Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

CYBER STATECRAFT
INITIATIVE

THE REVERSE CASCADE:
Enforcing Security On The Global IoT Supply Chain

Nathaniel Kim, Trey Herr, and Bruce Schneier

Scowcroft Center for Strategy and Security

*The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.*

Cyber Statecraft Initiative

*The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.*

Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

CYBER STATECRAFT
INITIATIVE

THE REVERSE CASCADE:
Enforcing Security On The Global IoT Supply Chain

Nathaniel Kim, Trey Herr, and Bruce Schneier

ISBN-13: 978-1-61977-106-2

Cover photo: A microwave, a wearable, and a thermostat connected on the Internet of Things.

June 2020

Table of Contents

1. Overview

The Internet of Things (IoT) refers to the increasing convergence of the physical and digital worlds. Hundreds of "things" are being connected to the Internet and each other, with more than fifty billion devices expected to be connected by 2030.[1] These devices vary from Internet-connected power-generation equipment to wearable health trackers and smart home appliances, and generally offer some combination of new functionality, greater convenience, or cost savings to users.

As with all benefits, IoT also comes with serious risks, with impacts ranging from individual consumer safety to national security. IoT gives computers the ability to directly affect the physical world: toys, small and large appliances, home thermostats, medical devices, cars, traffic signals, and power plants. This transfers the traditional computer risks to these devices. Cybersecurity is now a relevant concern for even the most mundane household objects—smart electric kettles can be set to explode, while compromised smart toys might eavesdrop on private conversations.[2] Hacked thermostats can cause property damage. Hacked power generators can cause blackouts. Hacked cars, traffic signals, and medical devices can result in death. IoT devices taken over en masse can be used for distributed denial-of-service (DDoS) attacks, paralyzing critical Internet resources and corporate websites with a flood of Internet traffic. In April 2020, a security firm observed a botnet emitting a Linux malware known as "Kaiji" using SSH brute-force techniques to target IoT devices.[3] Examples such as these suggest that attempts by both criminals and governments to exploit vulnerabilities in insecure IoT devices will only increase. The result of these insecurities is an emerging national security threat likely only to grow without substantial countering action.[4]

These attacks are all the byproducts of connecting computing tech to everything, and then connecting everything to the Internet. They are made substantially more frequent and impactful by the poor state of security practice across many segments of IoT manufacturing and design. While the IoT needs reliable security throughout its ecosystem, the unsecure devices that make up the billions of nodes within that ecosystem are a significant part of the problem. Many vendors bring insecure or poorly configured products to market in response to competitive pressures and lack of clear secure-development standards. A variety of policies and best practices have been proposed, but all remain voluntary and have failed to stem the tide of insecure IoT. Cheeky Twitter feeds such as @InternetofShit offer endless one-liners about Wi-Fi-connected toasters, refrigerators, and adult toys, but the real downside is a diffuse, but growing, risk to public safety and the security of data.

Problem: Many IoT devices are manufactured abroad, and many of these products are extremely low cost with little consideration made for security.

The economics of IoT favor low-cost products. Unlike computers and smartphones, security isn't prioritized in the development process for IoT products. They are often designed under contract for the company whose brand is on the finished product. The design teams are temporary for the design process, and don't stay together through the product's lifecycle.

The United States has limited means to enforce its standards in foreign jurisdictions, like China, where the bulk of IoT products are manufactured. There is nothing inherently untrustworthy or insecure about foreign manufacturing; individual firms and product lines are much more fruitful levels to analyze in establishing good security practices from bad. Importantly, however, the United States has few tools to enforce its security standards on manufacturers located abroad. Thus, companies with poor security practices outside the United States create a challenge for established regulatory tools. Policymakers would benefit from more coherent and detailed IoT security standards, but what's urgently needed is a mechanism to enforce these standards abroad. A coherent set of standards and associated enforcement action against manufacturers throughout global IoT supply chains could well "lift all boats" and address IoT insecurities, which can impact the United States even when the devices themselves are well abroad.

This paper proposes to apply regulatory pressure to domestic technology distributors to drive adoption of security

1 "Number of Internet of Things (IoT) Connected Devices Worldwide 2030," Statista, February 19, 2020, https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/.

2 "International Product Safety Week 2018 (Conference)," European Commission, November 12, 2018, https://ec.europa.eu/info/events/international-product-safety-week-2018-2018-nov-12-0_en.

3 David Bisson, "New 'Kaiji' Linux Malware Targeting IoT Devices," *Security Intelligence*, May 6, 2020. https://securityintelligence.com/news/new-kaiji-linux-malware-targeting-iot-devices/.

4 Justin Sherman and Deb Crawford, "Securing America's Connected Infrastructure Can't Wait," War on the Rocks, December 4, 2018, https://warontherocks.com/2018/12/securing-americas-connected-infrastructure-cant-wait/.

standards throughout their supply chains. This *reverse cascade* enforces standards back to foreign manufacturers by preventing domestic sale or distribution of products that don't adhere to the standard. The reverse cascade's effectiveness is amplified where these supply chains are unusually concentrated in a single or small handful of firms. This approach addresses US regulators' limited influence in foreign jurisdictions and relinquishes the need to monitor hundreds, if not thousands, of overseas manufacturers directly.

This attempt to squeeze an upstream participant in a supply chain is not unprecedented. In the 1990s, Canadian civil-society organizations successfully used pressure on US home-goods companies like Sears and Home Depot to enforce a set of public standards for logging practice and conservation on Canadian logging firms.[5] Much more recently, the US Defense Department's Cybersecurity Maturity Model Certification (CMMC) program adopted a requirement for prime vendors—large firms with many subsidiary suppliers—to be responsible for the adoption of good supply-chain security practices by their suppliers.[6] In the CMMC model, rather than force the DoD to map complex supply chains two or three steps removed from the end product, prime vendors are leveraged to enforce standards directly on their supply chains.

This paper will

- briefly summarize previous approaches to IoT security;
- outline the challenge of enforcing domestic standards on a globalized supply chain;
- develop and apply the reverse cascade to the case of Wi-Fi home routers; and
- make specific recommendations for the United States and the EU.

5 Benjamin Cashore, Graeme Auld, and Deanna Newsom, *Governing Through Markets: Forest Certification and the Emergence of Non-State Authority* (New Haven, CT: Yale University Press, 2004), https://www.jstor.org/stable/j.ctt1npqtr; Trey Herr, "Cyber Insurance and Private Governance: The Enforcement Power of Markets," *Regulation & Governance*, July 3, 2019, https://www.onlinelibrary.wiley.com/doi/abs/10.1111/rego.12266.

6 "Cybersecurity Maturity Model Certification (CMMC)," Office of the Under Secretary of Defense for Acquisition and Sustainment, March 18, 2020, https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf.

2. The Challenge of International Enforcement

Intensive manufacturing and technical industries have experienced broad globalization. Cars and trucks, as much as sophisticated medical devices or home Wi-Fi routers, are manufactured with components from a kaleidoscope of foreign countries. This section discusses the challenge of enforcing domestic standards for security and safety on foreign-based manufacturers, building on comparable examples in the automotive and medical-device industries.

While there is no shortage of proposed security and privacy standards, none has moved beyond voluntary best practices, and all lack enforcement requirements. In a recent example from March 2019, Senator Mark Warner and Representative Robin Kelly in the US Congress introduced the Internet of Things Cybersecurity Improvement Act (S.734 and H.R. 1668). While it would certainly be a step in the right direction, the bill is limited in only addressing federal government procurement and use of IoT devices, leaving IoT purchases by millions of US consumers largely unprotected. Around the same time, California enacted its own IoT security law (S.B. 327), which had its own enforcement complications, including ambiguity—the California law requires connected devices to have "a reasonable security feature," without much guidance as to what those security features should include, beyond the devices having unique default passwords or requiring users to set their own passwords.[7]

The EU has been actively engaged with these issues. In early 2019, the European Standards Organization, ETSI, launched the world's first regional industry standard on Internet-connected consumer devices.[8] The standard was built on the United Kingdom's Code of Practice for Consumer IoT Security, which outlined recommended best practices for manufacturers of consumer IoT devices and associated services.[9]

As of this writing, the United States does not yet have a formal enforceable standard for IoT security. However that could change soon, with institutions in the EU setting a strong example, the International Organization for Standardization (ISO) gradually publishing standards for data security, cryptography, and IoT interoperability, and the National Institute of Standards and Technology (NIST) working on establishing a "Core Baseline" of security capabilities in IoT devices.[10] However, even if a formal security standard were to be adopted within the next few years, the reality of a globalized supply chain for consumer IoT products will pose a serious challenge for enforcement. This challenge is especially relevant and significant for the IoT, because most basic components and products are engineered abroad, outside of the regulatory jurisdiction of the United States.

It is worth noting that automobiles and medical devices differ markedly from Internet-connected devices in the economics driving consumer and product incentives. Namely, cars and medical devices are both perceived as expensive and potentially dangerous—and with such high costs involved, the economics of security for these industries are quite different from those for a connected home appliance or toy. People buying smart speakers simply do not consider safety as much as they do when buying a new car. Due to the lack of demand signal for security from the consumer, smart-speaker makers do not prioritize security, either.[11]

Despite this important difference, these examples can still reveal useful insights. The manner in which these other industries hold suppliers to account for minimum standards of design and manufacturing can help inform an enforcement scheme for consumer IoT security.

Automotive Industry

More than six decades after the first recorded traffic death in the United States, and about fifty years after the first stop sign was installed in Detroit, Congress passed the 1966

7 Hannah-Beth Jackson, Information Privacy: Connected Devices, 327 California Senate Bill § (2018). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

8 Sophia Antipolis, "ETSI Releases First Globally Applicable Standard for Consumer IoT Security," ETSI, February 19, 2019, https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security.

9 "Code of Practice for Consumer IoT Security," Department for Digital, Culture, Media & Sport, October 14, 2018, https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security.

10 "ISO/IEC JTC 1/SC 27 — Information Security, Cybersecurity and Privacy Protection," International Organization for Standardization, accessed May 16, 2020, https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/committee/04/53/45306.html; "ISO/IEC JTC 1/SC 41 - Internet of Things and Related Technologies," International Organization for Standardization, accessed May 16, 2020, https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/committee/64/83/6483279.html; Michael Fagan, et al., "Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline (2nd Draft)," National Institute of Standards and Technology, January 7, 2020, https://doi.org/10.6028/NIST.IR.8259-draft2.

11 For a more in-depth discussion of the economic considerations in cybersecurity, see: Tyler Moore and Ross Anderson, "Economics and Internet Security: A Survey of Recent Analytical, Empirical, and Behavioral Research," Harvard Computer Science Group Technical Report, 2011.

National Traffic and Motor Vehicle Safety Act. The bill, a response to rising highway deaths and growing calls for vehicle-safety laws, established the National Highway Traffic Safety Administration (NHTSA) to improve passenger survivability and vehicular safety.[12]

While the law enables NHTSA to develop safety standards and track vehicle crashes, it devolves responsibility for certifying that automakers are meeting these standards to the companies themselves. Under this scheme, companies test their own vehicles and move them to market having self-certified to the NHTSA safety standards.[13] NHTSA then verifies this self-certification by independently auditing the safety performance of newly released vehicles, and fining manufacturers whose products fail to pass up to $6,000 per violation.[14]

Just as the NHTSA does not approve or certify motor vehicles for standards compliance itself, it also does not directly enforce standards on suppliers outside of the United States. Instead, the agency offers a set of best practices (based largely on the US Consumer Product Safety Commission's *Handbook for Manufacturing Safer Consumer Products*) for companies like Ford and General Motors to minimize regulatory risk from endangering life and safety, including selecting a responsible overseas business partner, inspecting foreign manufacturing facilities, and instituting quality-control measures throughout the distribution process in the United States.[15]

As such, the NHTSA's model of standards enforcement serves as an encouraging example that enforcement need not take on a purely adversarial nature. In this case, the regulatory body employs a strategy of cooperation and deterrence: working with the auto manufacturers to help them with compliance, while setting up mechanisms that discourage cutting corners in the safety-check and quality-assurance processes. The result of this approach is a system that achieves good safety outcomes for automobile drivers—the fatality rate per one hundred million vehicle miles traveled has consistently declined since 1975.[16]

Medical-Devices Industry

The US Food and Drugs Administration (FDA) was authorized by Congress to enforce the Federal Food, Drug, and Cosmetic (FD&C) Act in 1938, with authority over medical devices following in May 1976.[17] The FDA mandates that a specific class of medical devices be subject to a premarket approval (PMA) process to evaluate and approve their safety and effectiveness, and also requires post-market surveillance (PMS) by medical device makers to track and monitor their products for malfunction once they are being used by consumers.[18] A mix of direct inspection and self-reporting, the PMS process can result in safety notifications, warning letters, and recalls when issues are found in the products.

With more than one third of the medical devices in the United States being imported, international enforcement is a major part of the FDA's work.[19] To tackle the challenges of transparency and accountability in globalized supply chains, the Office of Regulatory Affairs plays a key role in enforcing the FD&C Act through international inspections. Any "drug, medical device, biological, and food products manufactured in foreign countries and intended for U.S. distribution" are subject to inspection for compliance with standards.[20] While it does not directly examine components in a medical device, the FDA evaluates the evidence provided by the manufacturer, including third-party attestations by testing labs. At the same time, the FDA also directly performs inspections in manufacturing facilities, including those abroad, to check their quality systems and ensure they use approved manufacturing practices.

The FDA takes a more hands-on approach compared to NHTSA's self-certification scheme for automobile safety. The agency itself often inspects the manufacturing process of each product, and rewards certifications of compliance. In the event that a violation is found through these inspections, the FDA has a variety of tools at its disposal—ranging from warning letters and injunctions to criminal prosecution

12 Bill Canis and Richard K. Lattanzio, "U.S. and EU Motor Vehicle Standards: Issues for Transatlantic Trade Negotiations," Congressional Research Service, February 18, 2014, https://www.hsdl.org/?abstract&did=751039.

13 Motor Vehicle Safety: Certification of Compliance, Pub. L. No. 89–563, § 30115, 49 U.S. Code (1996), https://www.govinfo.gov/content/pkg/USCODE-2009-title49/html/USCODE-2009-title49-subtitleVI-partA-chap301-subchapII-sec30115.htm.

14 "Recommended Best Practices for Importers of Motor Vehicles and Motor Vehicle Equipment," National Highway Traffic Safety Administration, accessed December 18, 2019, https://one.nhtsa.gov/Laws-%26-Regulations/Recommended-Best-Practices-for-Importers-of-Motor-Vehicles-and-Motor-Vehicle-Equipment.

15 Ibid.

16 "2018 Fatal Motor Vehicle Crashes: Overview," National Highway Traffic Safety Administration, October 22, 2019, https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812826.

17 "PMA Historical Background," US Food and Drug Administration, November 3, 2018, http://www.fda.gov/medical-devices/premarket-approval-pma/pma-historical-background.

18 "Premarket Approval (PMA)," US Food and Drug Administration, July 9, 2019, http://www.fda.gov/medical-devices/premarket-submissions/premarket-approval-pma; "Postmarket Requirements (Devices)," US Food and Drug Administration, December 1, 2018, http://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/postmarket-requirements-devices.

19 "FDA Globalization," US Food and Drug Administration Office of the Commissioner, November 27, 2019, http://www.fda.gov/international-programs/fda-globalization.

20 "Foreign Inspections Overview," US Food and Drug Administration Office of Regulatory Affairs, December 14, 2018, http://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/foreign-inspections/foreign-inspections-overview.

and heavy fines—to ensure that unsafe and unlawful products are removed from the market.[21]

While this allows for a far more comprehensive inspection process that catches potentially unsafe products before they go on the market, it also forces medical-device manufacturers to confront lengthy product-review periods stretching many months. Such prolonged review periods may be more acceptable for medical devices whose consequences for failure are far higher than a compromised smart refrigerator, but they demonstrate some consumer appetite for delaying products from market to be evaluated for security and safety. The FDA's approach also suggests that even in a complex international supply chain where lives are at stake, effective security standards can be designed, adopted, and enforced without crippling industry. The FDA also offers a model of exhaustive technical evaluation that could also be formalized and shifted to third-party auditors. Finally, the NHTSA and FDA together demonstrate that demand from consumers for safe and secure products in a marketplace helps push product manufacturers toward standards compliance, while also reinforcing the authority and efficacy of regulators' enforcement power.

FDA in Focus

The FDA faces significant challenges in the coming decades as the food, pharmaceuticals, and medical-devices industries continue to grow. The FDA has had to increasingly rely on third-party testing labs and assessors in order to carry out regulatory evaluation and enforcement. Because third-party testing is always paid for by the manufacturers, perverse incentives and conflicts of interest may arise without adequate oversight. This problem is compounded by the fact that—unlike matters more firmly grounded in the laws of physics and chemistry, like safety from electrical faults or proper sterilization—cybersecurity standards for secure design and implementation have been less consistent over time and are more subject to context, including the specific risk tolerance of individuals and organizations. This makes it more difficult for the FDA to develop and enforce a set of test criteria that is objective, repeatable, observable, and verifiable without regular attention and updating.

Consumer IoT

A central US regulator for consumer IoT devices is the Federal Trade Commission (FTC), which has been involved in policing electronic commerce and privacy since 1990.[22] The Consumer Product Safety Commission has an active agenda in this area as well. This paper focuses on the FTC because of its history of public enforcement actions against unsafe and insecure products. As the Internet of Things grew ubiquitous, so did the FTC's interest in IoT as a domain of consumer protection. The FTC was one of the first regulators on the IoT scene, hosting a workshop in November 2013 to discuss security and privacy risks, and later publishing recommended best practices for IoT companies.[23] The FTC's work across a number of consumer IoT security cases has been complicated by the challenge of international enforcement—IoT product manufacturers based abroad are not legally compelled to respond to FTC actions against them.[24]

Nowhere is this better highlighted than the FTC's recently settled case against D-Link Corporation. In January 2017, the FTC issued an official complaint against the Taiwanese IoT manufacturer and its US subsidiary D-Link Systems for failing "to take reasonable steps to secure the routers and Internet-protocol cameras they designed for, marketed, and sold to United States consumers."[25] Contrary to D-Link's promises to consumers that its products were protected by "advanced network security," the FTC found that the company had failed to test its products for "well-known and easy-to-fix security flaws" before selling them to consumers. Among other security vulnerabilities, D-Link's products used hard-coded passwords that consumers could not change, and stored user credentials in plaintext, rather than encrypted and secret from attackers.[26]

The FTC ultimately settled the case in 2019, only after the parent company (D-Link Corporation) managed to extricate itself by separating from its US-based subsidiary, leaving the FTC to deal only with California-based D-Link Systems. The FTC forced the US-based firm to discontinue certain practices that left consumers vulnerable to security and privacy risks. The FTC settled another case on a data-security breach last year, underlining its newfound focus on

21 "Types of FDA Enforcement Actions," US Food and Drug Administration Center for Veterinary Medicine, November 3, 2018, http://www.fda.gov/animal-veterinary/resources-you/types-fda-enforcement-actions.

22 Chris Jay Hoofnagle, *Federal Trade Commission Privacy Law and Policy* (Cambridge, UK: Cambridge University Press, 2016).

23 "FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks," Federal Trade Commission, January 27, 2015, https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices.

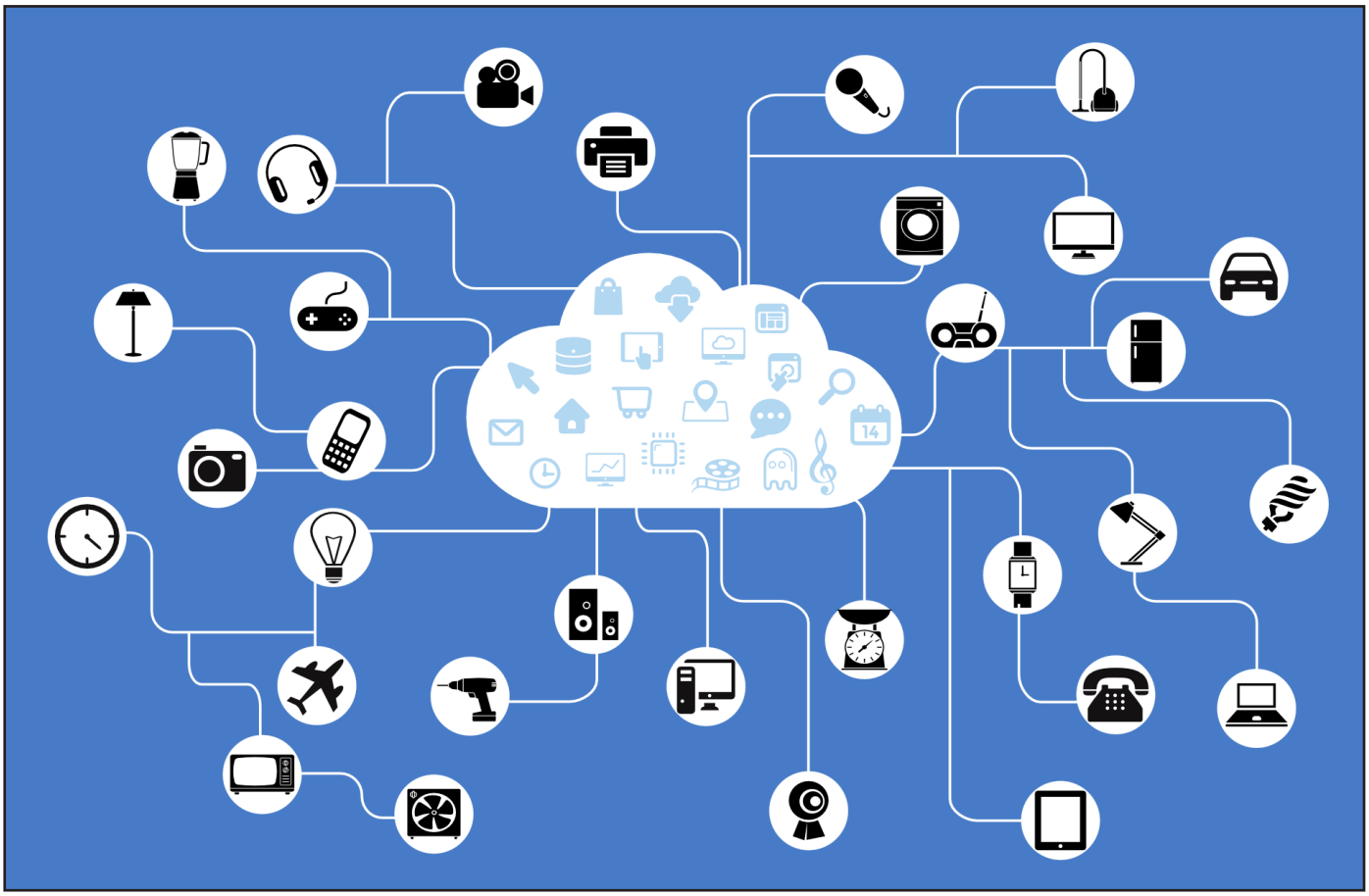
24 Regulatory action is not a hard and fast requirement for positive change in the marketplace for IoT; indeed, the threat of costly and potentially disruptive regulatory action could serve as incentive to change enough. This paper focuses on the role of the FTC in the proposed regulatory scheme to work through the content of this proposal to address foreign-manufactured and insecure products.

25 "D-Link," Federal Trade Commission, July 2, 2019, https://www.ftc.gov/enforcement/cases-proceedings/132-3157/d-link.

26 Leslie Fair, "D-Link Settlement: Internet of Things Depends on Secure Software Development," Federal Trade Commission, July 2, 2019, https://www.ftc.gov/news-events/blogs/business-blog/2019/07/d-link-settlement-internet-things-depends-secure-software.

the security of consumer technology. LightYear Dealer Technologies ("DealerBuilt"), an Iowa company that sells data-management software to auto dealerships nationwide, was held to account after a "hacker gained access to the unencrypted personal information of about 12.5 million consumers stored by DealerBuilt customers."[27] Notably, the FTC was able to point to the Standards for Safeguarding Customer Information Rule (16 C.F.R. Part 314) of the Gramm-Leach-Bliley Act, which required DealerBuilt to develop and maintain a comprehensive information-security program to protect customer information from this kind of breach. The DealerBuilt case also shows that the FTC does not have to wield rulemaking authority to cause companies to correct problematic practices—it can instead leverage existing standards to support its regulatory actions against companies. The reverse-cascade proposal builds on this precedent and suggests a way to leverage a coherent set of external security standards to drive change in IoT design and manufacturing.

In connection with the DealerBuilt case, the FTC's D-Link action also helped communicate the FTC's focus on consumer security. But, the D-Link settlement underlines the limitations of any domestic regulator in trying to shift the incentives and behavior of a foreign company to adopt acceptable security practices. Even with the additional leverage afforded by the existence of a US subsidiary, the FTC was unable to hold the parent company accountable for its lack of care in the security of its products. This is because the FTC—or any US government agency, for that matter—does not have legal authority over companies based abroad. Getting this right is critical—consumer IoT cybersecurity has impacted, and will continue to impact, people and the physical world, causing harm and potentially death. The consequences of IoT security are not confined to users alone. The D-Link case highlights the need for a policy tool that would enable domestic regulators to bring pressure on foreign-based companies, especially in the case of IoT, where the bulk of manufacturing happens outside the United States.



27 "Auto Dealer Software Provider Settles FTC Data Security Allegations," Federal Trade Commission, June 12, 2019, https://www.ftc.gov/news-events/press-releases/2019/06/auto-dealer-software-provider-settles-ftc-data-security.

3. The Reverse Cascade

Enter the reverse cascade. This paper proposes a policy tool premised on strategic upward pressure applied to information and communications technology (ICT) product supply chains, using domestic distributors as a point of leverage to enforce standards on foreign-based manufacturers. This section develops a detailed case study of how this reverse cascade would apply to home Wi-Fi routers.

The FTC and other domestic regulators should recognize and exploit the fact that while supply chains are global, they often terminate with a domestic distributor. The reverse cascade starts with applying regulatory pressure on the distributor to sell products that adhere to a specified set of design and manufacturing standards. In a competitive market like home routers, where multiple vendors compete in the same product segments, a small number of compliant vendors could threaten others' market access through distributors in the same jurisdiction. This creates subsequent pressure from vendors up their own supply chain for hardware components and software.

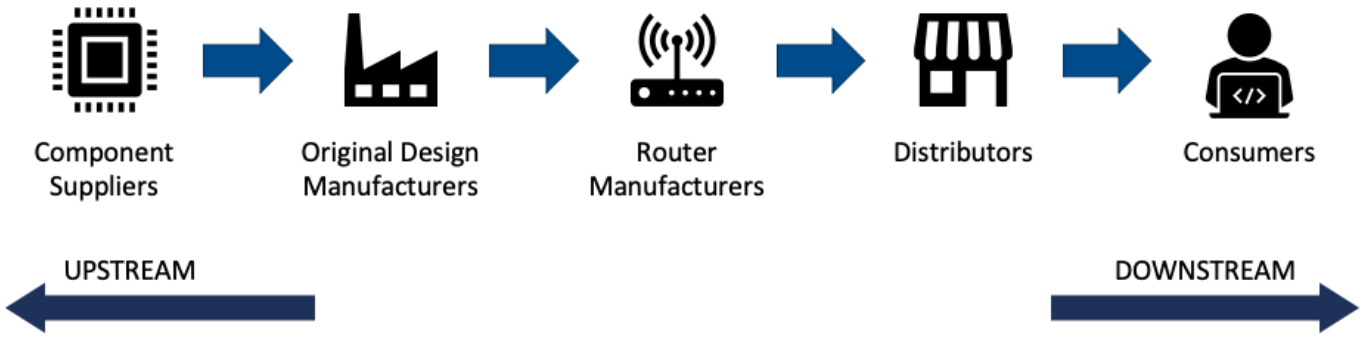
Home Wi-Fi Routers and IoT Security

The reverse cascade's essential components are a regulator's jurisdiction over a domestic distributor and a source of security standards. The home Wi-Fi router is a particularly useful example because its security impacts the security of all other devices connected to it. Home routers are also representative of other consumer IoT products; routers are mostly inexpensive consumer-electronics products largely built offshore by a plethora of foreign manufacturers.

Routers can be understood as the entrance between a home's local network and the broader Internet. Routers are responsible for ensuring data is "routed" correctly from sender to destination, and can manage a variety of network maintenance and security functions, such as firewalls to block malicious or sensitive content, running virtual private networks (VPNs), and limiting the bandwidth of the network to particular sites or at high-demand times of day.[28] As a network switch, a router also helps computers communicate with each other within the same network, acting as a communications hub for computers and other IoT devices.[29]

The router's role as Internet gateway and network hub makes it an important and useful case study on security risks in the Internet of Things. Absent an independent cellular connection, all connected devices in the home talk to the router, sending sensor and user data, as well as receiving the manufacturer's software updates. It is, therefore, not surprising that the router has been a frequent target for security breaches and exploitation. In May 2018, the Federal Bureau of Investigation (FBI) found "hundreds of thousands of routers" had been compromised by Russian hackers to "collect user information or shut down network traffic."[30] Another investigation less than a year later found that up to one hundred and thirty thousand Asus routers

Figure 1. Simplified illustration of Wi-Fi rout er supply chain



28 Lauren Hockenson, "This Is How a Router Really Works," *Mashable*, February 4, 2013, https://mashable.com/2013/02/04/router-faq/.

29 Jason Fitzpatrick, "Understanding Routers, Switches, and Network Hardware," *How-To Geek*, July 5, 2017, https://www.howtogeek.com/99001/htg-explains-routers-and-switches/.

30 "FBI Warns Russians Hacked Hundreds of Thousands of Routers," Reuters, May 29, 2018, https://www.cnbc.com/2018/05/29/fbi-warns-russians-hacked-hundreds-of-thousands-of-routers.html.

Securing the Router

What does it mean for a Wi-Fi router to be secure? One way to assess a Wi-Fi router's security is by thinking in terms of its components: hardware, software, and firmware.

Hardware: All routers have some kind of microprocessor to enable the device to blink and route data over antennas and cables, as well as a radio for wireless signals. These are usually combined on printed circuit boards that physically support the chips, as well as connect the chips to other components and a power supply. Hardware security can involve unnecessarily easy access to the microprocessor and radio, unused ports that are open for surreptitious malicious physical connections, or the use of components without adequate security safeguards. Recommendations to avoid hardware vulnerabilities include limiting the number of physical external ports, and integrating security hardware directly on the microprocessor to validate all of the hardware attached to the router, inside and out, on startup.[1]

Software: Software has eaten the world, and routers right along with it. Long a "set it and forget it" kind of device, routers were something most people rarely interacted with after initial setup. In recent years, however, routers have become more sophisticated as users look to them for additional security and network-management functionality. Manufacturers have moved to include small applications to collect data and shape network behavior, even on low-cost routers. Some of these applications are open-source projects, but most are developed by router manufacturers or an expanding network of third-party developers. The principles of secure software development fit well here; developers should be securing user credentials and sensitive data with widely used cryptographic protocols, and ensuring users can receive signed updates to prevent unauthorized changes.[2]

Firmware: Firmware is software built for a specific hardware component to permit interaction with the user and higher-level applications Essentially, firmware is what lets a hardware device communicate with hardware and software. Firmware for routers is typically written by the router manufacturers, who take code that is widely available on open-source projects such as DD-WRT (https://dd-wrt.com/) and customize it for their products, including adding or modifying security functionality. Unfortunately, router manufacturers consistently fail to properly secure their firmware. A recent study by the Cyber Independent Testing Lab (CITL) examining thousands of firmware samples from popular router brands revealed poor security across the board and, worse, little meaningful improvement from versions spanning the last fifteen years. CITL examined thousands of firmware versions issued by some of the most highly rated router brands, including Asus, D-Link, Linksys, and Netgear. Astoundingly, firmware updates issued by manufacturers were, on average, more likely to weaken security.[3] "There is no consistent security industry practice. It's very haphazard, and any features that we found appeared to be there by accident," Sarah Zatko, chief scientist at CITL, explained to the author. "There's just no evidence that any of the vendors we looked at [in the study] prioritize security in that way."[4]

1 "Mapping Security & Privacy in the Internet of Things," Copper Horse, September 24, 2018, https://iotsecuritymapping.uk/code-of-practice-guideline-no-6/.

2 "Secure by Design," Department for Digital, Culture, Media & Sport, March 7, 2018, https://www.gov.uk/government/collections/secure-by-design.

3 "Binary Hardening in IoT Products," Cyber Independent Testing Lab, August 26, 2019, https://cyber-itl.org/2019/08/26/iot-data-writeup.html.

4 Sarah Zatko, chief scientist, Cyber Independent Testing Laboratory, interview by Nathaniel Kim, January 24, 2020.

contained a software-security flaw that could enable massive identity theft.[31]

A poorly secured router leaves every connected device on its network vulnerable to an attack. Router manufacturers have a responsibility to implement basic secure design and manufacturing standards and to mitigate known vulnerabilities. The D-Link case makes the US government's position clear—these manufacturers will be held accountable for reasonable security processes and practices, or will else be held liable for unfair or deceptive practices. The FTC's public settlement with D-Link goes so far as to attach a relevant international standard for the security of industrial automation-and-control systems (IEC 62443-4-1) as an exhibit of these reasonable processes. So, how to drive enforcement on foreign manufacturers?

31 Thomas Brewster, "FBI Warned of Fraudster's Paradise: Up To 130,000 Hacked Asus Routers on Sale For A Few Dollars," *Forbes*, February 28, 2020, https://www.forbes.com/sites/thomasbrewster/2020/02/28/fbi-warned-of-fraudsters-paradise-up-to-130000-hacked-asus-routers-on-sale-for-a-few-dollars/.

Home Wi-Fi Router Supply Chains

Similar to many high-tech industries, the home router industry's supply chain is large and complex, with a web of connections across vendors along the chain.[32] Figure 1 serves as a simplification of those supply chains, capturing the basic roles and types of companies involved.

There are four key stages in a typical Wi-Fi router supply chain, before reaching the consumer, that matter for security: component suppliers; original design manufacturers (ODMs); router manufacturers; and distributors. The flow from initial components to the finished product is often referred to as going "downstream," and the opposite direction "upstream."

1. **Component suppliers:** The vendors of hardware, software, and firmware components for the router (e.g., Broadcom, which manufactures radio chips and antenna).

2. **ODMs:** ODMs design and mass produce hardware that product manufacturers can purchase as private or white-label products. The product manufacturers then sell the products under their own names.[33] An ODM can be seen as the final assembler of various components before the finished product is sent to the router manufacturer for branding and marketing. Foxconn (which acquired Belkin and its Linksys portfolio in 2018) also provides ODM services to router manufacturers.[34]

3. **Router manufacturers:** These are the companies whose names are on routers and manage their sales to distributors. Popular brands include Netgear, Belkin, Linksys, Asus, Huawei, TP-Link, and D-Link. Of these, only Netgear and Belkin (which acquired Linksys in 2013) are based in the United States; the rest are in China or Taiwan.

4. **Distributors:** While some router manufacturers sell their products directly to consumers through their own brand stores (e.g., Google sells its Nest Wi-Fi routers through its online store), most products reach consumers through third-party retailers like Best Buy or Amazon, or consumer Internet service providers like Comcast, which buys and rents routers from companies like Arris and Cisco.[35]

> ODMs are different from OEMs (original equipment manufacturers). OEMs offer technical expertise and mass-production services to other companies that bring their own designs. For example, Apple as the product manufacturer can bring its iPhone design to Foxconn the OEM to manufacture according to Apple's specifications. By contrast, ODMs design and manufacture products themselves.[36]

The Reverse Cascade in a Wi-Fi Router Supply Chain

The reverse cascade begins with domestic distributors. Assume a product whose manufacturer is based in a foreign country, but with a local distributor.[37] A regulator, like the FTC, identifies an adequate IoT security standard for manufacturers and vendors. This could be an international standard, a National Institute of Standards and Technology (NIST) publication like the recent NIST Internal Report 8259 defining an IoT design security baseline, or even something integrated into a law enacted by Congress.[38] This standard serves as the baseline the FTC can point to for distributors of relevant products. A distributor caught selling an IoT device whose design or manufacture fails to meet this standard would be subject to an enforcement action under FTC's authority to challenge deceptive or unfair trade practices.

Threat of action from the FTC, and resultant penalties, creates a strong incentive for distributors to look upstream and evaluate their potential vendors according to the IoT security standard; for example, Best Buy could demand that all routers

32 Kate Crawford and Vladan Joler created a fascinating mapping of the components and supply chain for an Amazon Echo. Crawford and Joler, "Anatomy of an AI System," 2018, https://anatomyof.ai/.

33 Kai Huang, "OEM vs ODM: Difference between OEM and ODM: OEM and ODM," *China Sourcelink*, October 21, 2018, https://cnsourcelink.com/2018/06/04/oem-vs-odm/.

34 Jacob Kastrenakes, "Foxconn Buys Belkin, Linksys, and Wemo," *Verge*, March 26, 2018, https://www.theverge.com/2018/3/26/17166272/foxconn-buys-belkin-fit-linksys-wemo.

35 "Overview of Xfinity Gateways," Xfinity, September 10, 2012, https://www.xfinity.com/support/articles/broadband-gateways-userguides.

36 While Foxconn was made famous because Apple uses it as an OEM for most of its smartphone manufacturing, many Wi-Fi router companies also go to Foxconn for its ODM services. Foxconn has also grown its in-house router business significantly through the acquisition of Belkin in September 2018.

37 For the purposes of the reverse cascade, the relevant cases are when the router manufacturer sells poorly secured products through a third-party retailer or broadband provider. If the manufacturer sells poorly secured products directly to the customer through its own brand stores, the FTC would be able bring a case directly against that manufacturer on the grounds of unfair practices since the firm would be failing to take reasonable steps to secure products according to the security standard.

38 Fagan, et al., "Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline (2nd Draft)."

placed on its shelves follow the new standard. This would put pressure on router manufacturers to certify adherence to those steps they could control and pressure their ODMs and component manufacturers on the remainder.

Continuing the example, assume Best Buy pressures Netgear, threatening to move to a competing manufacturer unless Netgear brings its Nighthawk router into compliance with the IoT security standard. Netgear can account for some of the router's software and functionality, such as eliminating the use of default passwords, but must turn upstream in the supply chain for more. Netgear might levy new requirements on contracts with a component manufacturer like Broadcom (a chipset builder) and ODMs like Foxconn to follow the relevant design and manufacturing principles of the IoT security standard. Where vendors refuse, Netgear looks to alternatives. The FTC's initial action on the US distributor drives a cascade of actions up the supply chain, helping to overcome legal and geographic boundaries to influence behavior globally.

When there are only a few firms concentrated at a single step in the upstream supply chain, pressure from the distributor can be passed up to greater effect and, potentially, speed. One such point is within the component-manufacturing phase. Chipset manufacturers integrate the components of a computer, including the central processing unit, memory, and storage into a single board. The majority of home Wi-Fi routers use chipsets manufactured by just a handful of companies: Broadcom, Qualcomm Atheros, Marvell, and Annapurna Labs.[39] Simplifying things for US regulators, Broadcom and Qualcomm are both headquartered in the United States, and would thus be directly subject to an applicable new IoT security standard.

Another promising pocket of concentration exists at the ODM step. Brian Knopf, a security researcher who worked as director of application security for Linksys and Belkin, observed that just a handful of ODMs in the world are responsible for supplying Wi-Fi router companies. He explained this at a DEF CON talk.

"If you start looking for vulnerabilities, and you find, 'Hey—Linksys has a vulnerability,' the question is, is it really a Linksys vulnerability, or is it Edimax, Arcadyan, Sercomm, or any number of the ODMs used by tons of vendors, like Asus, Netgear, D-Link—they're using a lot of the same ODMs…What you'll find is, if you put the pressure on the right place, we can get things fixed a lot easier."[40]

The prospect of holding distributors to account for the security of their products is not far-fetched. Major third-party retailers, such as Target and Best Buy, already require vendors to comply with relevant safety and quality standards.[41] These same two firms have also advocated for testable IoT standards that would enable businesses to "make consistent representations to customers regarding the security and privacy attributes of the IoT devices they offer."[42] Among third-party retailers, Best Buy, Walmart, and Amazon collectively account for a significant majority of consumer electronics sales in the country.[43] In the United States, there is also a relative paucity of home internet service providers (ISPs)—further limiting the number of firms that independently source routers and need to enforce a new IoT security standard. Less than a dozen broadband providers, including such names as Comcast, Charter, AT&T, Verizon, and CenturyLink, serve all connected US households, and the top-three providers own more than half the market.[44]

Part of the FTC's prospect for success is enforcing this standard across all major router distributors in the United States at the same time. Ideally, this action could be taken in concert with EU regulators in the digital single market. The FTC or other domestic regulators' use of an international security standard would only make this easier. While a monumental task of political coordination, such transatlantic alignment would benefit from the IoT's rising popularity as a topic in security policy. Cross-national action would help minimize the risk of noncompliant manufacturers simply hopping across a border and continuing to sell their wares online.

39 "Understanding Router Chipsets: Broadcom vs. Atheros vs. Marvell," *FlashRouters Networking & VPN Blog* (blog), January 22, 2018, https://blog.flashrouters.com/2018/01/22/understanding-router-chipsets/.

40 "DEF CON 23 - IoT Village - Brian Knopf - Yes You Can Walk on Water," 2015, YouTube video, https://www.youtube.com/watch?v=aTirAl-B-dl.

41 "Product Safety and Quality Assurance Tools and Processes," Target Corporate, accessed February 13, 2020, http://corporate.target.com/corporate-responsibility/responsible-sourcing/product-safety-quality-assurance/product-safety-and-quality-assurance-tools-and-pro.

42 "Fiscal Year 2019 Corporate Responsibility & Sustainability Report," Best Buy, accessed February 13, 2020, https://corporate.bestbuy.com/wp-content/uploads/2019/06/FY19-full-report-FINAL-1.pdf.

43 Consolidated data on router sales by retailer are difficult to find. However, a couple sources seem to indicate that Best Buy, Walmart, Amazon, and Target are the leading consumer electronics retailers, which could serve as proxy data for home router sales. "Best Buy: The Largest Consumer Electronics Retailer," Market Realist, https://marketrealist.com/2015/01/best-buy-largest-consumer-electronics-retailer/; "Share of Consumer Electronics Units," Seeking Alpha, https://static.seekingalpha.com/uploads/2012/4/9/saupload_Share-of-Consumer-Electronics-Units.png.

44 "Market Share of Three Largest U.S. Broadband Providers 2006-2013," Statista, accessed February 12, 2020, https://www.statista.com/statistics/256424/market-share-of-three-largest-us-broadband-providers/;S. O'Dea, "Number of Broadband Internet Subscribers in the United States from 2011 to 2019, by Cable Provider," Statista, March 10, 2020, https://www.statista.com/statistics/217348/us-broadband-internet-susbcribers-by-cable-provider; S. O'Dea, "Charter U.S. Broadband Internet Subscribers 2009-2018," Statista, February 27, 2020, https://www.statista.com/statistics/292366/charter-internet-broadband-subscribers/.

4. Recommendations

IoT security is a pressing national security issue, as these devices increasingly permeate homes and lives. The home Wi-Fi router is a good example of the IoT security challenge, and helps to illustrate the reverse cascade in action. Implementing this approach requires a handful of steps in the policy community and industry.

Clarity on Enforcement: While the FTC has successfully leveraged its authority to police unfair or deceptive trade practices to go after firms with poor security practices, this is a slow process requiring demonstration of harm. The Senate Commerce Committee should make a small, but important, change to Section 5(a) of the FTC Act, adding "unsafe acts or practices" to the current statute's provision for "unfair or deceptive acts or practices." Together with the DealerBuilt, LabMD, and D-Link precedents, this should clarify FTC's enforcement authority on cybersecurity issues, and allow for action prior to the imposition of harm where practices are demonstrably unsafe in a lab environment or based on expert consensus.

Pick a Baseline: The linchpin of the reverse cascade for IoT is an international, or at the least broadly recognized, set of standards for the secure design and manufacturing of IoT devices. These standards will need to encompass a variety of different product types and manufacturing stages. To avoid excessive fragmentation, it would be desirable for this recognized baseline, or framework, to permit the inclusion and relative cross-compatibility of specific standards. The earlier portion of this paper suggested several candidates, but additional endorsement by US and EU cybersecurity agencies would help elevate and focus on one. The Cybersecurity and Infrastructure Security Agency of the US Department of Homeland Security together with NIST and the EU Agency for Cybersecurity (ENISA) play important, if somewhat differing, roles in their respective cybersecurity policy apparatuses. Agreement from both agencies that a single IoT security standard was their focus, and an adequate guide for secure design and manufacturing, would support efforts such as the reverse cascade to bring pressure on non-expert distributors and IoT firms alike. The Cyberspace Solarium Commission's proposal for a National Cybersecurity Certification and Labeling Authority (NCCLA) would fit well with this recommendation. A future NCCLA would be the logical entity to pick up and endorse such an international standard, as well as taking on responsibility for supporting its continued development over time.

Create a Label for Good Security Practices: There are frequent debates about how to better leverage the consumer marketplace to reward good security practices. A label for adherence to security standards under the baseline mentioned would be a useful foundation for this proposal and related efforts to improve consumer decision-making about secure products and services. A recent survey by a cybersecurity firm found that nearly three quarters of consumers expected their IoT devices to be secured by the manufacturers, with 87 percent believing that it is the manufacturers' responsibility to do so.[45] A future NCCLA, or an existing agency like NIST, could create a simple labeling scheme for the selected international standard—creating a second source of pressure on distributors and, thereby, manufacturers. Properly labeled products could help mobilize consumers against insecure alternatives, filling the gap while FTC enforcement actions work to conclusion against non-compliant manufacturers. Rather than require complex evaluation and auditing, the use of a single standard would allow standardized technical assessment of new products to assign a suitable label per this scheme. This would avoid unnecessary demand on specialized technical skillsets, and permit the existing healthy market of consulting and compliance firms to support audits in line with this label.

Align Standards and Collaborate with Allies: To prevent manufacturers or distributors from jurisdiction hopping, the United States and key allies in the EU should make it a priority to align on an appropriate international security baseline and coordinate enforcement actions. This is not an inconsiderable challenge, since the EU organizes its efforts to coordinate national activities on consumer safety and competition differently than the United States. A good starting point would be for the FTC to collaborate with the EU's Directorate General for Competition Policy and other national government agencies as appropriate, to drive an IoT security-enforcement working group.[46] It will take time to converge these and other agencies' theories of action, especially moving in advance of demonstrated harm to the public. The earlier this coordination starts, the better.

45 "Survey: Consumer IoT Customers Expect Manufacturers to Embed Security in Devices," *Karamba Security* (blog), December 8, 2019, https://www.karambasecurity.com/blog/2019-12-08-consumer-iot-survey.

46 Statista, "IoT Market Size by Country in Europe 2014 and 2020," November 28, 2016. https://www.statista.com/statistics/686435/internet-of-things-iot-market-size-in-europe-by-country/.

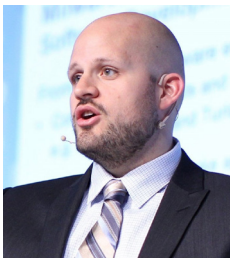
Conclusion

For many years, experts both in and out of government have been calling for a set of standards to hold manufacturers accountable for poor software and hardware security. The rising pace of IoT adoption and continued insecurity of many widely accessible devices sets the stage for regulatory action of one kind or another soon. For many of these devices, manufacturers and key portions of the supply chain are based outside of the United States, presenting a challenge of enforcement in foreign jurisdictions.

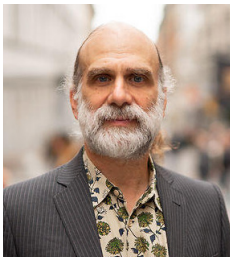
This paper presents the reverse cascade as a means to address this foreign-enforcement problem, encouraging regulators to leverage downstream distributors to ensure standards compliance by upstream foreign IoT manufacturers. Growing consumer awareness and demand for better security in smart devices, as well as internationally harmonized standards, will further aid enforcement efforts and help improve the security of IoT devices. This is about more than just keeping thousands of home routers safe from hacking—addressing foreign enforcement of security standards is an essential hurdle that governments must clear in order to ensure that digital transformation continues to provide benefits without compromising consumer product safety or national security.

About the Authors

Nathaniel Kim is a Presidential Management Fellow at the Office of Science and Data Policy in the U.S. Department of Health & Human Services, and an incoming Technology Law & Policy Scholar at Georgetown Law. He aims to help shape good policies for cyber safety and digital governance, and has written on the security and safety challenges of the Internet of Things as part of the OECD's Digital Economy Division and the Belfer Center for Science and International Affairs. He has previously worked as a researcher at Harvard Business School and as a consultant at the Economist Intelligence Unit. Nathaniel received an MPP from the Harvard Kennedy School and BS in Brain & Cognitive Sciences from MIT.



Dr. Trey Herr is the Director of the Cyber Statecraft Initiative under the Scowcroft Center for Strategy and Security at the Atlantic Council. His team works on the role of the technology industry in geopolitics, cyber conflict, the security of the internet, cyber safety, and growing a more capable cybersecurity policy workforce. Previously, he was a Senior Security Strategist with Microsoft handling cloud computing and supply chain security policy as well as a fellow with the Belfer Cybersecurity Project at Harvard Kennedy School and a non-resident fellow with the Hoover Institution at Stanford University. He holds a PhD in Political Science and BS in Musical Theatre and Political Science.



Bruce Schneier is an internationally renowned security technologist, called a "security guru" by the Economist. He is the New York Times best-selling author of 14 books -- including *Click Here to Kill Everybody* -- as well as hundreds of articles, essays, and academic papers. His influential newsletter Crypto-Gram and blog Schneier on Security are read by over 250,000 people. Schneier is a fellow at the Berkman-Klein Center for Internet and Society at Harvard University; a Lecturer in Public Policy at the Harvard Kennedy School; a board member of the Electronic Frontier Foundation, AccessNow, and the Tor Project; and an advisory board member of EPIC and VerifiedVoting.org. He is the Chief of Security Architecture at Inrupt, Inc.

Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor, Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org