16 Berin Szoka and Graham Owens, "FTC Stakeholder Perspectives: Reform Proposals to Improve Fairness, Innovation, and Consumer Welfare" (Testimony before the Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security of the US Senate Committee on Commerce, Science, & Transportation, September 26, 2017).
[17] Privacilla, *The Privacy Torts: How U.S. State Law Quietly Leads the Way in Privacy Protection*, July 2002.

Former FTC Chairwoman Edith Ramirez spoke positively of a common law approach to unfairness claims, stating that it is "well-suited to find the right balance [between flexibility and certainty]."[18] This statement is also true for the common law's ability to handle security-specific issues through existing privacy torts. Since legal scholar William L. Posser posited four common law privacy torts in 1960, most states have adopted and codified this typology through precedent or statute.[19]

Since relatively early in the digital era, these torts have evolved to accommodate reasonable expectations of privacy in cyberspace. The simultaneous adaptability and consistency of the common law gives it a clear advantage over statutory solutions.[20]

In the case of the informational harms proposed, courts have either handled or could handle these issues with existing tort law. For example, concerns about "dataveillance"—the monitoring of online activity—or other potentially deceitful injuries or subversions of consumer choice could be handled by applying intrusion into voluntary seclusion.[21] Intrusion is not necessarily physical in nature, so courts at common law can consider whether perceived online disclosures or other monitoring such as spyware can be challenged under the existing law.[22] Because the common law does not require a specific physical presence, the existing privacy torts can be extended and do not require an additional element of enforcement.

Some have expressed concerns that the anonymity and distance from the victim associated with using the internet or other technology to carry out intentional torts cause physical or financial harms that are not addressed by current privacy torts[23]; however, torts such as libel or intentional infliction of emotional distress do not require physical proximity to the victim as an element. Cyberspace may change the forum in which such acts are conducted, but it does not change the required elements. Moreover, the common law has evolved to account for situations when the alleged perpetrator remains anonymous through the use of internet platforms. Yelp has been forced to disclose the identities of anonymous reviewers when the reviews are found to be libelous, and individuals have been held liable for defamation or libel for fraudulent negative reviews.[24]

Courts are in a better position than regulators to determine when there is a legal duty in handling data and when that duty has been breached. Regulation is inflexible and preemptively shuts down

---

[18] Edith Ramirez, "Unfair Methods and the Competitive Process: Enforcement Principles for the FTC's Next Century" (Speech at the George Mason University School of Law, Arlington, VA, February 13, 2014).
[19] Privacilla, *The Privacy Torts*.
[20] Jim Harper, "Remember the Common Law" (Cato Policy Report, Cato Institute, Washington, DC, March and April 2016).
[21] Benjamin Zhu, "A Traditional Tort for a Modern Threat: Applying Intrusion upon Seclusion to Dataveillance Observations," *New York University Law Review* 89 (2014): 2401–2407.
[22] American Law Institute, *Restatement of the Law of Torts*, 2nd ed., § 652.
[23] See Mark MacCarthy, "New Directions in Privacy: Disclosure, Unfairness and Externalities," *I/S Journal of Law and Policy* 6 (2011): 425.
[24] Paresh Dave, "California Supreme Court to Review a Libel Case over Negative Yelp Reviews," *Los Angeles Times*, September 21, 2016); Kellan Howell and Phillip Swarts, "Yelp Critics Must Be Identified, Court Rules in Online Landscape Altering Decision," *Washington Times*, January 8, 2014).

potential avenues of innovation. In contrast, the courts are more flexible as they rule over specific contested avenues of innovation without curtailing other experiments.[25]

Currently, there is no established legal duty to handle most data or privacy in a certain way; however, a breach of terms of service or other data security claims could be handled under existing tort or contract law without additional regulatory intervention. The courts have been able to adapt existing common law torts of privacy to new media and technology in the past and should be able to adapt to current digital technology. Moreover, for the most vulnerable data, other statutory provisions already exist to establish a duty when handling the information. For example, the Health Insurance Portability and Accountability Act covers the duty surrounding medical information and data, the Children's Online Privacy Protection Act creates certain duties regarding data collected on children, and the Consumer Financial Protection Bureau's "unfair, deceptive, or abusive practices" standard can be employed against financial services companies for advertising false data management practices.[26]

A BAD ALTERNATIVE: A THEORY OF EVERYTHING

Chairwoman Ohlhausen has made it clear that the FTC is not seeking to "deduce a definition of injury from first principles."[27] Rather, she calls upon the community to consider (1) whether the FTC's current case-by-case approach toward privacy- and security-related "informational injury" is representative,[28] (2) whether any element may require government intervention, and (3) how the list of injuries corresponds with the FTC's statutory deception and unfairness authorities.[29]

We applaud the FTC for eschewing the temptation to develop a ground-up "theory of everything" to drive privacy and security oversight. Too often, members of the academy, the policy-making community, and the general public default to promoting jury-rigged, one-size-fits-all approaches toward concerns about public health and safety.[30] More thoughtful scholars, meanwhile, have attempted to sketch out an actionable rubric for informational harms and adequate remedies, to little avail or consensus.[31] We anticipate that the prominence of newsworthy data security incidents, particularly the recent compromise of Equifax's expansive personal finance datasets, will

---

[25] "Because the tort system operates retrospectively, it is restitution-based, not permission-based. This also creates incentives for firms to make their products safer over time so they can avoid lawsuits." Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*, 2nd ed. (Arlington, VA: Mercatus Center at George Mason University, 2016), 122.

[26] Consumer Financial Protection Bureau, "CFPB Takes Action against Dwolla for Misrepresenting Data Security Practices," March 2, 2016.

[27] Ohlhausen, "Painting the Privacy Landscape."

[28] The FTC currently groups its enforcement actions relating to privacy and security incidents into five categories: (1) deception injury, or subverting consumer choice, (2) financial injury, (3) health and safety injury, (4) unwarranted intrusion injury, and (5) reputational injury. Enforcement actions may be brought against individuals or groups if the harm caused to parties was inflicted through the FTC's authority to investigate unfair or deceptive practices. See Ohlhausen, "Painting the Privacy Landscape."

[29] Ohlhausen, "Painting the Privacy Landscape."

[30] For a specific critique of this approach as applied to online privacy standards, see Adam Thierer, "The Pursuit of Privacy in a World Where Information Control Is Failing," *Harvard Journal of Law and Public Policy* 36 (2013): 409–54.

[31] See, for example, M. Ryan Calo, "The Boundaries of Privacy Harm," *Indiana Journal of Law* 86 (2011): 1131–61; Joel R. Reidenberg, "Privacy Wrongs in Search of Remedies," *Hastings Law Journal* 877 (2003): 877–98; Daniel J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review* 154, no. 3 (2006): 477–560.

fuel feedback to the FTC urging just this kind of approach. We suggest that the FTC stay the course in rejecting such calls for several reasons.

First, broadly defining informational harms could impose serious and unnecessary damage to the information economy. Europe has chosen to institute such a broad definition,[32] and the result has been to diminish competition and innovation in the EU information technology field.[33] Avoiding this approach will ensure that the United States remains a leader in information technology innovation.

Additionally, an expansive view of informational harms may conflict with First Amendment–protected speech. Scholars such as Eugene Volokh have pointed out that when the government determines an information privacy standard that extends into the private sector and prevents the sharing of information, it is inevitably silencing speakers.[34] This is not to say that restrictions on speech for privacy reasons are never allowed, but as with all limitations on free speech, such restrictions must be narrowly tailored.[35] The commission should draw on the current heightened standards for other speech-induced harms, such as defamation and libel, when considering restrictions on information sharing to ensure they do not risk unnecessarily limiting speech.

In practical terms, it is virtually impossible to develop and enforce a kind of overarching theory of harm appropriate for the internet age.[36] Opinions on what constitutes harm and appropriate redress are almost as varied as the number of people online, and different people have different risk thresholds.[37] In general, US regulators have eschewed this kind of approach, preferring instead to outline hard limits on certain behaviors—say, regarding child safety online—rather than attempting to pursue this Sisyphean task.

Furthermore, such attempts are simply unlikely to single-handedly improve security and privacy outcomes. Security is a fast-paced and dynamic space, and static frameworks will be ill suited to adapt to the evolving nature of developing threats. Similarly, opinions on what constitutes an adequate level of privacy are almost as varied as the personalities of the people who hold them, and these opinions evolve over time. Smart policies require a degree of flexibility to best address both security and privacy.

How, then, can the FTC improve its privacy and security enforcement in a manner that addresses consumer needs without foisting an onerous and ineffective standard on private parties? The answer is by moving FTC enforcement closer to the ideal of common law evolution.

---

[32] Specifically, the EU's Data Protection Directive (DPD) of 1995 and General Data Protection Regulation (GDPR) of 2016 (to take effect in 2018) impose strict top-down regulations protecting a defined "right to privacy" in EU member states. The GDPR is even more expansive than the DPD, applying to companies not based in the EU that process data of EU residents. For more information, see Bert-Jaap Koops, "The Trouble with European Data Protection Law," *International Data Privacy Law* 4, no. 4 (2014): 250–61.

[33] Adam Thierer, "How Attitudes about Risk & Failure Affect Innovation on Either Side of the Atlantic," *Plain Text*, June 19, 2015; Larry Downes, "How Europe Can Create Its Own Silicon Valley," *Harvard Business Review*, June 11, 2015.

[34] Eugene Volokh, "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You," *Stanford Law Review* 52 (2000): 1088–89.

[35] Volokh, "Freedom of Speech and Information Privacy," 1106–22.

[36] Adam Thierer, "Online Privacy Regulation," Presentation to the Washington Legal Foundation, June 22, 2015.

[37] Daniel J. Solove, *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2010).

BRIDGING THEORY AND PRACTICE: HOW THE FTC CAN IMPROVE

Chairwoman Ohlhausen notably characterized the FTC's current approach to privacy and security issues as common law–like. She described how the agency's "case-by-case enforcement . . . integrates feedback on earlier cases from advocates, the marketplace and, importantly, the courts. This ongoing process preserves companies' freedom to innovate with data use. And it can adapt to new technologies and new causes of injury."[38] The chairwoman's statements echo those of previous commissioner Julie Brill, who stated that the FTC's actions had created a "common law of privacy" in the United States.[39]

Unfortunately, the FTC's approach to privacy and security issues only superficially resembles a true common law path.[40] Rather than developing a real body of law through traditional litigation in the courts, the FTC has built up a mountain of loosely related consent orders[41] that all private parties must sift through to determine whether or not their businesses comply with FTC standards. Notably, this system operates in the absence of a defined rulemaking process; it does not include notice and comment, nor does it provide clear guidelines.[42]

Recent case law has shown the difficulty in applying an unclear standard of unfair or deceptive practices for both regulated entities and the courts. In the recent *LabMD* case,[43] for example, where the FTC attempted to bring action against a Georgia-based health laboratory despite a lack of notice or guidance, Judge William S. Duffey Jr. criticized the agency's approach to using consent orders to create regulation or duties without public awareness, stating that the FTC "ought to give [regulated parties] some guidance as to what you do and do not expect, what is or is not required. You are a regulatory agency. I suspect you can do that."[44]

Others have expressed similar frustration. In the *LabMD* case, the FTC attempted to launch a legal theory that had never been considered in court against the defendant, prompting FTC Chief Administrative Law Judge Michael Chappell to ask, "Where is the fairness in that, Counselor? If you're a company, you're a corporation, where is the fairness in a standard of what the law is being issued or published after the case is brought?"[45]

In *FTC v. D-Link*, the FTC claimed that firmware issues that made a router susceptible to hacking were an unfair and deceptive trade practice because they placed consumers' personal information

---

[38] Ohlhausen, "Painting the Privacy Landscape."

[39] Julie Brill, "Privacy, Consumer Protection, and Competition" (Speech before the 12th Annual Loyola Antitrust Colloquium, Loyola University Chicago School of Law, Chicago, IL, April 27, 2012).

[40] The following court cases are all cited in Hurwitz, "Data Security and the FTC's UnCommon Law."

[41] A consent order is an agreement between the FTC and a private party to settle a purported violation of an FTC rule or law under its authority. In entering into a consent order, the private party agrees to cease or correct the activity under FTC investigation.

[42] Szoka and Owens, "FTC Stakeholder Perspectives."

[43] It should be noted that the events preceding the action against LabMD are unusual, to put it charitably. A private intelligence firm called Tiversa apparently alerted the FTC that LabMD data was available on a P2P network sometime in 2010. LabMD disputes this version of events, claiming that Tiversa actually illegally accessed the data and passed it on to the FTC, creating the appearance of impropriety where there was none. Furthermore, LabMD alleged that Tiversa was actually in the pay of federal parties. Regardless of the intrigue surrounding the genesis of this action, the legal issues regarding notice and overreliance on consent decrees are more relevant for the purposes of this comment. For more information, see Evan M. Wooten and Lei Shen, "The Curious Case of LabMD: New Developments in the 'Other' FTC Data-Security Case," Mayer Brown, August 11, 2014.

[44] Closing Arguments at 8, LabMD, Inc., v. FTC, No. 9357 (F.T.C. Sep. 16, 2015).

[45] Transcript of Proceedings at 91, LabMD, Inc. v. FTC, No. 1:1 4 -CV-81o-WSD, 2014 WL 198716 (N.D. Ga. May 7, 2014).

and networks at risk.[46] A federal court for the Northern District of California found that while the FTC's claims that D-Link's comments about its security were sufficient to allow that portion of the case to continue, there was insufficient evidence to proceed under California's unfair trade practices law. The court also questioned the sufficiency of the claim regarding unfair trade practices under federal law.[47] The court dismissed the FTC's unfairness claims against D-Link for lack of an adequate injury, because the FTC did not "allege any actual consumer injury."[48] This shows at least that some courts will not allow the FTC to pursue a claim when there is no evidence that harm or injury has actually occurred.

FTC v. Wyndham Worldwide provides an example of how the FTC's current system not only fails to provide a common law itself, but complicates or confuses the existing common law with its lack of clarity. The FTC alleged that Wyndham hotels' lack of cybersecurity for consumer information, including credit card data and addresses, was an unfair practice when it was hacked, potentially exposing such information. The law is unclear about what constitutes an unfair practice for addressing data breaches, which in one case led the FTC to ask a district judge to take the unusual step of certifying the question to the Third Circuit on interlocutory appeal.[49] The Third Circuit affirmed the FTC's ability to use its Section 5 authority to enforce data security in the context of that litigation, but it questioned the lack of guidance provided for both the public and regulated individuals.[50] This struggle shows that the existing difficulties also prevent courts and common law from evolving their own definitions while the FTC standard remains notably vague.

Such concerns are not confined to the use of unfairness but also include the use of deception. Perhaps no case study illustrates this more clearly than *Nomi Technologies*.[51] Nomi collected shopping data and offered customers an option to opt out of both physical store data collection and website data collection. However, the data collection from physical stores was not successfully removed even when a consumer had opted out. Nomi served as a third-party contractor for the retailers in the collection of data and therefore, as Commissioner Ohlhausen stated in her dissent, had no obligation to provide consumers an opt-out.[52] By offering an option, however, the company was found to be deceptive despite having no duty to provide such an option and despite the lack of evidence of harm to any consumers. As some commenters at the time pointed out, the FTC's ruling made it better for an app developer not to provide any privacy policy rather than to provide one that may later prove to be flawed.[53] Not only does this ruling fail to provide clear standards for what constitutes deceptive practices for data privacy, it also punishes a company in the absence of consumer harm.

Rather than building on existing precedent to establish a series of understandable, stable norms, these orders and actions do little to clarify what the FTC considers an unfair or deceptive practice

---

[46] FTC v. D-Link Sys., No. 3:17-cv-00039-JD, at *2 (N.D. Cal. Sep. 19, 2017).
[47] *D-Link Sys.* at *3-*10.
[48] *D-Link Sys.* at *14.
[49] Hurwitz, "Data Security and the FTC's UnCommon Law."
[50] Federal Trade Commission v. Wyndham Worldwide Corp., 799 F.3d 236, 240, 257 n.23 (3d Cir. 2015).
[51] In the Matter of Nomi Technologies, Inc., FTC Matter No. 1323251, September 3, 2015.
[52] "Dissenting Statement of Commissioner Maureen K. Ohlhausen," In the Matter of Nomi Technologies, Inc., FTC Matter No. 1323251, April 23, 2015.
[53] Letter from Donald S. Clark, secretary of the Federal Trade Commission, to Michelle Lease et al., "Re: In the Matter of Nomi Technologies, Inc., File No. 1323251," August 28, 2015.

and fail to provide adequate guidance to regulated parties. Common law provides a precedent that regulated parties and individuals can build upon. The current system fails to adequately provide this guidance. The courts and current tort law may be better equipped to develop a system of common law to establish what duties are required.

Returning such issues properly to the courts as opposed to using administrative consent orders would not leave individuals without remedy and could provide better information to all involved. Class actions or individual lawsuits typically accompany or precede regulatory action. Courts have ruled that actual harm caused by the theft of personal information from a known data breach need not be proved; the heightened threat of identity theft from a "fairly traceable" data theft and the cost necessary to protect oneself from such risks following information exposure are sufficient to allow a case to proceed.[54] Courts are also able to provide injunctive relief to plaintiffs when necessary to stop further harm from occurring. While there is always a risk that common law could evolve in a less than ideal way, the risk of more consequential and restrictive regulations is far more likely to have a negative impact on both consumers and regulated industries.

Any regulation in this area should have a high bar of providing guidance that does not impact the continued development of new technology. It should also retain the right of both consumers and regulated entities to go to court and trust the common law instead of an administrative process.

CONCLUSION

In calling this workshop to examine the FTC's history and future of enforcement actions relating to privacy and security issues, the agency demonstrates that it recognizes feedback from industry and commentators and wishes to constructively improve upon its record. We applaud the FTC for recognizing this opportunity to improve, and we have outlined a framework that can maintain both consumer redress and regulatory flexibility.

We believe that the FTC and industry have the same goal: to protect consumers from informational harm without imposing a brittle bureaucratic structure that does little to promote actual security. To that end, we encourage the FTC to eschew any calls to develop rigid, all-encompassing theories of "informational injury" to guide future actions. Rather, the FTC should strive to develop a true body of common law precedent.

[54] Attias v. CareFirst, No. 16-7108 (D.C. Cir. Aug. 1, 2017) (allowing a class action concerning a data breach to go forward).

MERCATUS CENTER
George Mason University

Bridging the gap between academic ideas and real-world problems

PUBLIC INTEREST COMMENT

THE INTERNET OF THINGS AND CONSUMER PRODUCT HAZARDS

ADAM THIERER
Senior Research Fellow, Technology Policy Program, Mercatus Center at George Mason University

JENNIFER HUDDLESTON SKEES
Legal Research Associate, Technology Policy Program, Mercatus Center at George Mason University

ANNE HOBSON
Program Manager, Academic and Student Programs, Mercatus Center at George Mason University

Agency: US Consumer Product Safety Commission
Comment Period Opens: March 27, 2018
Comment Period Closes: June 15, 2018
Submitted: June 14, 2018
Docket No. CPSC-2018-0007

We appreciate the opportunity to respond to the request by the US Consumer Product Safety Commission (CPSC) for written comments on the potential safety issues and hazards associated with internet-connected consumer products. The internet of things (IoT) is a burgeoning ecosystem. Promoting resilience—that is, the capacity to withstand and learn from cyberattacks—in this ecosystem without hampering innovation is crucial for the ecosystem's full benefits to be realized.

IoT devices enhance productivity and convenience, helping to automate household chores from vacuuming to food preparation. The first recorded consumer IoT device was a Coca-Cola machine programmed in the 1980s by the Carnegie Mellon University Computer Science Department that used an internet connection to inform would-be drinkers about the status of its contents.[1] The added convenience ensured that students and professors didn't have to cross campus only to find an empty machine or a warm beverage. In the consumer market, the IoT gives users more instant control over devices such as TVs and thermostats. According to McKinsey Global Institute, the economic impact of household IoT applications will amount to $350 billion per year in 2025, cutting the time required for chores by 17 percent.[2] Additionally, the IoT industry will generate millions of job opportunities and trillions of dollars in both economic growth and cost savings.[3]

---

[1] Jordan Teicher, "The Little-Known Story of the First IoT Device," *IBM Industries Blog*, February 7, 2018, https://www.ibm.com/blogs/industries/little-known-story-first-iot-device/.
[2] James Manyika et al., *Unlocking the Potential of the Internet of Things* (New York: McKinsey Global Institute, June 2015).
[3] Adam Thierer and Andrea O'Sullivan, "Projecting the Growth and Economic Impact of the Internet of Things," Economic Perspectives, Mercatus Center at George Mason University, June 15, 2015.

For more information, contact
Mercatus Outreach,
Mercatus Center at George Mason University
3434 Washington Blvd., 4th Floor, Arlington, VA 22201

The ideas presented in this document do not represent official positions of the Mercatus Center or George Mason University.

Like many products, the IoT can be leveraged for beneficial or harmful ends. For example, botnets that harness the distributed computing power of connected devices may be used to disrupt major websites; yet the same technology may be used to raise money for charities or perform medical research.[4] Similarly, while software is key to the success of the digital economy, malware may damage computer systems. Thus, policymakers approaching the IoT must focus on preventing botnets and malware while avoiding efforts that make beneficial uses of software more difficult.

Our comments will emphasize developing a comprehensive, long-run approach to achieving a resilient IoT ecosystem. Resilience is the capacity to persist, adapt, learn, and recover from an adverse event. We argue below that a multistakeholder approach to the governance of the IoT is best suited to the dynamism and complexity of this ecosystem. By multistakeholder approach, we mean governance that involves government agencies as well as manufacturers, industry organizations, advocacy groups, researchers, and consumers in key decision-making. Focusing on resilience will minimize the safety risks associated with flaws or malfunctions in cyber-physical systems while promoting innovation in the consumer market.

THE LIMITATIONS OF RULEMAKING IN THE IOT ECOSYSTEM

The IoT is an array of connected, uniquely identified objects that are able to transfer data over a network.[5] These objects include emerging technologies such as smart speakers, autonomous vehicles, and drones, as well as more mature technologies such as smartphones and security cameras. There is a huge amount of variety in these devices. For example, not all IoT devices have sensors, but many do. Some devices are "always-on" (always connected to the internet), whereas some are intermittently connected. Some devices communicate only locally, whereas others have access to a larger network. Devices can be intended for consumer, industrial, or military use. Finally, devices can have intangible (digital) or tangible (physical) effects. Because of the variety in the IoT, a one-size-fits-all regulatory approach has a high potential for creating unintended consequences that hamper IoT development.

The breadth of the IoT ecosystem makes rulemaking and regulation regarding basic device design standards, certification programs, or required technical criteria particularly risky. It is important to understand the secondary effects of pursuing new requirements. Design standards can solidify inadequate or overly complex requirements and introduce costs that deter IoT innovation by redirecting labor and resources toward meeting regulatory compliance. In contrast, voluntary performance standards specify a desired outcome as opposed to dictating the way to achieve that outcome.[6] Performance standards more effectively align the incentives of companies and regulators because they reward activities directed at achieving security rather than specific compliance tasks that may or may not actually reach security goals.

---

[4] Charity Engine, "About Us," accessed June 1, 2018, http://www.charityengine.com/about; Folding@Home, home page, accessed June 1, 2018, http://folding.stanford.edu/.

[5] Anne Hobson, "Aligning Cybersecurity Incentives in an Interconnected World" (R Street Institute Policy Study No. 86, R Street Institute, Washington, DC, February 2017).

[6] David Hemenway, *Performance vs. Design Standards* (Washington, DC: US Department of Commerce, National Bureau of Standards, October 1980), 1–35.

It is important to be specific about the devices to which safety standards apply. For example, the state legislature of California proposed an early draft of a bill targeting all IoT devices that required manufacturers to "design the device to indicate when it is collecting information."[7] However, for always-on devices such as autonomous vehicles, smartphones, or digital assistants, this indicator loses its meaning. IoT devices fall into dozens of overlapping categories depending on the prevalence of certain features and differences in use cases. Furthermore, use cases may change over time. For example, smartphones are cameras and recording devices, and are even becoming personal assistants. Home assistants may now serve predominantly as timers, music players, and online shoppers, but will soon commonly be connected with HVAC systems, doorbells, and laundry machines. The changing landscape of use cases and potential threat vectors can cause standards to be easily outdated.

A truly resilient IoT ecosystem requires that stakeholders have the ability to adapt and learn from failures and mistakes. Compliance tasks resulting from poorly implemented standards or certifications can introduce complacency, foster a false sense of security in the face of evolving threats, and compromise an organization's or individual's ability to learn how to recover from and respond to threats.

In order to meet the challenge of large-scale cyber insecurity, federal agencies should empower stakeholders at multiple levels to persist in their efforts to develop and adopt new technologies, and these agencies should not be deterred by cybersecurity threats and attacks. Industry groups and agencies should constantly update guidelines to adapt to emerging threats. Small and large manufacturers should invest in cyber insurance and adhere to the National Institute of Standards and Technology (NIST) guidelines to manage risk. Consumers groups can develop certification programs and can complement agencies in educating consumers about cyber threats. In general, federal agencies should empower stakeholders by giving them the space to develop solutions.

For systems to endure and function under and after cyberattacks, stakeholders must be able to have at their disposal multiple pathways of response so that no single vulnerability disrupts the operation of the entire system. In order to allow for those multiple pathways of response to be available, a multifaceted approach to governance should include industry-led standards, voluntary certification programs, cyber-insurance adoption, increased use of guarantees and warranties, and education of consumers.

Some cybersecurity solutions in the IoT already exist and are pursued by federal agencies, international bodies, industry groups, and third parties. In 2016, Underwriters Laboratories launched a Cybersecurity Assurance Program,[8] providing certifications to products that meet testable criteria. Voluntary premarket or postmarket certifications can also provide consumers with the necessary certainties to make informed choices about what devices they purchase and promote best practices within the industry. This has been seen in other industries, such as with the Green Building Initiative.[9]

---

[7] S.B. 327, 2018 Leg., 2017–18 Sess. (Cal. 2018).

[8] UL, "UL Launches Cybersecurity Assurance Program," news release, April 5, 2016, https://www.ul.com/newsroom/pressreleases/ul-launches-cybersecurity-assurance-program/.

[9] John J. Kirton and Michael J. Trebilcock, eds., *Hard Choices, Soft Law: Voluntary Standards in Global Trade, Environment, and Social Governance* (London: Routledge, 2004); US Green Building Council, "About USGBC," accessed June 1, 2018,

Efforts also include the development of flexible guidelines such as the NIST Cybersecurity Framework,[10] the Online Trust Alliance's Trust Framework,[11] and 30 other standards of varying technical specificity and focus from groups such as the International Organization for Standardization, Institute of Electrical and Electronics Engineers, and the Internet Engineering Task Force.[12] The NIST framework provides a common language for cybersecurity risk management. It characterizes the various levels of investment in cybersecurity that organizations currently adopt to manage threats—ranging from simple awareness to having adaptive systems. The framework also groups specific implementation measures across five large risk-management functions: identifying threats, protecting systems, detecting threats, responding to threats, and recovering from attacks. The CPSC should be involved with efforts to update and expand the NIST framework and encourage its adoption among manufacturers of consumer products. Furthermore, rather than starting its own certification program or standards efforts, the CSPC should collaborate with entities already pursuing solutions to cyber insecurity. For example, the Consumer Technology Association (CTA) created a security checklist for sellers and manufacturers of household connected devices.[13] These groups have already developed industry practices and norms that should be considered in any potential regulatory or guidance-related measures. The CPSC can work with industry groups to create voluntary guidelines or checklists for vendors that focus specifically on implications for physical safety in the IoT ecosystem. Working with such groups would produce positive collaborative consensus for consumer safety.

The CPSC should also encourage industry adoption of a growing range of cyber insurance offerings. The process of acquiring cyber insurance involves cyber risk assessments. The insured parties are incentivized to become aware of vulnerabilities and put basic cyber practices in place to receive lower premiums.[14] Basic cyber practices can include shipping devices with up-to-date software, allowing users to change device passwords, employing strong authentication and cryptography best practices, and testing device configurations.[15] Currently, the manufacturing sector lags the healthcare and financial services sectors in insurance uptake.[16]

The IoT is a complex and ever-changing global ecosystem. The role of the CPSC and other agencies in addressing cyber insecurity is to foster the ecosystem's ability to adapt and learn. This requires an approach that emphasizes resilience as the end goal.

---

https://new.usgbc.org/about; Marine Stewardship Council, "Sustainable Seafood: The First 20 Years: A History of the Marine Stewardship Council," accessed June 1, 2018, http://20-years.msc.org/.

[10] National Institute of Standards and Technology, "Cybersecurity Framework," accessed June 1, 2018, https://www.nist.gov/cyberframework.

[11] Online Trust Alliance, "OTA Releases IoT Trust Framework," press release, March 2, 2016, https://otalliance.org/news-events/press-releases/ota-releases-iot-trust-framework.

[12] National Telecommunications and Information Administration, Existing Standards, Tools and Initiatives Working Group, *Catalogue of Existing IoT Security Standards*, n.d.

[13] Consumer Technology Association, "Device Security Checklist," accessed June 1, 2018, https://www.cta.tech/Membership/Member-Groups/TechHome-Division/Device-Security-Checklist.aspx.

[14] Hobson, *Aligning Cybersecurity Incentives.*

[15] Broadband Internet Technical Advisory Group, *Internet of Things (IoT) Security and Privacy Recommendations: A Broadband Internet Technical Advisory Group Technical Working Group Report*, November 2016.

[16] Council of Insurance Agents and Brokers, *Cyber Insurance Market Watch Survey: Executive Summary*, 2017.

FAVORING A RESILIENCE APPROACH RATHER THAN A PRECAUTIONARY APPROACH

The CPSC should take an approach that encourages and collaborates with existing efforts to make the IoT ecosystem more secure. The resilience approach to the IoT requires bottom-up, distributed efforts from all stakeholders. It recognizes that IoT technology improves existing consumer products but also improves safety overall.[17] These devices will promote an overall improvement in the safety and standard of living for many and will be able to develop more quickly in the absence of unnecessary regulatory barriers.[18] In general, the common law and consumers should be left to determine the appropriate level of safety in products on the market. Regulatory intervention should be reserved for those cases where the harm is highly probable, tangible, immediate, irreversible, and catastrophic.[19] It is highly unlikely that consumer IoT devices would result in this type of harm.

To date, we could not find recorded incidents of the use of household consumer products resulting in physical harm to consumers or their property as a result of their internet-connected nature. While the potential for consumer products causing physical harm to consumers or their property has been demonstrated in closed settings,[20] a precautionary approach involving new security baselines or certification program is not necessary at this point, and it could in fact prove harmful. This is especially true for IoT products where an overabundance of caution may result in establishing a duty that would not have otherwise existed.

Furthermore, current CPSC standards, including ASTM F963, and existing regulations, such as the Children's Online Privacy Protection Act, already prevent against hazards resulting from inadequate safety and data security protections for connected toys and devices marketed to children.[21] The CPSC must resist the urge to develop a "theory of everything" that would trade innovation for a false sense of having avoided risk. Instead, it should embrace a ground-up development of best practices and pursue additional actions only on a case-by-case basis and limited to the narrow applications necessary.

The CPSC should embrace an approach that emphasizes innovation and encourages self-governance. In a policy environment that promotes resilience as an end goal, creators are likely to develop safety processes and measures that appeal to consumers' actual preferences and not merely their expressed ones. For example, many consumers say they value their privacy, but few choose to change their behavior or take additional steps to protect information they reveal online.[22] Consumers select different blocking and screening technologies for websites, and similar features are developing in the IoT market. Consumers exhibit many different safety and security preferences. The CPSC should consider that despite consumers expressing a desire for increased

---

[17] Geoff Wheelwright, "IoT-Linked Wearables Will Help Keep Workers Safe," *Financial Times*, October 17, 2017.
[18] Cliff Saran, "Realising the Benefits of a Totally Connected World," *Computer Weekly*, December 2013.
[19] Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (Arlington, VA: Mercatus Center at George Mason University, 2014), 4.
[20] Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—with Me in It," *Wired*, July 21, 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
[21] ASTM International, "ASTM F963 - 17: Standard Consumer Safety Specification for Toy Safety," accessed June 1, 2018, https://www.astm.org/Standards/F963.htm; Federal Trade Commission, "Children's Online Privacy Protection Rule ("COPPA")," accessed June 1, 2018, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.
[22] Tom Hall and Kathleen Cahill, "The Privacy Paradox: We Say We Value It. What We Do Online Suggests Otherwise," *WYPR*, May 9, 2017.

privacy, they are often unwilling to deal with the accompanying inconveniences.[23] As a result, it is important to consider limiting the number of default requirements to truly catastrophic cases, and instead encouraging the development of optional privacy and security settings that consumers may opt into or out of as fits their needs.[24]

The CPSC should participate in existing multistakeholder processes for developing standards and certifications. Initiatives that include industry representatives, regulators, and consumer groups will ensure that the technology is developed in a way that preserves the desired consumer experience. In general, a soft-law, multistakeholder approach is more likely to result in the desired results without sacrificing the potential development of better, safer products for consumers.[25] Soft law refers to informal and flexible rulemaking, as opposed to the strict, formal rules of statutes and administrative regulations. Because of the tentative and provisional nature of soft law, regimes governed by soft law allow a wider variety of methods to be proposed and tested, resulting in systems that are less uniform, more decentralized, and less vulnerable to systemic threats.[26]

CPSC'S ROLE AS A CONSUMER EDUCATOR

We believe there is a role for the CPSC in educating and empowering consumers. When physical harm does occur, the CPSC can draw attention to recalls. The CPSC can also work with the affected company to leverage the IoT to notify consumers of the nature of the harm through push notifications or other forms of notice. It is important to focus on identifiable IoT-related harms rather than potential or hypothetical harms to avoid warning fatigue or unnecessary precaution. In this way, the IoT can be a boon for getting critical information to consumers.

There is also a growing set of IoT devices and services intended to mitigate some of the common problems with other consumer IoT devices. For example, smart firewalls and routers can track network traffic within a home, identifying malware or flagging patterns in traffic that reflect malicious botnet activity.[27] Larger consumer awareness of these products could improve baseline cybersecurity and hold manufacturers responsible. Online feedback mechanisms such as product reviews and ratings are already effective ways consumers and consumer groups can warn others about flawed products. Similarly, brands and reputations will develop over time. Increased use of warranties and guarantees related to cybersecurity can help boost consumer trust and provide a mechanism to hold manufacturers accountable.[28]

Consumers, when they know about poor data security practices, can be effective advocates for change. For example, after a DDoS attack in November 2016 in which the Mirai malware infected hundreds of thousands of IoT devices, the Chinese company responsible for manufacturing the webcams implicated in the attack voluntarily recalled millions of insecure devices to avoid the

---

[23] Alan McQuinn, "The Economics of 'Opt-Out' versus 'Opt-In,'" *Innovation Files*, October 6, 2017.
[24] McQuinn, "The Economics of 'Opt-Out' versus 'Opt-In.'"
[25] Ryan Hagemann, Jennifer Skees, and Adam Thierer, "Soft Law for Hard Problems: The Governance of Emerging Technology in an Uncertain Future," *Colorado Technology Law Journal* (forthcoming).
[26] Hagemann, Skees, and Thierer, "Soft Law for Hard Problems."
[27] Anne Hobson, "Cybersecurity in the Internet of Things Is a Game of Incentives," *The Hill*, Jan 19, 2017.
[28] Anne Hobson and James Czerniawski, "What the Internet of Things Can Learn from Used Cars," *Real Clear Future*, July 17, 2017.

scorn of the public and other entities.[29] We believe that the CPSC can play a complementary role in helping to inform consumers of incidents and recalls when necessary.

UTILIZING MULTISTAKEHOLDER PROCESSES AND OTHER COLLABORATIVE GOVERNANCE AS AN ALTERNATIVE TO TRADITIONAL REGULATION

As part of an overall approach to fostering resilience against cyber threats in IoT technologies, the CPSC should consider continuing the collaborative governance, or soft law mechanisms, rather than a more formal hard law approach of mandatory rules and restrictions. The CPSC can follow the example and collaborate with agencies like the Federal Trade Commission (FTC), the Food and Drug Administration (FDA), NIST, and National Telecommunications and Information Administration (NTIA), which have already worked with industry innovators and civil society leaders to develop informal standards and norms on topics like privacy and security. On the potential for malfunction related to IoT devices that include radios, the CSPC should communicate with the Federal Communications Commission (FCC). The Department of Homeland Security (DHS) plays a critical role in coordinating cybersecurity efforts across the federal government with a focus on risk management and resilience.[30] By focusing on collaborative, informal processes that are adaptive to new innovations in this space, the CPSC will be more likely to create an environment that allows consumers access to safe products without sacrificing innovation.

The FTC and NTIA have already conducted multistakeholder processes related to IoT devices and have generated best practices and norms through which the private sector has been able to engage in self-regulation to a large degree, with the government minimally formalizing the norms that emerge from such discussions.[31] NTIA's green paper on IoT development defines an appropriate role for government as supporting emerging technologies.[32] As the Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team pointed out in a 2017 green paper, the framework of allowing the private sector to lead in technology advancement and engage in collaborative processes when needed should work well for the IoT, as it did for the development of the original internet.[33] The CPSC should work collaboratively with these departments that have already engaged in collaborative discussions on these issues, rather than issue additional requirements that may result in fewer of the products or innovations that might actually make the technology safer for consumers.

Existing working groups at the NTIA have already established best practices for a wide variety of issues such as security upgradability and patching of devices.[34] The CPSC should draw on these

---

[29] Michael Mimoso, "Chinese Manufacturer Recalls IoT Gear Following Dyn DDoS," *Threat Post*, October 24, 2016.
[30] US Department of Homeland Security, *Cybersecurity Strategy*, May 15, 2018.
[31] Federal Trade Commission, *Internet of Things: Privacy and Security in a Connected World*, January 2015; National Telecommunications and Information Administration, "Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching," November 7, 2017, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security; Hagemann, Skees, and Thierer, "Soft Law for Hard Problems."
[32] US Department of Commerce, Internet Policy Task Force & Digital Economy Leadership Team, *Fostering the Advancement of the Internet of Things*, January 2017.
[33] Internet Policy Task Force & Digital Economy Leadership Team, *Fostering the Advancement of the Internet of Things*, 11; Ryan Hagemann, "Green Paper: Fostering the Advancement of the Internet of Things" (Public Interest Comment, Niskanen Center, Washington, DC, February 8, 2017).
[34] 81 Fed. Reg. 64139 (September 19, 2016).

groups' recommendations in determining if any further safety or security is necessary. These working groups have shown an ability to focus on both industry and consumer needs in a way that is able to dive deeper and result in more practical consensus than a top-down regulatory approach would. Additionally, the reliance on working group recommendations as opposed to harsher, more formalized rulemaking allows for such recommendations to more easily account for new concerns or adapt to changes in other regulatory schemes or issues.

Generally these groups are able to engage in a more democratic process that results in a voluntary, self-regulatory format that balances private industry interests with the government's desire to protect the public interest.[35] These processes also insure that regulatory bodies are able to learn from expertise in the industry rather than relying on their own internal and often outdated knowledge of the industry.

Approaching these problems through a soft law, collaborative governance framework does not mean that other policy mechanisms shouldn't exist. Consumer smart products are subject to the same safety standards as their nonsmart counterparts; likewise, they are subject to the FTC Section 5 unfair and deceptive trade practice standards for their claims. The FTC took D-Link to court for shipping routers and internet cameras with default passwords despite their claims of advanced network security.[36] With these existing standards in mind, the CPSC should consider the potential for conflicting regulation to give rise to uncertainty and result in less innovation and lower-quality products.[37]

LIABILITY QUESTIONS IN CONSUMER SAFETY AND THE IOT

Not only are consumer products already subject to safety regulations and requirements through other agencies, there are already safety standards for most traditional products now connected via the IoT. Additionally, the common law surrounding product liability provides certain de facto regulations, owing to the threat of liability should a problem arise.[38] Unless the introduction of an IoT element fundamentally changes a product by increasing or decreasing the safety, then it is unlikely additional safety standards need generally be established. The CPSC should avoid establishing broad regulations that do not account for the diversity of technologies captured by the term "internet of things." At the same time, the CPSC must also be careful not to regulate too narrowly and target a useful technology before its potential advantages are known.

In most cases, the CPSC should allow common-law products liability to apportion fault. If the CPSC or other regulators step in, it should be to limit the liability of internet-enabled devices for injuries that are not caused by the innovation but by a more traditional product. In determining whether the internet-connected element is associated with the injury, the CPSC should look at whether the injury would have occurred without the connected element. In such situations, the responsibility and liability should rest only on the traditional product. The CPSC has experience

[35] Hagemann, Skees, and Thierer, "Soft Law for Hard Problems."
[36] Federal Trade Commission, "FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras," press release, January 5, 2017, https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate.
[37] Philip K. Howard, "Radically Simplify Law," *CATO Online Forum*, November 12, 2014.
[38] Alexandra B. Klass, "Tort Experiments in the Laboratories of Democracy," *William and Mary Law Review* 50 (2009): 1508–9.

making such distinctions between component parts and the finished product for other consumer products that use new technologies.[39]

When adding a third-party internet-enabled element to an existing product, the original product manufacturer should simultaneously be relieved from liability for any harm caused by the device and should not be held responsible for violations of existing standards that were caused by the technology and not the original product. Many states have adopted substantial modification as a defense to products liability claims, and the CPSC's regulations should follow suit.[40]

To effectively protect consumer safety, the CPSC must be careful that any safety regulations regarding IoT devices address only the part actually at risk of causing harm. Rather than raising the regulatory burden on both standard and IoT devices, the CPSC should consider lowering burdens on all devices as technological advances make them safer.[41]

CONCLUSION

We applaud the CPSC's efforts to examine questions about the safety of connected devices as this technology rapidly evolves, and to consider the framework that will encourage consumer trust in these new products' safety while still encouraging innovation in this area. We encourage the CPSC to take a flexible approach that fosters resilience, respects the complexity and dynamism of the IoT, and embraces a multistakeholder process. The CPSC should draw on the recent experiences of other bodies interacting with IoT technology and carefully consider if any additional regulations would improve consumer safety.

The CPSC is unique in its focus of communicating with consumers about harms associated with consumer devices. Accordingly, the CSPC should leverage IoT technology to educate and empower consumers about incidents of physical harm or product recalls. In this rapidly changing field, a flexible approach that minimizes bureaucratic requirements is likely to achieve results that protect both consumers and innovation. The right policy environment will allow a wide set of solutions to evolve, improving cybersecurity and safety outcomes for consumers of internet-connected products.

---

[39] Conditions and Requirements for Relying on Component Part Testing or Certification, or Another Party's Finished Product Testing or Certification, to Meet Testing and Certification Requirements, 16 C.F.R. 1109 (2012).
[40] Jones v. Hittle Services, 549 P.2d 1383 (1976).
[41] Adam Thierer, "Converting Permissionless Innovation into Public Policy: 3 Reforms," *Plain Text*, November 29, 2017.

Free markets. Real Solutions.

Before the
National Telecommunications and Information Administration
Washington, D.C.

In the Matter of	)	Docket No. 170105023-7023-01
	)	
The Request for Comments	)	82 Fed. Reg. 4313
On the Benefits, Challenges,	)	
and Potential Roles	)	
for the Government	)	
in Fostering the	)	
Advancement of	)	
The Internet-of-Things	)	

COMMENTS OF
THE R STREET INSTITUTE

March 13, 2017

Prepared by:
Anne Hobson
Technology Policy Fellow
R Street Institute
1050 17th St NW #1150, Washington DC, 20036

Introduction

On behalf of the R Street Institute, we respectfully submit these comments in response to the National Telecommunications and Information Administration (NTIA) request for comments on the benefits, challenges and potential roles for the government in fostering the advancement of the internet-of-things.[1] The R Street Institute is a free-market think tank with a pragmatic approach to public policy challenges.

We thank NTIA for the opportunity for further comment on this important emerging technology. The Department's green paper sets the appropriate tone by framing NTIA's role as one of support and encouragement of emerging technology.[2] While we will comment broadly on the role of the Department of Commerce ["Department"] in advancing a light-touch regulatory approach to the internet-of-things, our comments focus on our areas of expertise, including cybersecurity and user privacy. With this focus in mind, the below sections define the unique challenges and benefits the internet-of-things poses, outline the role for government (question 1), comment on areas of engagement (question 2) and detail how the Department should engage to advance the development of the internet-of-things (questions 3-4).

I. Benefits and Challenges in Internet-of-Things Development

As NTIA's green paper points out, the internet-of-things is challenging to define. Broadly, the "internet-of-things" is an array of connected objects with unique identifiers that have the ability to transfer data over a network.[3] These technologies have exciting applications in the fields of infrastructure, agriculture, energy, transportation, manufacturing, health and communications and more. According to McKinsey & Company, global internet-of-things adoption could generate between $3.9 and $11.1 trillion per year by 2025, equivalent to up to 11 percent of the global economy.[4] Internet-of-things devices can streamline routines and chores. They can leverage sensors and data to smooth traffic flows or signal when infrastructure need repairing. The combined scale, scope and interconnectivity can lead to economic growth and increases in productivity and prosperity. Yet, these features also present unique challenges.

---

[1] Department of Commerce, National Telecommunications and Information Administration, "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things," Request for Public Comment, Federal Register, Vol. 82, No. 9, January 13, 2017. https://www.ntia.doc.gov/files/ntia/publications/fr_iot_notice_rfc_01132017.pdf

[2] Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, "Fostering the Advancement of the Internet of Things," January 2017. https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

[3] Anne Hobson, "Aligning Cybersecurity Incentives in an Interconnected World," R Street Institute Policy Study No. 86, February, 2017. http://www.rstreet.org/policy-study/aligning-cybersecurity-incentives-in-an-interconnected-world/

[4] James Manyika, et al., "Unlocking the Potential of the Internet of Things," McKinsey Global Institute, June 2015. http://www.mckinsey.com/business-functions/digitalmckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physicalworld

Because of network effects, one device's vulnerability can become a problem for the entire network. Malware can infect vulnerable internet-of-things devices, form a botnet and organize distributed denial of service (DDoS) attacks to bombard websites or service providers with traffic. Such attacks can result in costly internet outages. The average DDoS attack can cost $500,000 for a firm.[5] Furthermore, the internet-of-things can be an avenue for physical attacks, cyber espionage, eavesdropping, data exfiltration or other attacks on our private data.[6] The consequences of device vulnerabilities are magnified by interconnectivity. Combating issues related to cybersecurity and privacy will require efforts from industry, policymakers, consumers and third parties. The Department can play a role in improving security outcomes by supporting market solutions and adopting a light-touch regulatory approach.

II. Role for Government

In addressing question 1,[7] we believe there is a role for the Department in supporting market-based mechanisms to addressing challenges in privacy and cybersecurity related to the internet-of-things. These market-based mechanisms should include private certification programs, industry-led information-sharing efforts, after-market solutions such as smart-routers and efforts to promote cyber-insurance adoption.

Health care, manufacturing, financial services, government and transportation were the top five industries that fell victim to cyber-attacks in 2015.[8] Some of these industries are more equipped to handle cyber risk. For example, the cyber-insurance take-up rate in the retail, health and financial services sectors is around 80 percent; however, less than 5 percent of the manufacturing sector has cyber-insurance coverage.[9] Cyber-insurance helps companies reflect on risks and plan for them and it aligns the incentives of insurers with the insured. Insurers perform risk assessments to ensure that the premium will cover the risk. Companies that demonstrate preparedness can get lower premiums.

The government is a high-profile cyber target with access to sensitive data about citizens. It is also a large buyer of internet-enabled devices. The Department can use this purchasing power to award contracts to internet-of-things contractors that emphasize data protection. It can also urge other federal entities to do the same.

---

[5] Incapsula, "Survey: What DDoS Attacks Really Cost Businesses," pp. 1-9, 2014. https://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20 Impact%20Survey.pdf

[6] Mohamed Abomhara and Geir M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," Journal of Cyber Security, Vol. 4, pp. 65-88, May 22, 2015. http://riverpublishers.com/journal/journal_articles/ RP_Journal_2245-1439_414.pdf

[7] Question 1) Is our discussion of IoT presented in the green paper regarding the challenges, benefits, and potential role of government accurate and/or complete? Are there issues that we missed, or that we need to reconsider?

[8] IBM X-Force Research, "IBM 2016 Cyber Security Intelligence," 2016. http://www-03.ibm.com/security/data-breach/cyber-security-index.html

[9] Council of Insurance Agents and Brokers, "cyber-insurance Market Watch Survey," October 2016. https://www.ciab.com/uploadedFiles/Resources/Cyber_ Survey/102016CyberSurvey_Final.pdf

One way to encourage cyber preparedness among contractors is to require contractors to demonstrate financial responsibility over the cyber risk they pose to the federal government. In this way, the Department can play a role in supporting broader adoption of cyber-insurance coverage to mitigate risks associated with cyberattacks. The Department can set an example as a market participant by signaling to industry that it is serious about encouraging cyber-insurance adoption to improve cybersecurity nationwide. Regulatory efforts that rely on market-based incentives such as cyber-insurance can have better, longer-lasting results than other legislative approaches.

We commend NTIA for following the approach detailed in the 1997 Framework for Global Electronic Commerce.[10] This framework reinforces the importance of industry-led policies and defines government's role as fostering that development. In the green paper, NTIA recognizes the danger of inconsistent or unpredictable regulation and acknowledges the importance of letting companies experiment.[11] Promoting an open global environment for internet-of-things development is key to realizing the benefits of this technology.

As this technology matures, the Department should pursue a light-touch regulatory approach to the internet-of-things. Because devices are diverse in functionality and nature, one-size-fits-all regulation based on design standards is bound to have deleterious effects. Design requirements risk being overly complex or inadequate and would be difficult to change over time once they are applied. Moreover, compliance costs with such requirements could deter internet-of-things innovation. Lastly, such requirements would crowd out private efforts to improve cybersecurity and privacy at the industry and firm level.

Any requirements should be as narrowly focused as possible and should emphasize performance standards rather than design standards. Performance standards specify the desired outcome of a policy while allowing companies the flexibility to identify the best means or design to achieve it.[12] By contrast, design standards specify the manner in which the outcome is achieved. NTIA should refrain from constructing restrictive regulatory regimes, while seeking out ways to encourage firms to share threat information, promote cyber-insurance adoption, encourage private efforts to recognize security-conscious products with certifications, develop and adopt best practices voluntarily and reward innovative after-market approaches to policy issues such as cybersecurity and privacy.

The internet-of-things is a complex system. There is no simple regulatory fix. Instead, industry, governments, consumers and third party stakeholders will have to work together to improve security and privacy outcomes. NTIA should continue to play the role of convening stakeholders and encouraging discussion around issue areas such as cybersecurity and privacy.

---

[10] The Framework for Global Electronic Commerce (July 1997), https://clinton4.nara.gov/WH/New/Commerce/.

[11] Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, "Fostering the Advancement of the Internet of Things," January 2017, page 14. https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

[12] David Hemenway, "Performance vs Design Standards," U.S. Department of Commerce, NIST, pp. 1-35, October 1980. http://gsi.nist.gov/global/docs/pubs/NISTGCR_80-287.pdf

III. Areas of Engagement and Next Steps

The approach detailed for departmental action includes appropriate areas of engagement; however, to address questions 2 and 3,[13] there are specific opportunities for engagement that should be included. For example, the green paper argues the Department can play a role in encouraging risk-based approaches. One of these risk-based approaches should be promoting cyber-insurance adoption. The Department can encourage cyber-insurance adoption and risk mitigation among the vendors with whom it contracts.

In the section "Proposed Next Steps," NTIA suggests the Department can "leverage its role as an internet-of-things consumer to promote a market for secure internet-of-things technologies and the supply chains supporting those technologies."[14] In answer to question 4,[15] we propose the Department can achieve this goal by introducing a financial responsibility requirement in its contracts with internet-of-things device vendors to transfer the financial and operational risks of cyber-attacks. This will help companies recover and prevent high vendor turnover due to a cyberattack. It will promote cyber-insurance adoption more broadly, helping to immunize the entire internet-of-things ecosystem from cyberattacks. Moreover, it will encourage market growth for risk-based products and increase the availability and affordability of insurance products. Such an approach would signal to industry that the Department is serious about bolstering the nation's cyber preparedness in light of the unique challenge posed by the internet-of-things.

Conclusion

We are encouraged by NTIA's efforts so far to understand the internet-of-things, engage stakeholders and develop a constructive policy approach. There is a role for the Department of Commerce to support market-based solutions to cybersecurity and privacy concerns related to the internet-of-things. We look forward to continuing to engage with the Department on this topic.

Respectfully submitted,
Anne Hobson
Technology Policy Fellow
R Street Institute

---

[13] Question 2) Is the approach for Departmental action to advance the internet-of-things comprehensive in the areas of engagement? Where does the approach need improvement?
Question 3) Are there specific tasks that the Department should engage in that are not covered by the approach?

[14] Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, "Fostering the Advancement of the Internet of Things," January 2017, page 54.
https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

[15] Question 4) What should the next steps be for the Department in fostering the advancement of IoT?

Free markets. Real solutions.

R STREET POLICY STUDY NO. 86
February 2017

ALIGNING CYBERSECURITY INCENTIVES IN AN INTERCONNECTED WORLD

Anne Hobson

CONTENTS

Introduction 1
State of the internet of things 3
Federal approach to cybersecurity policy 4
Growing cybersecurity risk in the internet of things 6
Case for a light-touch regulatory approach 7
Market solutions 8
Cyber insurance 8
Filling the information gap 10
Cyber insurance for federal vendors 11
Conclusion 12
About the author 13

INTRODUCTION

In the stop-motion animated short "Wallace & Gromit: The Wrong Trousers," the protagonist Wallace's alarm clock kicks off a Rube Goldberg-like chain of machines and devices that dress him and make him breakfast. The so-called "internet of things" is set to make this sort of fiction a reality. Connected homes, appliances and infrastructure have the potential to make us more productive. Today, you can set your alarm clock remotely and have it signal your coffee maker to start and the water heater to get your shower ready.

The term "internet of things" dates to 1999, when the founders of the Massachusetts Institute of Technology's Auto-ID Labs began using it to describe a class of identification technologies used in automation processes.[1] The actual technologies are significantly older. It's believed the computer science department at Carnegie Mellon University programmed the first internet-connected device—a Coca-Cola vending machine—in the mid-1970s.[2] As the story goes, the department installed microswitches to sense whether bottles were present in the machine, with that information relayed to a server that students could access from anywhere on the internet.

Though the term has been with us nearly two decades, there remains significant disagreement about what, precisely, the "internet of things" describes. Since its inception, it has been used alternatively to include or exclude various classes of connected objects. Key to its global spread was a 2005 report by the United Nations' International Telecommunication Union that characterized the internet of things as "ubiquitous computing," complete with machine-to-machine communication and real-time connectivity.[3] In the United States, the Federal Trade Commission has adopted a definition that hinges on whether or not a given class of objects traditionally had embedded computing power; networked appliances and thermostats thus qualify as internet-of-things devices, but computers, tablets and smartphones do not.[4] The management consultant McKinsey & Co. employs a definition that also excludes computers and smartphone apps, on grounds that they are designed to receive intentional human input.[5] The Institute of Electrical and Electronics Engineers defined the internet of things as "a network of items—each embedded

1. Gérald Santucci, "The Internet of Things: Between the Revolution of the Internet and the Metamorphosis of Objects," European Commission, 2010. https://pdfs.semanticscholar.org/adb7/03eb4c53ccba53a8973fbff2f30563363a58.pdf

2. Carnegie Mellon University Computer Science Department, "The Only Coke Machine on the Internet," https://www.cs.cmu.edu/~coke/history_long.txt

3. International Telecommunication Union, "The Internet of Things," *ITU Internet Reports*, 2005. https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf

4. Federal Trade Commission, "Internet of Things: Privacy and Security in a Connected World," FTC Staff Report, January 2015. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

5. James Manyika, et al., "Unlocking the Potential of the Internet of Things," *McKinsey Global Institute*, June 2015. http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

with sensors—which are connected to the internet."[6] The U.S. Commerce Department's National Institute of Standards and Technology (NIST)—recognizing there is no universally agreed-upon definition—defines internet-of-things devices by the presence of certain behavioral features: a sensing function, an aggregating function, a communications channel and a decision trigger.[7]

For the purposes of this paper, we use the term "internet of things" to refer to an array of connected objects with unique identifiers that have the ability to transfer data over a network. The internet of things consists of a variety of network-enabled physical objects, including appliances, objects using near-field communications, machine components, sensors, endpoints, wearables, computers and phones. That being said, we recognize that objects that are tagged with unique identifiers, but are not "smart," in that they do not have the ability to both send and receive data, present less cybersecurity risk. Conflating these things into one category can be problematic. Our definition approximates the category of objects included in the internet-of-things issues that policymakers will likely face.

The internet of things holds promise for applications in the fields of transportation, infrastructure, agriculture, energy, manufacturing, health and communications, among others. McKinsey predicts that internet-of-things adoption worldwide could generate between $3.9 and $11.1 trillion per year by 2025, equivalent to up to 11 percent of the global economy.[8] Internet-of-things devices can help monitor chronic conditions, such as diabetes. Smart homes made up of networked appliances can help to streamline routines and chores. Smart cities composed of networked infrastructure can smooth traffic flows and allocate energy more efficiently. Sensor-laden trash cans can signal when they need to be emptied, while sensors in bridges and roads can signal the need for repair.

For all the amazing potential of the internet of things to be realized, systems need to anticipate and design against vulnerabilities. The most common of these is a cyber-attack, a malicious attempt to access, damage or disrupt information or systems. To fend off potential attacks, internet-of-things devices and systems need to be equipped with appropriate cybersecurity defenses, which are designed to protect information systems from criminals, nation-states and unauthorized users.

Different aspects of connected devices pose different kinds and degrees of cybersecurity risk, with the internet-enabled features being the root source of most concerns. For example, there are privacy and surveillance implications associated with identifying technologies like RFID, as well as with "always-on" sensing capabilities.[9] Devices that interact directly with the physical world or that have clear real-world consequences can result in safety issues, as was seen in the recent hacks of the Ukrainian power grid.[10]

Because of the nature of network effects, internet-of-things devices present a unique problem to the internet as a whole. When devices are connected, one device's vulnerability becomes a problem for the entire network. This is not a new threat, as networked devices have been around since the 1960s. However, the scale of interconnection among today's devices magnifies the consequences of insecurity. Common vulnerabilities include insecure network services, software and firmware; insecure security configurability and authentication, authorization and verification systems; and insecure cloud, mobile and web interfaces.

The insecurity of the internet of things has helped to create the equivalent of an active warzone. Compromised devices can be organized into "botnets" that are used to disrupt internet service broadly in what are known as distributed denial of service (DDoS) attacks. Large-scale internet outages due to denial of service attacks are increasing in number and frequency.[11] Other types of internet-of-things-based attacks include physical attacks, reconnaissance attacks, access attacks and attacks on privacy, including data-mining, cyber espionage and eavesdropping, as well as tracking and password-based attacks.[12]

A massive Oct. 21, 2016 cyber-attack rendered popular sites such as CNN, Twitter and Netflix inaccessible worldwide.[13] That event prompted the U.S. House Committee on Energy and Commerce to convene hearings to understand the role

6. Roberto Minerva, Abyi Biru, and Domenico Rotondi, "Towards a Definition of the Internet of Things," IEEE Internet Initiative, May 2015. http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

7. Jeffrey Voas, "Network of 'Things'," NIST Special Publication 800-183, July 2016. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf

8. Manyika, 2015.

9. Gilad Rosner, *Privacy and the Internet of Things: Challenges and risks of connected devices*, O'Reilly Media, 2017. http://www.oreilly.com/iot/free/privacy-and-the-internet-of-things.html

10. Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

11. Arbor Networks, "Worldwide Infrastructure Security Report," 11: 1-115, 2016. https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf

12. Mohamed Abomhara and Geir M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," *Journal of Cyber Security*, Vol. 4, pp. 65-88, May 22, 2015. http://riverpublishers.com/journal/journal_articles/RP_Journal_2245-1439_414.pdf

13. Sara Ashley O'Brien, "Widespread Cyberattack Takes Down Sites Worldwide," CNN Money, Oct. 21, 2016. http://money.cnn.com/2016/10/21/technology/ddos-attack-popular-sites/

of connected devices in the internet disruption.[14] The outage was also at least partially responsible for the National Institute of Standards and Technology moving up the release date of the final draft of planned guidance to provide cybersecurity and mitigation resources for internet-of-things manufacturers.[15]

The pace of progress in creating effective cybersecurity protocols currently lags the speed with which internet-of-things systems are developing, but this does not always have to be the case. The risk of cyber-attack is becoming both more costly and more visible. Companies do not want the reputation or brand damage associated with selling insecure devices. As one recent example illustrates, the company responsible for the vulnerable webcams leveraged in the October 2016 Mirai botnet chose voluntarily to recall millions of devices.[16] Insecure internet-of-things devices cause negative externalities, as one individual's use of a vulnerable product can reduce the well-being of others within the network. Bruce Schneier—a fellow at Harvard University's Berkman Klein Center for Internet & Society—is among the prominent voices calling for government to intervene to correct this "market failure."[17]

However, if we turn Schneier's logic on its head, market failures can become market opportunities.[18] In other words, the absence of security is an opportunity for entrepreneurs to sell secure internet-of-things devices, make security cheaper to implement and to broker information about device security. Users currently are largely unaware of the negative effects of their insecure devices and companies are often unaware of vulnerabilities in their devices. Such information asymmetries offer opportunities for strong private mechanisms to evolve. Third-party accreditation organizations, standards organizations and ratings bodies can provide information to consumers about their products' security, just as the nonprofit Underwriters Laboratories certifies safe products with their "UL" mark.

Cyber insurance also can help the market to manage and transfer risk, and to internalize the negative externality through risk-based insurance premiums. Through the processes of cyber-insurance underwriting and ratemaking, manufacturers are offered incentives to become aware of vulnerabilities. So long as insurers remain free to craft new products and charge appropriate risk-based prices, and efforts are not made to displace private coverage with some kind of government "backstop," the market for cyber insurance should continue to develop rapidly. The federal government could help encourage the burgeoning market by requiring that federal internet-of-things contractors use insurance or other risk-transfer mechanisms to take financial responsibility for cyber liabilities they may create for taxpayers.

Given the challenge posed by an insecure internet of things, policymakers must avoid the knee-jerk response to institute regulations that require certain prescribed device-security standards. Government is limited in its cyber-security expertise and local knowledge, particularly given the complexity and speed of technological development, which make it impossible for lawmakers and regulators to know what type of requirements to impose. Because devices have unique functions, protocols and uses, one-size-fits-all regulation based on design standards would set inadequate or overly complex standards in stone, not to mention introducing compliance costs that could deter internet-of-things innovation. Overly prescriptive regulations also could limit companies' flexibility to respond to issues as they arise.

Because of potential pitfalls in a federal regulatory approach to internet-of-things standards, identifying market-based solutions is critical. This paper explores two market-based mechanisms—cyber insurance and third-party accreditation—that could help secure the internet of things. It also examines the role policymakers can play in supporting broader adoption of cyber insurance coverage.

STATE OF THE INTERNET OF THINGS

Depending on whether traditional human-interfacing devices like computers and smartphones are included in the definition, there currently are between 6.4 billion and 17.6 billion internet-of-things devices globally.[19] To put this in perspective, the world's population is around 7.3 billion people.[20] Projections for the number of connected devices in 2020 range from an estimate of 20.8 billion by the research firm Gartner Inc. to a 30.7 billion estimate from data analyst IHS Markit Ltd.

If manufacturer behaviors don't change, more internet-of-things devices could mean more potential attack vectors that

14. U.S. House Energy and Commerce Committee, "Understanding the Role of Connected Devices in Recent Cyber Attacks," Nov. 16, 2016. https://energycommerce.house.gov/hearings-and-votes/hearings/understanding-role-connected-devices-recent-cyber-attacks

15. Ron Ross, Michael McEvilley and Janet Carrier Oren, "Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," *Systems Security Engineering*, NIST Special Publication 800-160: 1-219, November 2016. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

16. Michael Mimoso, "Chinese Manufacturers Recalls IoT Gear Following Dyn DDoS," *Threat Post*, Oct. 24, 2016. https://threatpost.com/chinese-manufacturer-recalls-iot-gear-following-dyn-ddos/121496/

17. Bruce Schneier, "Regulation of the Internet of Things," *Schneier on Security*, Nov. 10, 2016. https://www.schneier.com/blog/archives/2016/11/regulation_of_t.html

18. Israel M. Kirzner, *Competition and Entrepreneurship*, rev. ed., Liberty Fund, 2010.

19. Amy Nordrum, "Popular internet of things Forecast of 50 Billion Devices by 2020 is Outdated," *IEEE Spectrum: Technology, Engineering, and Science News*, Aug. 18, 2016. http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated

20. U.S. Census Bureau, "U.S. and World Population Clock: Tell us what you think," accessed Feb. 9, 2017. https://www.census.gov/popclock/.

cyber criminals could exploit. According to research from Hewlett Packard Enterprise, 70 percent of the most common internet-of-things devices and infrastructure contain at least one security vulnerability.[21] Common vulnerabilities include lack of password security, insecure online user interfaces, inadequate encryption and overly broad user-access permissions. HPE's study found that 80 percent of internet-of-things systems did not require complex passwords and 70 percent did not encrypt data in transit.

The threat of proximate harm to owners of insecure internet-of-things devices is unknown. It is more likely that an individual will be the victim of a data breach. In 2015, cyber criminals accessed the records of 165 million Americans, roughly half the U.S. population.[22] In 2013, one in three victims of a data breach had their identity stolen. To date, the federal government's approach to address cyber risk has helped to move the conversation forward in three important ways: by facilitating development of voluntary cybersecurity standards, by helping address the lack of information about cyber incidents and by focusing on critical infrastructure.

FEDERAL APPROACH TO CYBERSECURITY POLICY

In 2013, then-President Barack Obama's Executive Order 13636 reignited a decadelong conversation on the role of government in cybersecurity.[23] The order instructed the National Institute of Standards and Technology to work with industry to develop voluntary cybersecurity standards to protect critical infrastructure, such as dams, electrical grids, financial institutions and transportation systems; asked the Department of Homeland Security to work with the private sector to develop an information-sharing program; and set goals for new hiring and training strategies for the cybersecurity workforce.[24] NIST's framework, originally released in February 2014 and updated most recently in January 2017, developed principles and best practices to help organizations manage, understand and communicate cyber risks. It highlighted five focus areas for cyber-planning, which it described as: identify, protect, detect, respond and recover.[25] It also included broad goals for technical outcomes, such as access control and data protection.

The framework is voluntary and compliance does not make companies immune from FTC enforcement actions. However, it appears from early surveys that companies that do not conform to the standards are more likely to be found liable after a cybersecurity incident.[26] Some industry associations have pushed back against further mandated technical standards for privacy or engineering, citing potentially duplicative or overly burdensome efforts.[27] Others have stressed the importance that the cybersecurity framework remain nonregulatory and voluntary, resisting any attempt by NIST to set compliance expectations for internet-of-things companies.[28]

Drawing on the NIST framework, DHS guidelines urge organizations to consider security during the system-engineering process, rather than the industry norm of adding firewalls, monitoring systems or applying encryption after the fact.[29] NIST also has published a guide for cybersecurity event recovery that stresses the importance of preparing cyber plans, policies and procedures.[30] These recommendations have implications for manufacturers of internet-of-things devices, as well as for networked infrastructure.

The Obama White House followed up Executive Order 13636 with Executive Order 13691 in 2015, which expanded the use of analysis organizations and information-sharing beyond critical infrastructure to any affinity groups that wanted to share threat information. In February 2016, Obama created the Commission on Enhancing National Cybersecurity, whose final report recommended public-private collaboration to address the internet of things as an area of special concern.[31] Action items included immediate collaboration between NIST and the internet-of-things industry to create voluntary standards organizations, as well as developing new cybersecurity standards, possible regulatory rulemaking to encourage adoption of those standards, a federal study

21. Hewlett-Packard Enterprise, "Report: Internet of things Research Study," 2014. http://go.saas.hpe.com/fod/internet-of-Things

22. Identity Theft Resource Center, "Data Breach Reports," Dec. 29, 2015. http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf

23. White House "Improving Critical Infrastructure Cybersecurity," Exec. Order No. 13636, 78 Fed. Reg. 11737, Feb. 12, 2013. https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

24. Eric A. Fischer, et al. "The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress" Congressional Research Service, Dec. 15, 2014. https://www.fas.org/sgp/crs/misc/R42984.pdf

25. National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity", Version 1.0, Feb. 12, 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

26. Hanley Chew and Tyler G. Newby, "Privacy Alert: NIST Updates Cybersecurity Framework to Address Supply Chain Security," Fenwick and West LLP, Jan. 8, 2017. http://www.fenwick.com/Publications/Pages/Privacy-Alert-NIST-Updates-Cybersecurity-Framework-to-Address-Supply-Chain-Security.aspx.

27. Diane Honeycutt, "Views on Framework for Improving Critical Infrastructure Cybersecurity," Docket No. 151103999-5999-01], Feb. 23, 2016. http://csrc.nist.gov/cyberframework/rfi_comments_02_2016/20160223_Symantec.pdf; http://www.itic.org/dotAsset/f/9/f9ef5f80-ffc5-4035-b274-87489605ab6e.pdf

28. CITA Wireless Association, "Views on the Framework for Improving Critical Infrastructure Cybersecurity," Feb. 23, 2016. http://csrc.nist.gov/cyberframework/rfi_comments_02_2016/20160223_CTIA-The_Wireless_Association.pdf

29. U.S. Department of Homeland Security, "Strategic Principles for Securing the Internet of things," Nov. 15, 2016. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf

30. Michael Bartock, et al., "Guide for Cybersecurity Event Recovery," Computer Security NIST Special Publication 800-184, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf.

31. Commission on Enhancing National Cybersecurity, "Report on Securing and Growing the Digital Economy," Dec. 1, 2016, https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

on laws relating to internet-of-things device liability and increased research and development funding for cybersecurity.

There also have been legislative proposals intended to address the cyber-threat information gap. The Cybersecurity Information Sharing Act, signed by Obama in December 2015, seeks to improve the flow of communication between companies and federal agencies by offering legal immunity to companies that share information. While information-sharing can be a net positive for stakeholders in the cybersecurity community, there also are concerning aspects–namely the potential to expand government surveillance and to overshare personally identifiable information.[32]

Data-breach notification requirements reduce the information gap for a specific type of cyber event: the unauthorized access of certain types of user data. Two federal laws–the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act–require health and financial institutions to explain their information-sharing practices and to protect user data.[33] HIPAA requires health entities to provide notification following a breach of health information. In addition, 47 states, Puerto Rico and the District of Columbia legally require companies to notify customers of a breach of protected information—including health or personally identifiable information.[34]

More recently, the question of regulatory intervention in the internet of things has been the subject of a series of public workshops hosted by the Federal Trade Commission,[35] as well as a hearing of the Senate Commerce, Science and Transportation Committee.[36] In fact, the FTC recently filed a complaint against computer-networking manufacturer D-Link Corp., asserting it put U.S. consumers' privacy at risk by leaving its routers and webcams vulnerable to hackers.[37] The agency has brought similar cases against manufacturers ASUS and TRENDnet and it's likely the FTC will continue to bring charges against manufacturers for false claims of security.

A number of advocacy groups— including the Electronic Privacy Information Center and the Center for Democracy and Technology—have urged the FTC to implement strong privacy and security standards, citing extensive data collection in the home, a lack of privacy by design, the potential for harm to persons or their property, surveillance concerns and device access to sensitive information, such as health data.[38] These recommendations mirror the European approach to privacy regulation, which includes requiring consumer consent for data collection, mandating transparency, imposing accountability requirements for data practices, limiting data collection and making collected data available to the user.

Following a comment period and a workshop in 2016, the U.S. Commerce Department also has asserted a role in the burgeoning internet-of-things market, releasing a green paper that outlined their responsibility in an interagency approach to foster advancement of the internet of things.[39] The paper asserts the Commerce Department will be involved in standards adoption, promoting an open global environment for internet-of-things development, convening stakeholders to address policy challenges and providing policy input. Critically, it recognizes the risk of premature and excessive regulation and acknowledges the importance of allowing market entrants to experiment and mature.

The new administration also has highlighted cybersecurity as a priority. President Donald Trump has announced plans to create a "cyber review team" of individuals from law enforcement, the private sector and the military to assess cybersecurity risk.[40] Trump announced the selection of former New York City Mayor Rudy Giuliani as his cybersecurity adviser, a role focused on assembling meetings with companies facing cyber threats.[41] It is unclear how much impact on policy this role will allow him. While Giuliani has been working as chairman of Greenberg Traurig's global cybersecurity practice and is the CEO of the international security-consulting firm Giuliani Partners, many observers note it is unclear if he has sufficient technical knowledge or

32. Greg Nojeim, et al. "Letter to Senate Select Committee on Intelligence: Oppose CISA," June 26, 2014. http://www.rstreet.org/outreach/letter-to-senate-select-committee-on-intelligence-oppose-cisa/

33. Steptoe & Johnson LLP, "Comparison of US State and Federal Security Breach Notification Laws," Jan. 21, 2016. http://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf

34. National Conference of State Legislators, "Security Breach Notification Laws," Jan. 4, 2016. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

35. Federal Trade Commission, January 2015.

36. Senate Committee on Commerce, Science and Transportation, "The Connected World: Examining the Internet of Things," Feb. 11, 2015. http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=d3e33bde-30fd-4899-b30d-906b47e117ca&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=2&YearDisplay=2015.

37. Federal Trade Commission, "FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras," Jan. 5, 2017. https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate

38. Center for Democratic Technology, "Re: Comments after November 2013 Workshop on the 'Internet of Things,'" Jan. 10, 2014, https://cdt.org/files/pdfs/iot-comments-cdt-2014.pdf.

39. Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, "Fostering the Advancement of the Internet of Things," January 2017. https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

40. Donald J. Trump, "Donald J. Trump Promises Immediate Action on Cybersecurity in His Administration," *Remarks to the Retired American Warriors*, Oct. 3, 2016. https://www.donaldjtrump.com/policies/cyber-security

41. Michael Shear, "Rudy Giuliani's Cybersecurity Role Reflects Diminished Place in Trump World," *The New York Times*, Jan. 12, 2017, https://www.nytimes.com/2017/01/12/us/politics/rudy-giuliani-cyber-security-trump.html?_r=1.

experience to engage the issue effectively.[42] Encouragingly, in an interview on Fox News, he emphasized the importance of market forces: "My belief is, as always, that the answer to cybersecurity is going to be found in the private sector."[43]

The extent of the Trump administration's engagement on cybersecurity also remains to be seen. A continued emphasis on cybersecurity presents an opportunity to advance the discussion about the insecurity of internet-of-things devices.

GROWING CYBERSECURITY RISK IN THE INTERNET OF THINGS

Cybersecurity is often an afterthought for manufacturers of internet-of-things devices, either because they deem effective measures too costly to implement, because the risks are not understood or because options to mitigate risk are not available or affordable. As a result, many devices are not designed with secure features and cannot be updated or patched after they are sold. In October 2016, hackers using the Mirai malware hijacked a network of internet-of-things devices and used the resulting botnet to perform a distributed denial of service attack on Dyn Inc., a domain-name service provider. The attack disrupted access to such websites as Twitter, Netflix, Amazon and Spotify. It's thought that Mirai malware has infected more than a half-million devices, including more than 10,000 network cameras produced by the Chinese company Hangzhou Xiongmai Technology Co. Ltd.[44] As a result, the company recalled more than 4 million of their networked webcams, which relied on default passwords that many users never changed.

According to an industry survey, 73 percent of internet technology professionals believe security standards are not sufficient to protect the internet of things.[45] Because security is not often "baked in" during the design phase, or throughout the lifetime of a product, the internet of things faces heightened risk of cybercrime. In addition, the challenge posed by internet-of-things devices is unique, because the insecurity of one device affects the ecosystem as a whole. Where a property owner whose home is insecure would bear the full consequences of a robbery, the owner of an insecure device may unknowingly harbor malware that disrupts someone else's online experience. The device owner enjoys the concentrated benefit of using the device, but the costs of insecurity are dispersed throughout the network. The "infection" metaphor is apt. Malware infects connected devices and the resulting botnet is representative of an acute outbreak.

In 2016, service providers listed DDoS attacks as the largest security concern and most common threat.[46] DDoS attacks barrage a target website or application with a large volume of "junk" data or traffic. Such attacks are increasing in frequency and in magnitude, now topping 500 gigabits per second. For a point of comparison, the average internet connection speed in the United States is 12.6 megabits per second, where 1 gigabit is equal to 1,000 megabits.[47] DDoS attacks increasingly target cloud and domain-name services. Criminals also use them to demonstrate their attack capabilities, as part of extortion schemes or to distract from malware infiltration or data breaches.[48] U.S. companies are known to be particularly at risk, as they are targeted frequently and incur larger financial losses than global companies.[49] The top five industries that fell victim to cyber-attacks in 2015 were health care, manufacturing, financial services, government and transportation.[50]

Like malicious insider and web-based attacks, DDoS attacks are high cost. According to an industry survey by the software firm Arbor Networks, 86 percent of respondents estimated the cost of internet downtime to be up to $5,000 per minute.[51] A similar industry survey found that half of DDoS attacks last between six and 34 hours, with an estimated cost of $40,000 per hour.[52] This means that the average DDoS attack can cost about $500,000 for a firm.[53]

Those tallies do not include the ancillary costs of cyberattacks, which can lead to loss of intellectual property; loss of data (including consumer data or sensitive information); physical infrastructure damage; and business and supply-chain interruption. Researchers at RAND Corp. estimate the average data breach costs companies $200,000, although a majority of such events amounted to less than 0.4 percent of a company's annual revenues.[54] Data exfiltration attacks

42. Trevor Timm, "Rudy Giuliani is an absurd choice to defend the US from hackers," *The Guardian*, Jan. 13, 2017. https://www.theguardian.com/commentisfree/2017/jan/13/rudy-giulianis-not-fit-to-protect-the-us-from-hackers

43. Fox & Friends, "Rudy Giuliani to Head New Cyber Security Committee for Trump," Fox News Insider, Jan. 12, 2017. http://insider.foxnews.com/2017/01/12/rudy-giuliani-heads-cyber-security-committee-donald-trump

44. Mimoso, 2016.

45. Jeremy Seth Davis, "Three-quarters of industry pros say a breach caused by an IoT device is likely," SC Magazine, Oct. 23, 2015. https://www.scmagazine.com/three-quarters-of-industry-pros-say-a-breach-caused-by-an-iot-device-is-likely/article/533829/

46. Arbor Networks, 2016.

47. Akamai, "State of the Internet Report," 2016. https://content.akamai.com/pg7425-uk-soti-report.html

48. Arbor Networks, 2016.

49. PricewaterhouseCoopers, "Global Economic Crime Survey," 2016. http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey.html

50. IBM X-Force Research, "IBM 2016 Cyber Security Intelligence," 2016. http://www-03.ibm.com/security/data-breach/cyber-security-index.html

51. Arbor Networks, 2016.

52. Incapsula, "Survey: What DDoS Attacks Really Cost Businesses," pp. 1-9, 2014. https://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf

53. Incapsula, p. 6, 2014.

54. Sasha Romanosky, "Examining the costs and causes of cyber incidents," *Journal of Cyber Security*, Aug. 8, 2016. http://cybersecurity.oxfordjournals.org/content/early/2016/08/08/cybsec.tyw001.

can be hard to detect. According to research firm Mandiant, the average lag time from initiation until a data breach is detected is 205 days.[55]

In some cases, data have national security implications or could affect relations with international allies. The 2015 hack of the U.S. Office of Personnel Management resulted in the loss of the sensitive personal information of 21.5 million federal employees, including the information of 19.7 million security-clearance applicants.[56] In 2009, a Chinese hacker acquired data relating to the F-22 and F-35 fighter jets from U.S. defense companies.[57]

The Online Trust Alliance indicated in a 2014 report that 90 percent of that year's breaches could have been prevented if organizations implemented basic cybersecurity best practices.[58] The Broadband Internet Technical Advisory Group has determined that the best current software practices for internet-of-things devices include shipping devices with current software; designing a mechanism for secure, automated software updates; employing strong authentication by default; using cryptography best practices; and testing and hardening internet-of-things device configurations.[59]

The Ponemon Institute estimates that one quarter of all breaches are due to human error,[60] including internal employee errors, as was the case with Hillary Clinton campaign chairman John Podesta's hacked email account. Podesta mistakenly clicked a link in a fraudulent phishing email that directed him to change his password, allowing hackers access to the account and 10 years' worth of his emails.[61] Such breaches can be prevented by encouraging basic security behavior, such as keeping devices up-to-date, increasing awareness about phishing and social-engineering attacks, using complex passwords with two-factor authentication and updating passwords regularly.

Combating an industrywide infection will require efforts to prevent, detect, mitigate and cure vulnerable devices. For device users and producers, security best practices must become habitual. For internet-of-things companies, proper cyber hygiene includes enforcing strong passwords and regular password changes; updating firewalls, anti-virus, anti-malware tools and other protection systems; encrypting sensitive data; implementing a data-loss protection solution that can monitor traffic; introducing vigorous updating and patching, including automatic patch deployment; and limiting configurations, ports, protocols and services to prevent remote access.[62] In the following sections, we will explore how industry, policymakers and third parties can offer incentives to adopt basic cybersecurity practices through market mechanisms.

CASE FOR A LIGHT-TOUCH REGULATORY APPROACH

As the internet of things continues to develop, policymakers should be careful not to construct overly restrictive regulatory regimes. Fear of insecure devices manufactured abroad or apprehensions about the privacy implications of data collection should not drive rash policy decisions. Rushing the rulemaking process could lead to poor implementation, exaggerated compliance costs and limited results.[63] Regulations may have unintended consequences that could strangle the internet-of-things industry while it's still in the cradle.

Heavily regulated industries experience fewer market entrants and slower employment growth, disproportionately affecting smaller firms and limiting competition.[64] Regulatory requirements can also dampen competition. In this way, regulations serve to shield large, well-represented companies from competition, because smaller companies can't afford to comply.[65] In effect, regulations act as a barrier to entry for entrepreneurs, allowing incumbent firms to raise prices, diminish quality and reduce expenditures on research and development.

55. Mandiant, "M-Trends 2015: A View from the Front Lines," FireEye, 2015. https://www2.fireeye.com/WEB-2015-MNDT-RPT-M-Trends-2015_LP.html

56. Jim Sciutto, "OPM government data breach impacted 21.5 million," *CNN Politics*, July 10, 2015. http://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/

57. Justin Ling, "Man Who Sold F-35 Secrets to China Pleads Guilty," *Vice News*, March 24, 2016. https://news.vice.com/article/man-who-sold-f-35-secrets-to-china-pleads-guilty

58. Online Trust Alliance, "OTA Determines Over 90% of Data Breaches in 2014 Could Have Been Prevented," Jan. 21, 2015. https://www.otalliance.org/news-events/press-releases/ota-determines-over-90-data-breaches-2014-could-have-been-prevented

59. Broadband Internet Technical Advisory Group, "Internet of Things (IoT) Security and Privacy Recommendations: A Broadband Internet Technical Advisory Group Technical Working Group Report," November 2016. https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

60. Ponemon Institute, "2015 Cost of Data Breach Study: Global Analysis," May 2015. https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF

61. Joe Uchill, "Typo led to Podesta email hack: report," *The Hill*, Dec. 13, 2016. http://thehill.com/policy/cybersecurity/310234-typo-may-have-caused-podesta-email-hack

62. Symantec Corp., "Internet Security Threat Report," Vol. 19, pp. 2-97, 2014. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

63. Jerry Ellig, Patrick A. McLaughlin and John F. Morrall III, "Continuity, Change, and Priorities: The Quality and Use of Regulatory Analysis across U.S. Administrations," *Regulation & Governance*, 7:153–73, Aug. 13, 2012. http://onlinelibrary.wiley.com/doi/10.1111/j.1748-5991.2012.01149.x/abstract; see also Jerry Ellig and Rosemarie Fike, "Regulatory Process, Regulatory Reform, and the Quality of Regulatory Impact Analysis," Working Paper No. 13-13, Mercatus Center at George Mason University, July 2013. http://mercatus.org/publication/regulatory-process-regulatory-reform-and-quality-regulatory-impact-analysis

64. James Bailey and Diana Thomas, "Regulating Away Competition: The Effect of Regulation on Entrepreneurship and Employment," *Mercatus Center*, September 2015 https://www.mercatus.org/system/files/Bailey-Regulation-Entrepreneurship.pdf

65. Matthew Mitchell, "The Pathology of Privilege: The Economic Consequences of Government Favoritism," Mercatus Research, Mercatus Center at George Mason University, July 8, 2012. https://www.mercatus.org/publication/pathology-privilege-economic-consequences-government-favoritism

By one estimate, the accumulation of regulations in the United States between 1949 and 2005 slowed overall economic growth by an average of 2 percent per year, amounting to $277,100 per household.[66] Regulatory accumulation increases compliance costs, takes resources away from productive activities[67] and can negatively impact job and wage growth.[68] Moreover, excessive regulation can introduce uncertainty that pressures companies to move operations to jurisdictions with more favorable regulatory regimes.[69] Foreign competitors who do not face the same regulations may be able to undercut their regulated competitors, putting U.S. companies at a competitive disadvantage.

Regulation aimed at encouraging cybersecurity in the internet of things should emphasize performance standards over design standards. Performance standards specify the outcome of a policy and allow companies the flexibility to identify the best means or design to achieve it.[70] For example, a performance standard could state that data at rest on internet-of-things devices needs to be protected, whereas a design standard might specify the type of encryption or layer that needs to be encrypted. An unseen secondary consequence of design standards is that they remove the incentive for companies to find alternative solutions to achieve the same outcome. Given the broad number of functions served by networked devices, it is unlikely that a design standard will be effective for all use cases. Air gapping, data backups or data-masking techniques may work better for some internet-of-things applications. Furthermore, developments in encryption techniques, or in the sophistication of criminals, quickly may render a given design standard ineffective.

Furthermore, there can be problems with inconsistent or incorrect administration and enforcement of standards. Performance standards can also be restrictive or misdirected, but exhibit advantages over design standards because they are not as prescriptive.[71] Moreover, performance standards do a better job of aligning the incentives of companies and regulators, because they reward behaviors directed at the desired outcome rather than at compliance tasks.

Regulatory programs that rely on market-based incentives can have better, longer-lasting outcomes than regulations that focus on design standards. Industry can participate in self-regulation, as well, by recalling unsecure products, updating products or changing policies to address cybersecurity concerns. To the extent possible, policymakers should allow companies the flexibility to adapt to changing threats and address concerns as they arise.[72]

MARKET SOLUTIONS

Cyber insurance

Cyber insurance policies, which first appeared during the dot-com boom of the early 2000s,[73] allow businesses to transfer the liability and operational risks of cyber-attack or other internet-based risks to insurers. In its earliest forms, cyber insurance covered first-party property loss—damage to an insured's own infrastructure and equipment—as well as liability coverage to defend clients against lawsuits.

Today's cyber insurance can cover breach-response costs, such as attorneys' fees; breach notification to consumers; credit monitoring for consumers; call centers; public relations services; and technical forensic investigations to determine the origin of the attack and how it occurred. Other costs covered by cyber insurance include regulatory fines and responses to regulators, as well as legal defense and settlement costs. More recently, cyber-insurance solutions have included DDoS mitigation services and costs associated with internet downtime.[74] In one notable recent claim, the Los Angeles Community College District used their cyber-insurance policy to cover a $28,000 ransom after a ransomware attack paralyzed the college's computer network and email system.[75] Cyber insurance allowed the college to recover and learn from the attack.

Evidence shows the commercial cyber-insurance market is growing. As of June 2016, the National Association of Insurance Commissioners found that more than 500 insurers are

66. John W. Dawson and John J. Seater, "Federal Regulation and Aggregate Economic Growth," *Journal of Economic Growth*, pp. 1-41, January 2013. http://www4.ncsu.edu/~jjseater/regulationandgrowth.pdf

67. Testimony by Patrick A. McLaughlin, The Searching for and Cutting Regulations that are Unnecessarily Burdensome Act of 2014," House Committee on the Judiciary, Subcommittee on Regulatory Reform, Commercial, and Antitrust Law, Feb. 11, 2014 http://docs.house.gov/meetings/JU/JU05/20140211/101738/HHRG-113-JU05-Wstate-McLaughlinP-20140211.pdf

68. Keith Hall, "The Employment Costs of Regulation," Mercatus Center, March 2013. https://www.mercatus.org/system/files/Hall_EmploymentCosts_v3.pdf

69. W. Mark Crain and Nicole V. Crain, "The Cost of Federal Regulation to the U.S. Economy, Manufacturing and Small Business," *National Association of Manufacturers*, pp. 1-73, Sept. 10, 2014. http://www.nam.org/Data-and-Reports/Cost-of-Federal-Regulations/Federal-Regulation-Full-Study.pdf

70. David Hemenway, "Performance vs Design Standards," U.S. Department of Commerce, NIST, pp. 1-35, October 1980. http://gsi.nist.gov/global/docs/pubs/NIST-GCR_80-287.pdf

71. Id., pp. 2-3.

72. Consumer Technology Association, "Internet of Things: A Framework for the Next Administration," November, 2016. http://www.cta.tech/cta/media/policyimages/policyPDFs/CTA-Internet-of-Things-A-Framework-for-the-Next-Administration.pdf

73.Michael Menapace, "Written Testimony to Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security: Examining the Evolving Cyber Insurance Marketplace," March 19, 2015. https://www.commerce.senate.gov/public/_cache/files/90fa0bc7-8686-4b90-9a1b-3525cc62d4fe/8A982AD17B40EDD0101AD5974A36AD73.menapace-testimony-for-senate-hearing-on-cyber-insurance.pdf

74. Christine Marciano, "Cyber Insurance can serve as an Ideal DDoS Attack Response Plan," June 12, 2014. https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-can-serve-as-an-ideal-ddos-attack-response-plan/

75. Soloman Smith, "Update: Valleys Pays Ransom with Cyber Insurance," *The Valley Star*, Jan. 6, 2017, http://thevalleystar.com/valleys-pays-ransom-with-cyber-insurance/#sthash.bBt6GcLi.dpbs

supplying cyber insurance in the United States, with direct written premiums of nearly $484 million for standalone cybersecurity policies and nearly $1 billion for package policies.[76] Total written premiums are expected to double over the next four years from $4 to $8 billion in 2020.[77] However, it's worth noting that adoption varies significantly by industry. While the takeup rate in the retail, health and financial services sectors is around 80 percent,[78] less than 5 percent of the manufacturing sector has cyber-insurance coverage.[79]

Because insurers must be certain they take in sufficient premiums to cover the risks they take on, risk assessment is a crucial part of the insurance process, both in the underwriting (determining whether to insure a given risk) and ratemaking (determining what premium to charge for that risk) functions. The predictable effect of this risk-based pricing is to expand the market incentives for risk mitigation, just as insurers also have sought actively to improve building standards in risk-prone areas[80] and encouraged other kinds of loss-mitigation planning.[81]

Similarly, cyber insurance can help companies to reflect on possible risks and plan for them. Cyber insurance policies often offer monitoring services that decrease the time needed to respond to a threat.[82] During risk assessments, cyber insurers evaluate the applicant's security, sometimes with an on-site visit and almost always with an online questionnaire designed to measure security infrastructure, available budget, virus-protection programs, outsourcing, and testing and security procedures.[83] During on-site visits, the insurer may perform a technical assessment of a network's internal and external vulnerabilities, including a review of firewalls, routers and network configuration. In this way, insurers can hold businesses accountable to their cybersecurity plans by having policy provisions in place that prevent firms from making claims if they have not taken reasonable steps to maintain or improve their security.

Cyber-insurance policies often require insureds to make data-encryption and security-patch commitments. In addition to these benchmark security requirements to be eligible for a policy, actuarially sound premiums also provide incentives to insureds to adopt better cyber practices.[84] Improving authentication processes by, for example, removing default passwords would prevent password-stealing botnets from deputizing internet-of-things devices. Encryption of data at-rest and data in-transit can protect private information.[85] Firewalls, anti-virus software and anti-malware tools can also help to protect data. Developing, updating and patching practices help companies to address evolving cyber threats. During the design phase, manufacturers can limit configurations, ports and protocols to prevent remote access. Those insureds who demonstrate compliance with these kinds of good cyber-hygiene practices may enjoy discounts. Those who do not may not be able to obtain coverage at all.

Information is crucial for underwriters to assess risks. Toward that end, public and private information-sharing efforts encourage access to data on the frequency, extent and type of cyber-attacks. The 2014 NIST framework, developed to advance discussion of best cybersecurity practices, codifies common expectations of cyber risk as perceived by industry and government. The framework could offer a valuable underwriting and ratemaking tool for insurers, in that it represents a shared cyber-risk language for companies, third parties and policymakers that previously was absent.[86]

But cyber insurance is not a cure-all and the market has not yet developed to the extent that it can manage all potential risks. While estimates show that policies with $50 million limits would be able to cover roughly 92 percent of cyber-event claims,[87] some models estimate the likelihood of a major "black swan" event in the next decade that causes between $250 billion and $1 trillion in damage to critical information infrastructure to be between 10 and 20 percent.[88]

It can be hard to quantify exposure to cyber risks, especially when a loss by one company affects other parts of the network. The motives for cyber-attack are diverse, multiple

76. National Association of Insurance Commissioners, "Early NAIC Analysis Sheds Light on Cybersecurity Insurance Data," June 30, 2016. http://www.naic.org/Releases/2016_docs/cybersecurity_insurance_data_analysis.htm

77. Jonathan Camhi, "The Cyber Insurance Report: Market potential, top industries, and the major challenge to offering a fast-growing insurance product," *BI Intelligence*, Feb. 2, 2016.

78. Council of Insurance Agents and Brokers, "Cyber Insurance Market Watch Survey," October 2016. https://www.ciab.com/uploadedFiles/Resources/Cyber_Survey/102016CyberSurvey_Final.pdf

79. Ibid.

80. Mike Tsikoudakis, "Hurricane Andrew Prompted Better Building Code Requirements," *Business Insurance*, Sept. 19, 2012, https://www.businessinsurance.com/article/20120819/NEWS06/308199985

81. Zurich Insurance Co., "Report: Enhancing Community Flood Resilience: A Way Forward," May 2014. https://www.zurich.com/en/media/news-releases/2014/2014-0612-01

82. Id., p. 11.

83. Id., pp. 11-12.

84. Jay Kesan, Ruperto Majuca and William Yurcik, "Cyberinsurance as a market-based solution to the problem of cybersecurity: a case study," University of Illinois at Urbana-Champaign, 2005. http://infosecon.net/workshop/pdf/42.pdf

85. Anurag Kumar Jain and Devendra Shanbhag, "Addressing Security and Privacy Risks in Mobile Applications," *Mobile and Wireless Technologies*, September/October 2012. https://pdfs.semanticscholar.org/aa53/1e41c4c646285b522cf6f33f82a9d68d5062.pdf

86. Federal Insurance Office, "Annual Report on the Insurance Industry," U.S. Department of the Treasury, pp. 1-81, September 2015. https://www.treasury.gov/initiatives/fio/reports-and-notices/Documents/2015%20FIO%20Annual%20Report_Final.pdf

87. Martin Eling and Jan Hendrik Wirfs, "Cyber Risk: Too Big to Insure?," Institute of Insurance Economics, pp. 6-7, 2016. http://www.ivw.unisg.ch/-/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf

88. Global Risk Network, "Global Risks 2010," World Economic Forum, January 2010 http://www.weforum.org/pdf/globalrisk/globalrisks2010.pdf

attacks can take place simultaneously or may repeat, business impact is hard to measure and attacks may take years to uncover and report. Risk assessments can be costly, with one small business reporting that getting insurance quotes and complying with the NIST framework took four months and cost more than $10,000.[89]

Given complaints by some in the business community about the cost of cyber coverage, especially for small and mid-sized firms, some policy analysts have begun to discuss the possibility of a temporary government backstop for cyber insurance,[90] similar to the $100 billion reinsurance backstop Congress created for terrorism risks in 2002. However, unlike terrorism risk in 2002, insurance and reinsurance markets are growing in their capacity and appetite for cyber risk. To the extent that some firms may have difficulty placing some kinds of cyber risks with third parties, there also are a variety of alternative risk-transfer mechanisms available, most notably company-owned captive insurers or closely held risk retention groups.

A closer examination of the problems with the Terrorism Risk Insurance Act, which has been renewed three times since its creation, should counsel policymakers to view any further "temporary" insurance backstops with skepticism.[91] Either a formal government backstop for cyber insurance or a system that hinges on future government bailouts would create moral hazard problems.[92] The government safety net not only reduces incentives to guard against risk, but such programs also displace private coverage options and prove politically difficult to unwind.

A robust private cyber insurance market will help raise the bar for device security, which is important for the entire internet ecosystem. Taking the steps necessary to ensure that such a market flourishes should be a policy imperative.

Filling the information gap

The lack of robust and broadly accessible experience data about past cyber events is a challenge for all parties involved in the cybersecurity and cyber-insurance markets. Key information associated with cyber incidents includes the type, severity, incident-detection methods used, incident response deployed, contributing causes, vulnerabilities, assets compromised, motive, timeline, risk-management approach, mitigation and prevention measures, impacts and costs.[93]

The Department of Homeland Security's Cyber Incident Data and Analysis Working Group has identified a number of obstacles to information sharing, including anonymization concerns, data security, cultural differences, perceptions of commercial disadvantage, internal process hurdles, technical design issues, problems with participation and misunderstandings about the value of information sharing.[94] CIDAWG proposed creating a Cyber Incident Data and Analysis Repository that would provide insurers and other stakeholders with information to develop coverage and risk-management solutions.[95]

While the insurance industry generally is supportive of CIDAWG's proposal, there are concerns about how the data repository would be implemented.[96] To secure participation, the repository would have to ensure contributors that submissions would be anonymous and secure. Inaccurate and inconsistent reporting would render the CIDAR less valuable, but more detailed reporting questions could risk prompting contributors to share details that reveal their identities. While the repository will not be government-operated, it is unclear how much access government will have. Also unclear is where the data should be housed, whether a university, a company, an insurer or some other third-party organization. Also, the incentives for larger insurers to participate, and share what would otherwise be proprietary underwriting data with smaller competitors, may prove to be weak.

If the data repository can overcome these obstacles, one would expect insurers will be able to expand coverage offerings to small and medium-sized businesses.[97] Insurers could reward better cybersecurity practices with lower insurance rates and encourage the adoption of best practices, such as the NIST framework. Moreover, policymakers, researchers and companies will have the information to inform public and private risk-mitigation strategies and to direct cybersecurity research and policy focus.

---

89. Ola Sage, "Prepared Testimony for Hearing on Examining the Evolving Cyber Insurance Marketplace," Senate Committee on Commerce, Science, and Transportation, Subcommittee on Consumer Protection, Product Safety, Insurance and Data Security, March 19, 2015. https://www.commerce.senate.gov/public/_cache/files/cfa8174a-e7f4-434a-9669-09282c0a8f1f/1572E3208FB577D440D5CF0DA13B9125.sage-testimony-for-the-record-march-2015-final.pdf

90. Judy Greenwald and Sarah Veysey, "Cyber Risk Insurance Backstop could Emerge in the Event of Catastrophic Attack," *Business Insurance*, Feb. 22, 2015. https://www.businessinsurance.com/article/20150222/NEWS06/303019998

91. Ibid.

92. Ian Adams, "The Promise and Limits of Private Cyber Insurance," R Street Institute, December 2016. https://www.rstreet.org/wp-content/uploads/2016/12/78.pdf

93. Department of Homeland Security, "Enhancing Resilience through Cyber Incident Data Sharing and Analysis: Establishing Community-Relevant Data Categories in Support of a Cyber Incident Data Repository," September 2015. https://www.dhs.gov/sites/default/files/publications/Data%20Categories%20White%20Paper%20FINAL_v3b.pdf

94. Ibid.

95. Ibid.

96. American Insurance Association, Email RE: National Protection and Programs Directorate's Cyber Incident Data Repository White Papers, May 24, 2016. https://www.dhs.gov/sites/default/files/publications/052416_AIA%20Letter_DHS_CIDAR_Final.pdf

97. Rep. Bennie G. Thompson, Letter RE: Docket No. DHS- 2015-0068, May 24, 2016 https://www.dhs.gov/sites/default/files/publications/052416_US%20HOR%20Letter_DHS_CIDAR_Final_0.pdf

Programs that share threat information with companies and the government are helping to fill in this information gap. Such programs include Facebook's ThreatExchange and the DHS's Cyber Information Sharing and Collaboration Program.[98] Threat-modeling can allow companies or federal agencies to identify and correct vulnerabilities in real time.[99]

On the other hand, consumers continue to face information deficiencies, as it is difficult for them to determine whether such products as routers, smart TVs, smart thermostats or webcams are secure. The public information gap about cyber events and vulnerabilities represents a market opportunity for entrepreneurs to create ratings bodies and voluntary certification organizations. By providing information about companies' cybersecurity track records, these entities could foster trust and exchange between consumers and internet-of-things device sellers.

Some of this is already happening. For example, Underwriters Laboratories introduced a cybersecurity assurance program to assess security risks in internet-of-things products.[100] The Online Trust Alliance recently published the second version of its "IoT Trust Framework" to serve as a risk-assessment guide for stakeholders.[101] The OTA guide details devices' design requirements and security processes, serving as a checklist for internet-of-things device-certification programs.

There's also a role for more informal processes to supply reputational information to consumers, as Yelp or Amazon reviews do today. The threat of a bad rating or review can prompt companies to adopt better cyber practices and hold companies accountable for data breaches or vulnerabilities. Businesses can gain a reputation for securing their products and consumers can know which products are safe.

CYBER INSURANCE FOR FEDERAL VENDORS

The federal government and its contractors are "the largest single producer, collector, consumer, and disseminator of information in the United States and perhaps the world."[102] As a consequence, federal agencies can use their power of the purse to signal to industry that considering security at all phases of the design process is paramount.

Given the risk and sensitivity of data held by the government–including IRS records, Social Security numbers, personnel records, public and private-sector intellectual property and classified information–cybersecurity must be a priority. The Office of Personnel Management data breach in 2015 led to the exposure of 21.5 million records, including Social Security numbers, and affected 6.7 percent of the U.S. population.[103]

Sensitive data also flows through contractor systems connected to government information-technology networks. In 2012, agencies reported that contractors performed one-third of all information-technology security duties.[104] As internet-of-things technologies develop, these devices will be present in a growing amount of IT systems, including those of the federal government.

Federal cybersecurity requirements for agencies began with the 2002 passage of the Federal Information Security Management Act. FISMA charged the White House Office of Management and Budget with agency oversight, required creation of a Federal Information Security Incident Center and delegated cybersecurity responsibilities to NIST.[105] The bill also appointed agencies to be responsible for the cybersecurity of their own information systems, as well as systems operated by contractors.[106]

The federal government also has taken steps to bolster cybersecurity protections by its contractors, using the acquisitions process. In 2013, the Department of Defense issued requirements for defense contractors to protect unclassified controlled technical information—defined as "technical information with military and space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure or dissemination"—from cyber intrusions and report incidents.[107]

98. Facebook for Developers, "ThreatExchange," 2016. https://developers.facebook.com/products/threat-exchange; see also Department of Homeland Security, "Cyber Information Sharing and Collaboration Program," May 4, 2016. https://www.dhs.gov/ciscp

99. Mark G. Hardy, "Beyond Continuous Monitoring: Threat Modeling for Real-time Response," *SANS Institute Infosec Reading Room*, Oct. 25, 2012. https://www.sans.org/reading-room/whitepapers/analyst/continuous-monitoring-threat-modeling-real-time-response-35185

100. Underwriters Laboratories, "UL Launches Cybersecurity Assurance Program," April 5, 2016. http://www.ul.com/newsroom/pressreleases/ul-launches-cybersecurity-assurance-program/

101. Online Trust Alliance, "IoT Trust Framework," Jan. 5, 2017. http://otalliance.actonsoftware.com/acton/attachment/6361/f-008d/1/-/-/-/-/IoT%20Trust%20Framework.pdf

102. White House Office of Management and Budget, "FY 2005 Report to Congress on Implementation of the E-Government Act of 2002," p. 5. March 1, 2005. https://georgewbush-whitehouse.archives.gov/omb/inforeg/reports/2005_e-gov_report.pdf

103. Jim Sciutto, "OPM Government Data Breach Impacted 21.5 Million," CNN Politics, July 10, 2015. http://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/

104. U.S. Government Accountability Office, "Agencies Need to Improve Oversight of Contractor Controls," GAO-14-612, August 2014. http://www.gao.gov/assets/670/665246.pdf

105. Robert Nichols, et al., "Cybersecurity for Government Contractors," Briefing Papers Second Series No 15, April 2014. https://www.cov.com/-/media/files/corporate/publications/2014/04/cybersecurity_for_govt_contractors.pdf

106. 44 U.S.C.A. § 3544(a)(1)(A)(ii).

107. 78 Fed. Reg. 69,273 (Nov. 18, 2013) (adding DFARS subpt. 204.73 and the clause at DFARS 252.204-7012).

The Obama administration's Executive Order 13636 instructed the General Services Administration and DOD to make recommendations on the benefits and feasibility of incorporating cybersecurity standards in the federal acquisition process.[108] The resulting report contained suggestions that may be implemented over the next few years, including instituting baseline cybersecurity requirements as a condition for contracts, harmonizing and developing common definitions, creating a governmentwide risk-management strategy and requiring government to procure certain items from trusted sources.[109]

At least two of these recommendations could be fulfilled by requiring that federal internet-of-things contractors procure certain types of cyber-insurance coverage. In particular, such a requirement would provide incentives for contractors to adhere to baseline cybersecurity standards and demonstrate these companies as trusted sources. The addition of a cyber-insurance requirement in federal acquisitions also would be consistent with the efforts of government entities to improve cybersecurity among government contractors.

In 2014, Eli Dourado and Andrea Castillo of the Mercatus Center proposed having federal agencies themselves buy cyber insurance through a competitive bidding process.[110] While the doctrine of sovereign immunity exempts most federal agencies from direct claims of tort, the courts have found some longstanding exceptions.[111] In the case of a cyber-attack or data breach that stems from the insecurity of a contractor or vendor's system, the contracting agency also could have to expend resources on a host of ancillary costs, which can include DDoS mitigation services, forensic investigations, user notifications and data recovery. Rather than pass such costs onto the taxpayers, agencies and government purchasing agents should assert in contractual language their right to subrogate these liabilities from the contractor or vendor. Thus, contractors and vendors also should be asked to demonstrate they are capable of bearing financial responsibility for any cyber-liabilities they might create for the federal government, including the risk that a breach or attack will render the contractor or vendor unable to deliver or complete a project.

Given the incredibly broad range of activities engaged in and potential risks faced by different kinds of federal vendors and contractors—not to mention that firms of different types and sizes each will have their own insurance and risk-management needs—no one-size-fits-all requirement could possibly cover all cases. For some firms, financial responsibility could be demonstrated in ways other than insurance coverage, including through a surety or other performance bond, or by posting collateral or cash equivalents, such as a letter of credit. But for many, the most cost-effective means to make such demonstrations would be to procure insurance, whether it be a commercial general liability and/or directors and officers program that includes cyber coverage; a stand-alone cyber package; by ceding risks to a company-owned captive insurer; or by participation in a risk retention group focused on cyber liabilities.

In contrast to enforcing specific security standards, stipulating a financial responsibility requirement would ensure that federal contractors evolve their security practices to find the most cost-effective risk-management strategies available. Aligning company incentives with market incentives will lead to better outcomes for the internet of things and for information security.

The implementation of a financial responsibility requirement for internet-of-things vendors would fall under the jurisdiction of the General Services Administration, which runs the Federal Acquisition Service responsible for awarding contracts to vendors. The requirement will have to be balanced to ensure that taxpayers are not held accountable for the poor cyber-hygiene or risk-management practices of federal contractors, but not to be so risk-averse as to add unnecessary costs to vendors or the government. For example, it may be prudent to cap the requirement to demonstrate financial responsibility to the size of a given contract. While it is possible for a contractor to create liabilities for the federal government far in excess of the value of their contract, uncapped liability could be unduly burdensome on smaller contractors

A vendor requirement intended to help with internet-of-things adoption could be implemented through an executive order, through a law enacted by Congress or through a guidance requirement issued by OMB or GSA. At the very least, requiring that federal internet-of-things vendors demonstrate a cyber plan to mitigate risk from DDoS attacks or data breaches will prompt federal contractors to examine their vulnerabilities more closely.

CONCLUSION

The internet of things introduces new attack vectors and has facilitated an increase in distributed denial of service attacks, among other types of cyberattacks. In the context of DDoS attacks, the lack of cybersecurity is often viewed as a demonstration of market failure. It should instead be

108. E.O. 13636 § 8(e).

109. General Services Administration and Department of Defense, "Improving Cybersecurity and Resilience through Acquisition," Jan. 23, 2014. http://www.defense.gov/news/Improving-Cybersecurity-and-ResilienceThrough-Acquisition.pdf

110. Eli Dourado and Andrea Castillo, "Why the Cybersecurity Framework Will Make Us Less Secure," Mercatus Center, April 17, 2014. https://www.mercatus.org/publication/why-cybersecurity-framework-will-make-us-less-secure

111. John Lobato and Jeffrey Theodore, "Briefing Paper No. 21: Federal Sovereign Immunity," Harvard Law School Federal Budget Policy Seminar, May 14, 2006. http://www.law.harvard.edu/faculty/hjackson/FedSovereign_21.pdf

viewed as a market opportunity for private actors to lower the cost of information exchange or to help companies mitigate cybersecurity risks. Policymakers can play a role in supporting market-based solutions like cybersecurity-assurance programs, information-sharing programs and adoption of cyber insurance.

One positive step policymakers can take to encourage adoption of good cyber practices is to leverage the power of the purse[112] to select government-facing internet-of-things vendors that have demonstrated their commitment to cybersecurity by employing appropriate risk transfer tools like cyber insurance. Encouraging the adoption of cyber insurance will help to usher in a culture of preparedness by offering incentives to companies that improve their basic security posture. It will also help companies to understand cyber risk and internalize the cost of device insecurity.

Policymakers should avoid any regulatory approaches that would require design standards rather than performance standards. Design standards include rules that would require products to use certain protocols or communication standards deemed secure, whereas performance standards would set a desired safety outcome without specifying the means to achieving it. This would motivate companies to focus on compliance, rather than security. Legislating specific technical solutions would codify easily outdated features, limit U.S. competitiveness abroad and stunt experimentation.

Market approaches to internet-of-things insecurity include adoption of cyber insurance, technical and managerial solutions, industry-led initiatives and voluntary certification and ratings efforts. In pursuing these efforts, industry leaders, third parties and policymakers can establish an environment where the security of connected devices is the norm rather than the exception.

ABOUT THE AUTHOR

Anne Hobson is a technology policy fellow with the R Street Institute, specializing in free-market approaches to emerging technologies, including virtual reality, artificial intelligence, the internet of things and the sharing economy.

Anne joined R Street in September 2016, having most recently served as a policy associate at Facebook's Washington office. She is an alumna of the Mercatus Center MA Fellowship at George Mason University, where she worked with the technology policy program, and was new media manager with The American Spectator as part of the Koch Associate Program.

112. Kate Stith, "Congress' Power of the Purse," *The Yale Law Journal* 97, no. 7 (June 1988): 1343–96.