Legacy Switches: A Proposal to Protect Privacy, Security, and the Environment from the Internet of Things

PAUL OHM* & NATHANIEL KIM†

The Internet of Things (IoT) promises us a life of automated convenience. Bright and shiny—if cheaply made and plasticky—"smart" thermostats, doorbells, cameras, and fridges carry out the functions once performed by "dumb" equivalents but in an automated, connected, and generally "better" way. This convenience comes at a significant cost. IoT devices listen to, record, and share our behavior, habits, speech, social interactions, and location minute-by-minute, 24/7. All of this information feeds a growing surveillance economy, as this data is bought, sold, and analyzed to predict our behavior, subject us to targeted advertising, and manipulate our actions. Many cheap IoT gadgets are developed on a shoestring budget, leaving them unsecure and vulnerable to attack. Malicious actors (and their automated computer programs) target IoT devices, breaking into them to spy on their owners or enlisting them into massive botnets used to cripple websites or critical infrastructure. These problems magnify over time, as IoT vendors focus on selling the next version of the device rather than on securing the preexisting installed base.

Consumers interested in protecting themselves from these harms may decide to replace outdated devices with newer, not-quite-yet-obsolete versions. Doing this does nothing to slow the growth of the surveillance economy and may even exacerbate it, as new devices tend to listen and record more than the models they replace. And even though replacing IoT devices can temporarily forestall security harms, asking consumers to replace all of their smart devices every few years introduces different harms. It harms the environment, filling our landfills with nonbiodegradable plastic housings and circuit parts which leach toxic materials into our air, soil, and water. It forces consumers to waste time, attention, and money tending to hard-wired, infrastructural devices that in the past would have lasted for decades. It compounds the

* Professor of Law, Georgetown University Law Center.

† J.D. Class of 2024, Georgetown University Law Center. The authors thank Elettra Bietti, Jody Blanke, Julie Cohen, John Duffy, Nikolas Guggenberger, Woody Hartzog, Thomas Kadri, Margot Kaminski, Nancy Kim, Amanda Levendowski, Aaron Perzanowski, Steve Salop, Chris Slobogin, and Susanne Wetzel for their helpful comments. We also thank the participants of the Georgetown Technology Law and Policy Colloquium, University of Colorado Technology Law Seminar, Consumer Law Scholars Conference, Privacy Law Scholars Conference, and the faculty workshops of the University of Georgia and Vanderbilt Law Schools for their many insightful comments.

harms of inequality, as those with more disposable income and connections to electricians and contractors have access to better security and privacy than those with less.

We propose a novel, simple, and concrete solution to address all of these problems. Every IoT device manufacturer should build a switch into their device called a "legacy switch." When the consumer flips this switch, it should disable the device's network connection, microphone, sensors, and any other features that contribute to security or privacy risks. A legacy switch will render a smart thermostat just a thermostat and a smart doorbell just a doorbell. Any user should find it easy to use and easy to verify whether the switch has been toggled.

This Article proposes legacy switches, elaborates key implementation details for any law requiring them, and connects them to the ongoing conversation about power, privacy, and platforms. The proposal to require legacy switches should be seen as a small but meaningful step toward taming the unchecked and destructive tendencies of the new networked economy.

TABLE OF CONTENTS

I. INTRODUCTION

Internet of Things (IoT) devices herald the future.[1] One step closer to providing the life of automated convenience promised in *The Jetsons* or *Back to the Future Part II*, these bright and shiny—if cheaply made and plasticky—

[1] The Department of Homeland Security defines IoT as "the connection of systems and devices with primarily physical purposes (e.g., sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems." U.S. DEP'T OF HOMELAND SEC., STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS 2 (Nov. 2016), https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf [https://perma.cc/UP2V-9J6F]. The Government Accountability Office defines IoT as "the technologies and devices that allow for the network connection and interaction of a wide array of devices, or 'things,' throughout such places as buildings, vehicles, transportation infrastructure, or homes." U.S. GOV'T ACCOUNTABILITY OFF., GAO-20-577, INTERNET OF THINGS: INFORMATION ON USE BY FEDERAL AGENCIES 1 (2020). Combined with the rise of artificial intelligence (AI), the IoT acts as a key driving force of digital transformation, bringing the physical and digital worlds together. *See* Iman Ghosh, *4 Key Areas Where AI and IoT Are Being Combined*, WORLD ECON. F. (Mar. 15, 2021), https://www.weforum.org/agenda/2021/03/ai-is-fusing-with-the-internet-of-things-to-create-new-technology-innovations/ [https://perma.cc/8LND-CE84].

"smart" thermostats, doorbells, cameras, and fridges carry out the same functions once performed by "dumb" equivalents but supposedly better in every way.[2] They learn from our behaviors, turning themselves on or off without our intervention.[3] They speak to us in soothing synthesized voices and listen to us from across the room.[4] They bristle with sensors that detect when we enter the kitchen or when a stranger approaches the front door.[5]

This future comes at a cost.[6] Almost all IoT devices embed tiny computers that wirelessly connect to the Internet, our smartphones, and one another.[7] Even when everything works as planned, these devices contribute to a growing and pervasive surveillance society, creating a detailed record of what individuals and groups do, say, think, and feel.[8] These records feed an expanding system of surveillance capitalism, through which powerful companies amass our deepest secrets, gain the power to manipulate our decisions, and profit by selling the traces of our lives to corporate partners and government actors.[9]

As if this were not bad enough, the problems compound when things inevitably do not go according to plan, as many IoT devices are developed on a

---

[2] *See, e.g.*, Simon Hill, *The Ultimate Guide to Setting Up Your Smart Home*, WIRED (Feb 23, 2023), https://www.wired.com/story/how-to-set-up-smart-home/ [https://perma.cc/WL5E-MK4J]; Anna Kodé, *Unwanted Connection: Who Has Control of Your Smart Home*, N.Y. TIMES (Feb. 17, 2023), https://www.nytimes.com/2023/02/17/real estate/smart-home-devices.html [https://perma.cc/J37A-GAZJ].

[3] *See* Hill, *supra* note 2.

[4] *Id.*

[5] *See id.*

[6] A growing literature identifies various harms posed by the Internet of Things and proposes legal reforms to address them. *See generally* Rebecca Crootof, *The Internet of Torts: Expanding Civil Liability Standards to Address Corporate Remote Interference*, 69 DUKE L.J. 583 (2019); Sara Sun Beale & Peter Berris, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, 16 DUKE L. & TECH. REV. 161 (2018); Charlotte A. Tschider, *Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age*, 96 DENVER L. REV. 87 (2018); Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, 50 U. MICH. J.L. REFORM 913 (2017); Stacy-Ann Elvy, *Hybrid Transactions and the INTERNET of Things: Goods, Services, or Software?*, 74 WASH. & LEE L. REV. 77 (2017); Margot E. Kaminski, Matthew Rueben, William D. Smart & Cindy M. Grimm, *Averting Robot Eyes*, 76 MD. L. REV. 983 (2017); Christina Mulligan, *Personal Property Servitudes on the Internet of Things*, 50 GA. L. REV. 1121 (2016); Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85 (2014).

[7] DAVID M. WHEELER, DAMILARE D. FAGBEMI & JC WHEELER, THE IOT ARCHITECT'S GUIDE TO ATTAINABLE SECURITY & PRIVACY 6 (2019).

[8] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 8 (2019).

[9] *Id.*; *see, e.g.*, JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 80–81 (2019) (discussing the "gamification of commercial surveillance" as an incentive to participation in the "surveillance economy").

shoestring budget, leaving them unsecure and vulnerable to attack.[10] Malicious actors (and their automated computer programs) target IoT devices, breaking into them to spy on their owners or enlisting them into massive botnets used to cripple websites or critical infrastructure.[11] These privacy and security problems magnify over time, as IoT vendors focus on selling the next version of the device rather than on securing the preexisting installed base.[12] Some IoT devices come with software that cannot be patched.[13] Those that can be patched often require a cumbersome and technical firmware update procedure that most users cannot master or be bothered to do.[14] Many devices are declared to have reached their "end of life" within a year or two, if they last that long,[15] rendering them security and privacy time bombs.

These outdated, unsecure IoT devices offer a vector for a host of harms from a collection of bad actors. Abusive ex-partners control the smart devices they leave behind to terrorize their victims.[16] Criminal syndicates and foreign powers

---

[10] *See* Beale & Berris, *supra* note 6, at 163–67; *Understanding the Role of Connected Devices in Recent Cyber Attacks: Hearing Before the Subcomm. on Commc'ns & Tech. and the Subcomm. on Com., Mfg., & Trade of the H. Comm. on Energy and Com.*, 114th Cong. 18 (2016) (statement of Bruce Schneier); Tatum Hunter, *Buggy Software in Off-Brand Smart Home Devices Is a Hacker's Playground*, WASH. POST (Nov. 18, 2021), https://www.washingtonpost.com/technology/2021/11/18/smart-home-security/ [https://perma.cc/LY5V-ZEEN].

[11] *See* Augustine Fou, *The Internet of (Creepy Spy-ey) Things*, FORBES (Sept. 1, 2020), https://www.forbes.com/sites/augustinefou/2020/09/01/the-internet-of-creepy-spy-ey-things/?sh=34a05ff25749 [https://perma.cc/ZL9G-KLYQ]; Beale & Berris, *supra* note 6, at 163–66; Elie Bursztein, *Inside Mirai the Infamous IoT Botnet: A Retrospective Analysis*, ELIE BURSZTEIN BLOG (Dec. 2017), https://elie.net/blog/security/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/ [https://perma.cc/S7FD-4ALT].

[12] Consider the smart home manufacturer Revolv, which marketed lights, alarms, and doors. Two years after acquiring Revolv, Google's Nest arm decided to disable their products, effectively "bricking" all of the Revolv devices consumers had purchased. Nick Statt, *Nest Is Permanently Disabling the Revolv Smart Home Hub*, VERGE (Apr. 4, 2016), https://www.theverge.com/2016/4/4/11362928/google-nest-revolv-shutdown-smart-home-products [https://perma.cc/UVZ4-8CCU]; Klint Finley, *Nest's Hub Shutdown Proves You're Crazy to Buy into the Internet of Things*, WIRED (Apr. 5, 2016), https://www.wired.com/2016/04/nests-hub-shutdown-proves-youre-crazy-buy-internet-things/ [https://perma.cc/KTZ9-9KPQ].

[13] Peppet, *supra* note 6, at 135–36 (describing how IoT devices often cannot be patched); FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY SECURITY IN A CONNECTED WORLD 13–14 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/ZX4S-MPCF].

[14] *See* Peppet, *supra* note 6, at 135–36; FED. TRADE COMM'N, *supra* note 13, at 13–14.

[15] *See* NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM., NISTIR 8228, CONSIDERATIONS FOR MANAGING INTERNET OF THINGS (IOT) CYBERSECURITY AND PRIVACY RISKS 8 (June 2019) [hereinafter NIST], https://doi.org/10.6028/NIST.IR.8228 [https://perma.cc/VT65-AD5C] (discussing the "differing lifespan expectations" of IoT devices).

[16] Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*, N.Y. TIMES (June 23, 2018), https://www.nytimes.com/2018/06/23/technology/smart-home-

amass massive armies of compromised smart devices to launch denial of service (DOS) attacks on rivals.[17] Creeps and snoops hack into the video and audio feeds from the cameras and microphones on these devices to spy on intimate moments.[18] As our homes have doubled as workspaces due to the COVID-19 pandemic, addressing the privacy and security risks posed by smart home devices has become ever more critical.[19]

Today, consumers interested in protecting themselves from these harms have only one effective self-help option: to replace a device with the newest, not-yet-obsolete version.[20] Forcing consumers to replace all of their smart devices every few years introduces new harms. It harms the environment, as the EPA has documented the crisis of e-waste, with our landfills filling with nonbiodegradable plastic housings that leak toxic materials into our air, soil, and water.[21] It forces consumers to waste time, attention, and money tending to hard-wired, infrastructural devices that in the past would have lasted for decades.[22] It compounds the harms of inequality, as wealthy people with disposable income

devices-domestic-abuse.html [https://perma.cc/FD6L-B5BW]; Dana Holmstrand, Note, *A Haunted (Smart) House: Smart Home Devices as Tools of Harassment and Abuse*, 6 GEO. L. TECH. REV. 223, 225–33 (2022); Kodé, *supra* note 2.

[17] *See, e.g.*, Bursztein, *supra* note 11; Steve Olshansky & Robin Wilton, *Internet of Things Devices as a DDoS Vector*, INTERNET SOC'Y (Apr. 11, 2019), https://www.internetsociety.org/blog/2019/04/internet-of-things-devices-as-a-ddos-vector/ [https://perma.cc/ETF2-RBW7].

[18] Neil Vigdor, *Somebody's Watching: Hackers Breach Ring Home Security Cameras*, N.Y. TIMES, https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html [https://perma.cc/T4NB-WATM] (Nov. 11, 2020); Amy B. Wang, *'I'm in Your Baby's Room': A Hacker Took Over a Baby Monitor and Broadcast Threats, Parents Say*, WASH. POST (Dec. 20, 2018), https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/ [https://perma.cc/NR4R-RMDB].

[19] *See* Danielle Abril, *Big Tech Is Pushing Smart Home Devices as the Latest Work-from-Home Tools*, WASH. POST (Nov. 22, 2021), https://www.washingtonpost.com/technology/2021/11/22/smart-home-devices-security-remote-workers/ [https://perma.cc/86KC-J35M]; *A Perfect Storm: The Security Challenges of Coronavirus Threats and Mass Remote Working*, CHECK POINT BLOG, https://blog.checkpoint.com/2020/04/07/a-perfect-storm-the-security-challenges-of-coronavirus-threats-and-mass-remote-working/ [https://perma.cc/3DA9-DGSB] ("71% of security professionals have noticed an increase in security threats or attacks since the beginning of the Coronavirus outbreak.").

[20] Cate Lawrence, *The IoT Graveyard: Device Obsolescence and the Right to Repair*, MEDIUM (Mar. 17, 2021), https://catelawrence.medium.com/the-iot-graveyard-device-obsolescence-and-the-right-to-repair-1857fb659529 [https://perma.cc/6S7B-H9X7].

[21] *See id.*; *Cleaning Up Electronic Waste (E-Waste)*, EPA, https://www.epa.gov/international-cooperation/cleaning-electronic-waste-e-waste [https://perma.cc/GA4Q-88JP] (Nov. 15, 2022).

[22] *See* Chris Jay Hoofnagle, Aniket Kesari & Aaron Perzanowski, *The Tethered Economy*, 87 GEO. WASH. L. REV. 783, 866 (2019).

and connections to contractors end up with better security and privacy than those with less.[23]

We propose a novel, simple, and concrete fix to address all of these problems. Every IoT device manufacturer should build a switch into their device we call a "legacy switch."[24] When the consumer flips this switch, it should disable any feature that contributes to surveillance capitalism or to the risk of other harms to privacy or security. A legacy switch will render a smart thermostat just a thermostat and a smart doorbell just a doorbell. The switch will disable microphones, sensors, and wireless connectivity. Any user should find it easy to use and easy to verify whether the switch has been toggled. Legacy switches will extend the life expectancy of devices, reducing the environmental toll of e-waste. They will restore choice and agency to the user, allowing them to opt out of a small part of the program of surveillance capitalism.

IoT device manufacturers are not likely to implement legacy switches without the government's encouragement. The Consumer Product Safety Commission (CPSC) and Federal Trade Commission (FTC) can use their current authorities to promulgate legacy switch standards and maybe even mandate them in some devices.[25] Congress and state legislatures should enact laws requiring legacy switches in long-lived devices that are prone to privacy or security harms.[26]

This proposal builds on broader trends in public policy and legal scholarship. It connects to an emerging literature on friction—a counter movement to normative theories of economic and other efficiency.[27] Given today's breakneck pace of innovation and change, often the best way to inject important human values into emerging technologies is to intentionally slow them down, to make them less efficient, less automated, and less streamlined.[28]

---

[23] *See* Maria Farrell, *The Internet of Things—Who Wins, Who Loses?*, GUARDIAN (Aug. 14, 2015), https://www.theguardian.com/technology/2015/aug/14/internet-of-things-winners-and-losers-privacy-autonomy-capitalism [https://perma.cc/YLM2-GHVJ]; Hannah Murphy, *Rich and Famous Turn to 'Personal Cyber Security' to Protect Phones*, FIN. TIMES (Jan. 30, 2020), https://www.ft.com/content/96c79040-40ea-11ea-bdb5-169ba7be433d [https://perma.cc/YJS9-KNH4].

[24] Although we have not before written about this proposal, Woody Hartzog has cited one of us as the progenitor of this idea, back when we referred to it as a "lobotomy switch," based on private conversations. *See* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 272 (2018).

[25] *See infra* Part IV.A.

[26] *See infra* Part IV.B.

[27] Paul Ohm & Jonathan Frankle, *Desirable Inefficiency*, 70 FLA. L. REV. 777, 803–05 (2018); Ellen P. Goodman, *Digital Fidelity and Friction*, 21 NEV. L.J. 623, 624–25 (2021) [hereinafter Goodman, *Digital Fidelity*]; William McGeveran, *The Law of Friction*, 2013 U. CHI. LEGAL F. 15, 17; *see also* Ellen P. Goodman, *Digital Information Fidelity and Friction*, KNIGHT FIRST AMEND. INST. (Feb. 26, 2020), https://knightcolumbia.org/content/digital-fidelity-and-friction [https://perma.cc/M999-ZFJY].

[28] Ohm & Frankle, *supra* note 27, at 785, 803–05.

This work is a close cousin to the "Right to Repair" movement, which declares that "if you can't open it, you don't own it" and has motivated significant state legislative reforms in recent years.[29] It turns the trendy focus on "design thinking" on its head by reinforcing the importance of thinking about design, while inviting the public—and its elected and appointed representatives—to participate in the design process.[30] In short, the proposal to require legacy switches should be seen as a small but meaningful step toward taming the unchecked and destructive tendencies of the new networked economy.

The Article proceeds in four additional parts. Part I considers the host of harms that result from the spread of cheap, poorly secured, panoptic IoT devices. Part II introduces the legacy switch proposal and connects it to emerging literatures about friction and design. Part III explores the legal bases for government mandates or incentives to bring about legacy switches and delves into many of the implementation details. Finally, Part IV offers some lessons legacy switches reveal for the broader project of designing new governance rules for the information economy.

II. IOT AND CONSUMER HARM

IoT devices pose threats to privacy, security, and the environment. Some of these threats are intrinsic to the underlying functionality while many others get worse over time. Consider each of the categories of harm below.

A. *The Internet of Things*

The Internet of Things (IoT) describes the wide range of technologies used to collect information through sensors and automate tasks that traditionally required manual human work.[31] The Organisation for Economic Co-operation and Development (OECD) has called it an "ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world."[32]

---

[29] *See* AARON PERZANOWSKI, THE RIGHT TO REPAIR: RECLAIMING THE THINGS WE OWN 10–11 (2022).

[30] HARTZOG, *supra* note 24, at 7–8.

[31] U.S. DEP'T OF HOMELAND SEC., *supra* note 1, at 1; U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 1, at 1; *What Is IoT?*, ORACLE, https://www.oracle.com/internet-of-things/what-is-iot/ [https://perma.cc/X9XC-H4E8]; Jennifer Stowe, *Automation and IoT: Transforming How Industries Function*, IOT FOR ALL (Oct. 12, 2020), https://www.iotforall.com/automation-and-iot-will-transform-how-industries-function [https://perma.cc/F3QX-KGS6].

[32] "The combination of network connectivity, widespread sensor placement, and sophisticated data analysis techniques now enables applications to aggregate and act on large amounts of data generated by IoT devices in homes, public spaces, industry and the natural world." ORG. FOR ECON. COOP. & DEV., THE INTERNET OF THINGS: SEIZING THE BENEFITS

We focus primarily on consumer-facing IoT, and especially on technologies associated with the smart home. The consumer market abounds with smart cameras, doorbells, televisions, thermostats, refrigerators, speakers, security systems, door locks, and more.[33] Significantly, many of these cheap consumer products replace devices that we once expected to last decades.[34] According to a 2007 study by the National Association of Home Builders, refrigerators have an average life expectancy of 13 years; doors (including their locks, presumably) are expected to last for the lifespan of the house; electrical components like light switches are expected to last 10+ years; and thermostats last 35 years.[35] In contrast, smart devices tend to be built from the kind of components and with the kind of hardware and software associated with smartphones, which last on average only 2 to 3 years.[36] It is unfathomable to imagine that a Nest thermostat manufactured in 2021 will continue to be supported and patched in 2031, much less thirty-five years from now![37]

AND ADDRESSING THE CHALLENGES 4 (May 2016) [hereinafter OECD], https://www.oecd-ilibrary.org/the-internet-of-things_5jlwvzz8td0n.pdf [https://perma.cc/B57B-R57J].

[33] Lucas M. Amodio, *The Intersection of Product Liability Law and the Internet of Things*, B.C. INTELL. PROP. & TECH. F. 1–2 (2021); Janet Morrissey, *The Race to Create the Coolest Smart Home Devices Is Hotter Than Ever*, N.Y. TIMES (Jan. 15, 2019), https://www.nytimes.com/2019/01/15/business/the-race-to-create-the-coolest-smart-home-devices-is-hotter-than-ever.html [https://perma.cc/L467-2PLE]; Kodé, *supra* note 2.

[34] Terrell McSweeny, *Consumer Protection in the Age of Connected Everything*, 62 N.Y.L. SCH. L. REV. 203, 213 (2017–2018) ("[A] consumer might buy an analog thermostat expecting it to last ten or more years, and she might understandably have the same expectation for the lifecycle of the thermostat's IoT equivalent. Manufacturers must either make clear to consumers how long to expect their devices will be supported or conform to reasonable consumer expectations."); FED. TRADE COMM'N, *supra* note 13, at 13 ("[A]lthough some IoT devices are highly sophisticated, many others may be inexpensive and essentially disposable.").

[35] NAT'L ASSN. OF HOME BUILDERS & BANK OF AM. HOME EQUITY, STUDY OF LIFE EXPECTANCY OF HOME COMPONENTS 7–11 (Feb. 2007) [hereinafter NAHB], https://www.hcmuddox.com/sites/default/files/library/nahb20study20of20life20expectancy20of20home20components.pdf [https://perma.cc/BN6B-C6V8].

[36] HARTZOG, *supra* note 24, at 268 ("The typical lifetime of software (the length of time that a company actively patches and updates any bugs or problems with the software) is around two years. But the estimated lifetime of some objects now connected to the Internet is around ten years."); *see also* Hoofnagle, Kesari & Perzanowski, *supra* note 22, at 789–90.

[37] GOOGLE NEST LEARNING THERMOSTAT PRODUCT ENVIRONMENTAL REPORT, GOOGLE 3, https://services.google.com/fh/files/misc/nestthermostat3rdgen_productenvironmentreport.pdf [https://perma.cc/KP62-ZS4C] (assuming a ten-year life cycle, spanning production, distribution, customer use, and recycling, for Nest thermostats in calculating environmental impact); *see* Ashkan Soltani, *What's the Security Shelf-Life of IoT?*, FTC (Feb. 10, 2015), https://web.archive.org/web/20210926093318/http:/www.ftc.gov/news-events/blogs/techftc/2015/02/whats-security-shelf-life-iot?utm_source=govdelivery ("If consumers are already exposed to security updates and end-of-life issues in more mature markets for routers and smartphones, one has to wonder what the security implication will be like of this new and rapidly emerging market of IoT.").

Although we are focused on the smart home, much of our analysis may extend to other IoT market segments. For example, smart city technologies include traffic control systems, street lighting, electrical meters, and transportation systems that similarly use embedded sensors, connectivity, and data processing capabilities to monitor and optimize energy use, traffic flows, and other municipal interests.[38] The risks to security and privacy from these devices are similar to what we document in the smart home.[39] The legacy switch solution can be extended to many smart city technologies without much modification, although we consider that outside the scope of this Article.

We are also not focused on so-called "wearable" devices worn or embedded on individuals, such as smartphones, smart watches, fitness counters, and sleep trackers.[40] Again, our discussion of the harms these devices may pose and the benefits of a legacy switch solution may apply to many of these technologies.

B. *Privacy and "Surveillance Capitalism"*

All IoT devices collect, compile, and process data about their users.[41] Smart speakers with digital assistants have been reported to retain a permanent record of not only our voice patterns but also the content of conversations,[42] while smartwatches and fitness trackers compile a wide variety of personal health information.[43] Smart TVs deploy automatic content recognition technology to

---

[38] *See* BEN GREEN, THE SMART ENOUGH CITY 3 (2019); Peter High, *The Top Five Smart Cities in the World*, FORBES (Mar. 9, 2015), https://www.forbes.com/sites/peterhigh/2015/03/09/the-top-five-smart-cities-in-the-world/?sh=1bd3663867ee [https://perma.cc/SWN2-BEAW] ("Examples of such systems include smart parking, where networked sensors enable congestion easing through both dynamic pricing and driver communications; smart grid, where PMUs and smart meter data serve to increase grid reliability; smart street lighting where LEDs and smart controllers enable reduced energy consumption according to footfall and traffic analysis.").

[39] *See generally* Janine S. Hiller & Jordan M. Blanke, *Smart Cities, Big Data, and the Resilience of Privacy*, 68 HASTINGS L.J. 309, 323–28 (2017).

[40] Matthew R. Langley, Note, *Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables*, 103 GEO. L.J. 1641, 1643–45 (2015).

[41] OECD, *supra* note 32, at 10 (discussing the IoT's ability to "create 'big data' ecosystems," which involve "[c]ollecting, compiling, linking and analysing very large data flows").

[42] Matt Day, Giles Turner & Natalia Drozdiak, *Amazon Workers Are Listening to What You Tell Alexa*, BLOOMBERG (Apr. 10, 2019), https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio [https://perma.cc/HYR5-PEPK].

[43] In comments provided to the National Telecommunications and Information Administration (NTIA), staff of the Federal Trade Commission's Bureau of Consumer Protection presented findings showing "the presence of numerous third parties in apps connected to IoT health and fitness wearable devices. A number of those third parties collected data such as persistent device identifiers, workout routines, eating habits, length of walking stride, medical search histories, zip code, gender, and geolocation." FTC, Comment

monitor the specific content viewed by users in order to deliver targeted ads, and often bury this fact in terms of use agreements or make it difficult for users to switch off monitoring.[44]

Just considering the sheer volume of data that is collected by IoT devices in the home can give a sense of the threat to privacy: A participant in a workshop hosted by the FTC in 2015 reportedly indicated that "fewer than 10,000 households using the [participant] company's IoT home-automation product can 'generate 150 million discrete data points a day' or approximately one data point every six seconds for each household."[45] That FTC workshop was eight years ago—one can only imagine how much more personal data has been collected by these devices as the number of IoT products sold globally has exploded.[46]

Privacy risks borne by IoT devices carry additional weight when considered in the context of the home.[47] Smart devices that we keep in our homes, ranging from motion sensors, to surveillance cameras, to smart speakers,[48] collect sensitive and intimate details from their users and transmit this information through the Internet as part of their regular functioning.[49]

Letter on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things 6 (June 2, 2016), https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-office-policy-planning-national-telecommunications/160603ntiacomment.pdf [https://perma.cc/ER8P-RF2N].

[44] *See* James K. Wilcox, *How to Turn Off Smart TV Snooping Features*, CONSUMER REPS., https://www.consumerreports.org/privacy/how-to-turn-off-smart-tv-snooping-features-a4840102036/ [https://perma.cc/2C84-M2R8] (Oct. 14, 2022); *see also* Press Release, FTC, VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent (Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it [https://perma.cc/E9T6-YCGU].

[45] FED. TRADE COMM'N, *supra* note 13, at 14.

[46] *See, e.g.*, Fredrik Dahlqvist, Mark Patel, Alexander Rajko & Jonathan Shulman, *Growing Opportunities in the Internet of Things*, MCKINSEY & CO. (July 2019), https://www.mckinsey.com/~/media/mckinsey/industries/private%20equity%20and%20principal%20investors/our%20insights/growing%20opportunities%20%20in%20the%20internet%20of%20things/growing-opportunities-in-the-internet-of-things-v5.pdf [https://perma.cc/WGE6-C82V].

[47] Crootof, *supra* note 6, at 596 n.48.

[48] Hill, *supra* note 2; Kodé, *supra* note 2; Lorenzo Franceschi-Bicchierai, *Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings*, MOTHERBOARD: TECH BY VICE (Feb. 27, 2017), https://www.vice.com/en/article/pgwean/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings [https://perma.cc/R7RL-2S6L]; David Kravets, *Sex Toys and the Internet of Things Collide—What Could Go Wrong?*, ARS TECHNICA (Sept. 13, 2016), https://arstechnica.com/tech-policy/2016/09/sex-toys-and-the-internet-of-things-collide-what-could-go-wrong/ [https://perma.cc/F777-BGL4].

[49] *See generally* Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1924–26 (2017) (discussing privacy implications of smart home products collecting and sharing personal information across third-party service providers and potentially the government).

IoT devices are inexpensive and sometimes sell for a price below the costs to the manufacturer,[50] indicating that they serve as loss leaders to other forms of value to the companies that sell them.[51] One source of value is the stream of information about people such devices collect and transmit back to the manufacturer, enabling them to compile a rich database of behavioral data the company can study to build other products, use to train machine learning models that predict user behavior, or resell to private parties or government agencies.[52]

Julie Cohen analogizes this activity to the extraction of natural resources, with information about human beings standing in for oil deposits or coal mines, the data sources being mined by corporate interests, with information about us like the oil driving the modern economy.[53] Shoshana Zuboff describes an emerging economic system of "surveillance capitalism," which renders human behavior and experience into information with which increasingly powerful platforms can profit on our secrets, predict our behavior, and manipulate us to act other than we would given ordinary free will.[54]

Cohen and Zuboff herald a growing group of scholars writing about harms to privacy much more broadly than others have in the past.[55] Beyond concerns about malicious bad actors or government officials spying on individuals, modern privacy scholars see unconstrained corporate data collection as the starting point for profound and unwelcome changes to the way society is ordered.[56] Neil Richards demonstrates how corporations and governments use data to exert power over individuals.[57] Alicia Solow-Niedermann focuses on how data and machine learning fuel inferential harms.[58] Salome Viljoen identifies relational harms.[59]

The harms of surveillance capitalism stem not only from what companies know about us, but also from their constant efforts to perform experiments on

---

[50] *See, e.g.*, Rich Smith, *Did Amazon Lose $100 Million Selling Its Most Popular Item?*, MOTLEY FOOL (Jan. 8, 2018), https://www.fool.com/investing/2018/01/08/did-amazon-lose-100-million-selling-its-most-popul.aspx [https://perma.cc/SC96-4VTA] (reporting research indicating that Amazon was selling its smart speaker products at a loss).

[51] *See* ZUBOFF, *supra* note 8, at 238 ("The very idea of a functional, effective, affordable product or service as a sufficient basis for economic exchange is dying.").

[52] *See, e.g.*, Day, Turner & Drozdiak, *supra* note 42; Matt Burgess, *The Internet of Things Is a Data Farm, Roomba Won't Be Its Only Profiteer*, WIRED (July 25, 2017), https://www.wired.co.uk/article/roomba-data-sell-internet-of-things [https://perma.cc/WM44-CRDF].

[53] COHEN, *supra* note 9, at 63–72.

[54] ZUBOFF, *supra* note 8, at 8.

[55] *See generally* COHEN, *supra* note 9; ZUBOFF, *supra* note 8.

[56] *See* ZUBOFF, *supra* note 8, at 8; *see also* COHEN, *supra* note 9, at 2.

[57] *See* NEIL RICHARDS, WHY PRIVACY MATTERS 7–8 (2021).

[58] *See* Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357, 361–64 (2022).

[59] *See* Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 580 (2021).

us and to manipulate our thoughts and behavior.[60] Brett Frischmann and Evan Selinger document myriad ways companies drive our choices.[61] Rebecca Crootof identifies this dynamic in the data collected through IoT devices specifically.[62] Much of this activity focuses on the choices we make as consumers, driving us to buy more, spend more, or select particular products and services over others.[63] When it comes to consumer manipulation, IoT devices are not only the sensor network that collects information about us, but they are also the actuation machines that nudge us to buy particular products.[64] Increasingly, these household devices use their speakers, screens, and other delightful user interfaces to push us to buy particular products at particular times.[65] Market research indicates, for example, that Amazon shoppers spend more after introducing an Amazon-branded smart speaker into their home.[66] The risks of IoT-abetted manipulation go beyond coercing commercial activity, as IoT devices provide the ability to control movement and behavior in fundamental ways.[67]

C. *Security*

Many of the security problems with IoT devices stem from unpatched software bugs.[68] Modern consumer electronics rely extensively on tiny

---

[60] *See, e.g.*, Shoshana Zuboff, *Surveillance Capitalism*, PROJECT SYNDICATE (Jan. 3, 2020), https://www.project-syndicate.org/onpoint/surveillance-capitalism-exploiting-behavioral-data-by-shoshana-zuboff-2020-01 [https://perma.cc/T2CJ-BE29] (describing social experiments conducted by Facebook and Google through their respective products that resulted in changes in "users' real-world behavior and emotions").

[61] BRETT FRISCHMANN & EVAN SELINGER, RE-ENGINEERING HUMANITY 1–6 (2018).

[62] Crootof, *supra* note 6, at 595–96.

[63] *See generally* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014); Daniel Susser, Beate Roessler & Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1 (2019).

[64] *See* ZUBOFF, *supra* note 8, at 217.

[65] *See id.* at 239–40 (describing Google's prediction in an SEC letter that it would soon be showing ads "on refrigerators, car dashboards, thermostats, glasses, and watches, to name just a few possibilities").

[66] John Koetsier, *Research Shows Amazon Echo Owners Buy 29% More From Amazon*, FORBES, https://www.forbes.com/sites/johnkoetsier/2018/05/30/40k-person-study-buying-echo-increases-amazon-purchases-29-especially-cpg-items/ [https://perma.cc/ZYY5-JN94] (May 31, 2018).

[67] ZUBOFF, *supra* note 8, at 293–96; NIST, *supra* note 15, at 6 ("The ubiquity of IoT sensors in public and private environments can contribute to the aggregation and analysis of enormous amounts of data about individuals. These activities can be used to influence individuals' behavior or decision-making in ways they do not understand . . . .").

[68] Noting this as a key source of the problem for IoT security, the National Telecommunications and Information Administration (NTIA) created a multi-stakeholder process on upgradability and patching. *See* NAT'L TELECOMMS. & INFO. ADMIN., MULTISTAKEHOLDER PROCESS; INTERNET OF THINGS (IOT) SECURITY UPGRADABILITY AND

microcontrollers—small computer processing chips—running software.[69] Because it is impossible to write perfect code, every IoT device has bugs, large and small, which get discovered gradually over time.[70] Bugs may be a bigger problem with IoT devices, many of which are developed by companies that are not experienced with the complexities of securing networked devices.[71] The worst of these bugs are vulnerabilities that can be exploited by malicious actors to do something unintended and unknown, such as spying on the occupants of the house or attacking other computers on the Internet.[72]

To combat threats like these, any manufacturer of a software-embedded product must continuously track and fix the bugs that are identified, a process known as patching.[73] This is an expensive, time-consuming, and non-revenue generating undertaking, which most companies see as a time-limited obligation, bookended with an "end of life" date, after which point newly discovered bugs simply will no longer be patched.[74] Devices that reach their end-of-life are usually not recalled or remotely disabled, but rather are left to live on in an

---

PATCHING (Nov. 7, 2017), https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security [https:// perma.cc/C85Z-EH4J]; *see also* FED. TRADE COMM'N, CAREFUL CONNECTIONS: KEEPING THE INTERNET OF THINGS SECURE 1–7 (Sept. 2020), https:// www.ftc.gov/system/files/documents/plain-language/913a_careful_connections.pdf [https:// perma.cc/Q3UH-QFF2].

[69] This fact was brought close to home for consumers across the world during the global chip shortage of 2021. *See, e.g.*, Asa Fitch, *Chip Shortages Are Starting to Hit Consumers. Higher Prices Are Likely.*, WALL ST. J. (June 21, 2021), https://www.wsj.com/articles/chip-shortages-are-starting-to-hit-consumers-higher-prices-are-likely-11624276801 [https://perma.cc/VK2Z-RGU3].

[70] *See* Ido Kilovaty, *Freedom to Hack*, 80 OHIO ST. L.J. 455, 468 (2019) (discussing bugs as "inevitable externalities" specifically in the context of IoT).

[71] FED. TRADE COMM'N, *supra* note 13, at 13 ("[A]s some [workshop] panelists noted, companies entering the IoT market may not have experience in dealing with security issues.").

[72] *See, e.g.*, Rudra Srinivas, *10 IoT Security Incidents That Make You Feel Less Secure*, CISOMAG (Jan. 10, 2020), https://cisomag.com/10-iot-security-incidents-that-make-you-feel-less-secure/ [https://perma.cc/D4ZD-BUCY] (describing examples of discovered IoT security vulnerabilities that could potentially allow bad actors to surveil users and launch cyberattacks).

[73] *Understanding Patches and Software Updates*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Feb. 23, 2023), https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates [https://perma.cc/86NH-P5EN].

[74] U.S. DEP'T OF HOMELAND SEC., *supra* note 1, at 7 ("Develop an end-of-life strategy for IoT products. Not all IoT devices will be indefinitely patchable and updateable. Developers should consider product sunset issues ahead of time and communicate to manufacturers and consumers expectations regarding the device and the risks of using a device beyond its usability date.").

afterlife as zombies, accreting newly discovered bugs that lead to new vulnerabilities and exploits over time, none of which are ever patched.[75]

Vulnerable IoT devices pose various threats to security, and it is important to distinguish between the different kinds. One reason is that different agencies oversee different forms of security.[76] We divide the threats to security into two types: cybersecurity and physical safety.

1. *Cybersecurity*

Every IoT device is a potential target of a cyberattack.[77] Information security experts speak of a network's "attack surface," the exposed points of a network where malicious actors can try to gain unauthorized access to hijack computers and steal information.[78] A home with a dozen network-connected IoT devices has a much larger attack surface than a "dumb" home with nothing but a handful of smartphones, laptops, and desktops.[79] The attack surface

---

[75] *See* Mark McFadden, Sam Wood, Robindhra Mangtani & Grant Forsyth, *The Economics of the Security of Consumer-Grade IoT Products and Services*, INTERNET SOC'Y (Apr. 24 2019), https://www.internetsociety.org/resources/doc/2019/the-economics-of-the-security-of-consumer-grade-iot-products-and-services/ [https://perma.cc/CA5U-ATJ2]; Paul Roberts, *Forget the IoT. Meet the IoZ: Our Internet of Zombie Things*, SEC. LEDGER (Feb. 5, 2023), https://securityledger.com/2023/02/iot-meet-the-ioz-our-internet-of-zombie-things/ [https://perma.cc/L4E7-6NSZ] ("In fact, zombie devices already fuel malicious botnets like Mirai or RSOCKS, a now defunct Russian-controlled cybercriminal botnet made up of hacked industrial control systems, time clocks, routers, audio/video streaming devices, and smart garage door openers.").

[76] For example, in the United States federal government, the "security" of an IoT device might fall to the Department of Homeland Security, Department of Justice, Federal Trade Commission, or Consumer Product Safety Commission, to name only four possibilities, depending on the type of security at issue. *See* U.S. DEP'T OF HOMELAND SEC., *supra* note 1, at 13–14; FED. TRADE COMM'N, *supra* note 13, at 53; CYBERSEC. UNIT, U.S. DEP'T OF JUST., SECURING YOUR "INTERNET OF THINGS" DEVICES 3 (July 2017), https://www.justice.gov/criminal-ccips/page/file/984001/download [https://perma.cc/K736-RSWQ]; Press Release, FTC, FTC's Bureau of Consumer Protection Staff Submits Comment on Internet of Things and Consumer Product Hazards (June 15, 2018), https://www.ftc.gov/news-events/press-releases/2018/06/ftcs-bureau-consumer-protection-staff-submits-comment-internet [https://perma.cc/QD33-6AZN].

[77] *See, e.g.*, Nicholas Fearn, *The Internet of Things Can Be Hacked—and the Risks Are Growing Every Day*, TECHRADAR (Feb. 12, 2017), https://www.techradar.com/news/the-internet-of-things-can-be-hacked-and-that-puts-your-life-at-risk [https://perma.cc/9YRX-T83F] ("Any internet-enabled device is potentially vulnerable to attack from hackers—so imagine the risks when virtually every object and appliance we use is connected.").

[78] *Attack Surface*, NIST COMPUT. SEC. RES. CTR., https://csrc.nist.gov/glossary/term/attack_surface [https://perma.cc/9PE7-MAG3] (Sept. 20, 2022).

[79] *See* Kilovaty, *supra* note 70, at 470; CHIEF INFO. OFFICER, U.S. DEP'T OF DEF., DOD POLICY RECOMMENDATIONS FOR THE INTERNET OF THINGS (IOT) B-1 (Dec. 2016), https://www.hsdl.org/?view&did=799676 (on file with the *Ohio State Law Journal*) ("The

increases with time as new vulnerabilities are found, vulnerabilities that never get patched due to manufacturer inattention, technical impossibility, consumer capability, or some combination of the above.[80] IoT devices often share the same wireless network used by a consumer's smartphones and computers, allowing outsider attackers to see network activity on the supposedly safe side of a router's protective firewall.[81] To make matters worse, the vendors of these devices underinvest in the security of these devices, selling products that lack even the most basic security features and failing to provide timely updates to patch newly exposed vulnerabilities.[82]

Vulnerable IoT devices pose cybersecurity risks to the homeowner who owns the device as well as systemic risk to other Internet users.[83] An example of the former is when an attacker takes control of a nursery camera to spy on sleeping children.[84] An example of the latter is the Mirai botnet, built out of hundreds of thousands of Wi-Fi routers, IP cameras, and home security cameras forcibly recruited by attackers to overload servers and render the Internet inaccessible to large parts of the U.S. East Coast.[85] From both the perspective of consumer protection and national security, there is a clear and urgent need for IoT products to be more resilient against security risks.

---

number and relative simplicity of IoT devices greatly expands the attack surface of the Internet.").

[80] *See* Hoofnagle, Kesari & Perzanowski, *supra* note 22, at 868; McFadden, Wood, Mangtani & Forsyth, *supra* note 75.

[81] *See* Chuck Davis, *Home Network Segmentation: A Must in the IoT Era*, BETWEEN THE HACKS BLOG (Oct. 15, 2018), https://www.ckd3.com/blog/2018/10/15/home-network-segmentation-a-must-in-the-iot-era [https://perma.cc/B3M2-DNR8].

[82] The use of universal default passwords, such as "12345" or "admin," is a common security weakness among manufacturers, which has led several governments to ban universal default passwords from Internet-connected devices. IOT SEC. FOUND., CONSUMER IOT SECURITY QUICK GUIDE: NO UNIVERSAL DEFAULT PASSWORDS 2 (2020), https://www.iotsecurityfoundation.org/wp-content/uploads/2020/08/IoTSF-Passwords-QG_FINAL.pdf [https://perma.cc/KC3Y-BB74] (listing multiple jurisdictions that have instituted such a ban, including California, Oregon, Australia, and the United Kingdom); *see* Ross Anderson, *Why Information Security Is Hard—An Economic Perspective*, 2001 17TH ANN. COMPUT. SEC. APPLICATIONS CONF. (manuscript at 2), https://www.acsac.org/2001/papers/110.pdf [https://perma.cc/W6LM-DWHY].

[83] *See* Davis, *supra* note 81.

[84] Allyson Chiu, *She Installed a Ring Camera in Her Children's Room for 'Peace of Mind.' A Hacker Accessed It and Harassed Her 8-Year-Old Daughter.*, WASH. POST (Dec. 12, 2019), https://www.washingtonpost.com/nation/2019/12/12/she-installed-ring-camera-her-childrens-room-peace-mind-hacker-accessed-it-harassed-her-year-old-daughter/ [https://perma.cc/JV5R-BZCJ].

[85] Bursztein, *supra* note 11; Lily Hay Newman, *What We Know About Friday's Massive East Coast Internet Outage*, WIRED (Oct. 21, 2016), https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/ [https://perma.cc/39VW-F8ZS].

2. *Threats to Physical Safety*

In addition to threatening intangible interests such as privacy or cybersecurity, vulnerable IoT devices threaten physical safety and property damage.[86] Security expert Bruce Schneier describes the Internet of Things as the new reality where "we've given the internet hands and feet: the ability to directly affect the physical world. What used to be attacks against data and information have become attacks against flesh, steel, and concrete."[87] A compromised door lock can be controlled to entrap building occupants during a fire or unlocked for an intruder.[88] Compromised thermostats can damage expensive mechanical systems, which control hot water, gas, air, and electricity.[89] Increasingly, IoT devices come with embedded speakers to play music or to allow us to communicate with smart assistants, but these speakers can be used by attackers to threaten or harass.[90] Similarly, microphones and cameras can be used to spy on people or to monitor when they leave the house.[91]

The threat is not only from strangers on the Internet. Journalists have documented how abusers use IoT devices to threaten and stalk ex-spouses or partners.[92] Domestic abuse help lines often receive calls from distressed victims disturbed by out-of-control IoT devices in their homes.[93] Abusers would reportedly remotely control these devices through the smart home system,

---

[86] *See generally* BRUCE SCHNEIER, CLICK HERE TO KILL EVERYBODY (2018) [hereinafter SCHNEIER, CLICK HERE] (pointing to physical safety risks resulting from cybersecurity risks in IoT, and discussing possible solutions).

[87] Bruce Schneier, *The Internet of Things Will Turn Large-Scale Hacks into Real World Disasters*, MOTHERBOARD: TECH BY VICE (July 25, 2016) [hereinafter Schneier, *Internet of Things*], https://www.vice.com/en/article/qkjzwp/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster [https://perma.cc/9QNJ-XPMU].

[88] *See, e.g.*, Alfred Ng, *Smart Lock Has a Security Vulnerability That Leaves Homes Open for Attacks*, CNET (Dec. 11, 2019), https://www.cnet.com/home/security/smart-lock-has-a-security-vulnerability-that-leaves-homes-open-for-attacks/ [https://perma.cc/4X45-FUC8]; *Can Your Dream Smart Home Get Hacked!!!*, ISOEH (Feb. 11, 2022), https://www.isoeh.com/exclusive-blog-details-can-your-dream-smart-home-get-hacked.html [https://perma.cc/ RU6C-G84Z].

[89] *See, e.g.*, Ankit Anubhav, *IoT Thermostat Bug Allows Hackers to Turn Up the Heat*, NEWSKY SEC. (July 20, 2017), https://blog.newskysecurity.com/iot-thermostat-bug-allows-hackers-to-turn-up-the-heat-948e554e5e8b [https://perma.cc/5UJ4-NXYF] (describing a security vulnerability in a smart thermostat that would allow temperature control tampering); Ed Higgins, *IoT: When My Home's Thermostat Becomes a Weapon*, ED.IT (Jan. 23, 2017), https://higgins-opinion.blogspot.com/2017/01/when-my-homes-thermostat-becomes-weapon.html [https://perma.cc/2VXS-9RFK].

[90] *See, e.g.*, Wang, *supra* note 18; Chiu, *supra* note 84.

[91] *See, e.g.*, Alex Riley, *How Your Smart Home Devices Can Be Turned Against You*, BBC (May 11, 2020), https://www.bbc.com/future/article/20200511-how-smart-home-devices-are-being-used-for-domestic-abuse [https://perma.cc/JYU5-DX7N].

[92] Bowles, *supra* note 16.

[93] *Id.*; *see also* Holmstrand, *supra* note 16, at 227.

monitoring the victims through cameras and forcefully affecting their physical environment by turning up the thermostat or blasting music from the speakers.[94]

Rebecca Crootof has highlighted how the risk to physical safety comes from IoT device manufacturers themselves.[95] She notes instances in which manufacturers have disabled IoT devices, often to enforce a purported violation of a term of service, creating risks to personal safety by making homes prone to fires or break-ins.[96]

D. *Environment*

The Internet of Things has often been heralded as a boon for the environment, as smart grids and smart thermostats allow individual households to minimize energy waste while also enabling utility companies to distribute that energy more efficiently.[97] However, the transformation of boring utilitarian tools like thermostats, light switches, and doorbells into smart connected devices suggests the short product lifespans that are typical of modern gadgets.[98] Consumers concerned about the cybersecurity risks of devices that are only a few years old may opt to replace them.[99] In describing what she calls the "Internet of Trash" problem, Stacey Higginbotham points out that "many small connected devices such as trackers, jewelry, or wearables are designed to fail once the battery dies," at which point the consumer simply replaces them with the latest product.[100] Manufacturers further exacerbate this problem with planned obsolescence,[101] building products that are difficult to repair and

---

[94] Bowles, *supra* note 16.

[95] Crootof, *supra* note 6, at 588–89.

[96] *Id.*

[97] FED. TRADE COMM'N, *supra* note 13, at 8 (discussing consumers benefitting from smart meters that optimize home energy use); OECD, *supra* note 32, at 16 ("The energy sector is under transformation with the introduction of smart meters informing consumers of their energy usage and patterns, and driving down their consumption and saving energy as a result.").

[98] *See* Lawrence, *supra* note 20; McSweeny, *supra* note 34, at 213; FED. TRADE COMM'N, *supra* note 13, at 13.

[99] *See* CYBERSEC. UNIT, *supra* note 76, at 3 ("You should consider disconnecting [potentially unsecure] devices and replacing them with newer, secure models.").

[100] Stacey Higginbotham, *The Internet of Trash: IoT Has a Looming E-Waste Problem*, IEEE SPECTRUM (May 17, 2018), https://spectrum.ieee.org/the-internet-of-trash-iot-has-a-looming-ewaste-problem [https://perma.cc/Q8W8-25E8].

[101] "Planned obsolescence" is the practice of consciously designing a product to have a short lifespan to force customers to have to make more frequent repeat purchases. Adam Sarhan, *Planned Obsolescence: Apple Is Not The Only Culprit*, FORBES (Dec. 22, 2017), https://www.forbes.com/sites/adamsarhan/2017/12/22/planned-obsolescence-apple-is-not-the-only-culprit/?sh=20084f523cf2 [https://perma.cc/2LLZ-CXR5]. The practice reportedly began in the 1920s when a cartel of major lightbulb manufacturers collectively decided to sell shorter-lived lightbulbs. Markus Krajewski, *The Great Lightbulb Conspiracy*, IEEE

making critical components (most commonly batteries) difficult to replace. Developers often discontinue service and updates to older versions of the IoT product's software.[102]

Though the focus of this Article is on smart home devices rather than wearables, the story of the Apple Watch provides an apt illustration of the problem of planned obsolescence in smart consumer products. When Apple announced a new version of its smartwatch operating system in 2018, it effectively rendered its original line of smartwatches obsolete because they could not run the new software.[103] These original smartwatches included the solid gold Apple Watch edition, launched in 2015 and sold for anywhere from $10,000 to as much as $17,000.[104] Traditional watches at that price range would have lasted decades; these Apple smartwatches were becoming outdated in three years.[105] While Apple has a trade-in program that helps customers recycle these unwanted devices easily, such programs are not common across the electronics industry.[106]

Apple has also been criticized for its planned obsolescence practices surrounding its iPhones.[107] After it was revealed that the company had been purposefully scaling back processing power in older iPhone models, Apple agreed to settle a class-action suit and a multi-state investigation last year.[108] A

SPECTRUM (Sept. 24, 2014), https://spectrum.ieee.org/the-great-lightbulb-conspiracy [https://perma.cc/F5H6-QE7S]. Though the lightbulb's useful life was clocked at 2,500 hours in 1924, the Phoebus cartel saw to it that by 1940, the lifespan of a bulb sold in the market was capped at 1,000 hours. *Id.*

[102] SCHNEIER, CLICK HERE, *supra* note 86, at 39 ("Engineering teams assemble quickly to design the products, then disband or go build something else. . . . The companies involved simply don't have the budget to make their products secure, and there's no business case for them to do so.").

[103] Andrew Griffin, *Apple Watch: $17,000 Smartwatch Is Obsolete After Latest Update*, INDEP. (June 6, 2018), https://www.independent.co.uk/life-style/gadgets-and-tech/news/apple-watch-update-latest-edition-watchos-5-expensive-out-of-date-obsolete-a8385291.html [https://perma.cc/YXS4-MMTY].

[104] *Id.*; Micah Singleton, *The Gold Apple Watch Edition Will Start at $10,000*, VERGE (Mar. 9, 2015), https://www.theverge.com/2015/3/9/8161553/apple-watch-edition-price-how-much [https://perma.cc/55KE-N3SM].

[105] Griffin, *supra* note 103.

[106] *Apple Trade In*, APPLE, https://www.apple.com/shop/trade-in [https://perma.cc/KPB7-DNSQ]; Ian Sherr, *Apple Is Opening Up Its World of iPhone Recycling*, CNET (Apr. 22, 2019), https://www.cnet.com/tech/mobile/apple-is-opening-up-its-world-of-iphone-recycling/ [https://perma.cc/EN9L-SVZN].

[107] Jack Nicas, *Apple Will Pay $113 Million to Settle States' Investigation into Battery Throttling*, N.Y. TIMES (Nov. 18, 2020), https://www.nytimes.com/2020/11/18/business/apple-will-pay-113-million-to-settle-states-investigation-into-battery-throttling.html [https://perma.cc/BJK2-NFXY].

[108] *Id.*

European consumer advocacy group has been filing class-action lawsuits on this issue in Belgium, Spain, Italy, and Portugal.[109]

Both of these examples of short product lifecycles come from Apple, one of the largest and wealthiest corporations in the world, and one quite likely to survive for decades if not longer.[110] Contrast Apple with the many smaller, younger, more financially contingent companies that produce smart home devices. How will many of these companies continue to operate and support old products on the ten-to-thirty-five-year time frame typically associated with thermostats, doorbells, TVs, and refrigerators?[111]

The result of these problems is an ever-growing volume of landfills full of obsolete IoT devices brimming with hazardous materials.[112] A report from the Platform for Accelerating the Circular Economy (PACE) and the United Nations E-Waste Coalition found that people generated more than 44 million metric tons of e-waste globally in 2016 and expects annual e-waste volume to surpass 52 million metric tons by 2021.[113]

III. THE PROPOSAL

To address the risks of harms posed by IoT smart home devices, particularly as they age, these devices should come with a switch that will disable the features that contribute to the risks when flipped. This proposal builds on several strands in legal scholarship relating to information privacy, platform power, friction, and design.

A. *The Legacy Switch*

We propose the "Legacy Switch" as a solution to tackle the potential harms of smart home IoT outlined in Part II. IoT manufacturers should manufacture a

---

[109] Stephen Jewkes & Elvira Pollina, *Italy Consumer Association Sues Apple for Planned iPhone Obsolescence*, REUTERS (Jan. 25, 2021), https://www.reuters.com/article/us-italy-apple-class-action-idUSKBN29U1BB [https://perma.cc/K8B6-YV4X].

[110] *See* Mark Kolakowski, *At $2.08 Trillion, Apple Is Bigger Than These Things*, INVESTOPEDIA (Mar. 17, 2021), https://www.investopedia.com/news/apple-now-bigger-these-5-things/ [https://perma.cc/T6AB-EVGZ].

[111] *See* NAHB, *supra* note 35, at 7–11; *InterNACHI's Standard Estimated Life Expectancy Chart for Homes*, INT'L ASS'N OF CERTIFIED HOME INSPECTORS [hereinafter INTERNACHI], https://www.nachi.org/life-expectancy.htm [https://perma.cc/4AP9-2YNN].

[112] *See* Alana Semuels, *The World Has an E-Waste Problem*, TIME (May 23, 2019), https://time.com/5594380/world-electronic-waste-problem/ [https://perma.cc/Y7CN-YB4H] ("[L]ess than a quarter of all U.S. electronic waste is recycled . . . . The rest is incinerated or ends up in landfills. That's bad news, as e-waste can contain harmful materials like mercury and beryllium that pose environmental risks.").

[113] PLATFORM FOR ACCELERATING THE CIRCULAR ECONOMY, A NEW CIRCULAR VISION FOR ELECTRONICS: TIME FOR A GLOBAL REBOOT 7, 10 (Jan. 2019), https://www3.weforum.org/docs/WEF_A_New_Circular_Vision_for_Electronics.pdf [https://perma.cc/S62G-ESXD].

switch into each of their connected smart home devices that allows consumers to cut off network connections and turn off certain "smart" features, without disabling other, more basic features of the product.[114] If refrigerators today have become "computer[s] that keep things cold,"[115] there should be a straightforward mechanism that renders them simple kitchen appliances that still make things cold.[116] By providing consumers a concrete way to flip their product from "smart, connected" to "legacy, disconnected," the legacy switch directly addresses the harms to security, privacy, and the environment.

Consider some examples: every smart doorbell should have a physical switch that renders it a simple, old-fashioned doorbell with no connectivity outside the home. The legacy switch on a smart thermostat should render the device merely a thermostat, meaning a device that regulates temperature, perhaps one with a screen and basic scheduling software (start and end times) but one that does not send any data to anybody outside the home. Every smart television should be switchable into a device that plays videos without sharing information about what is watched. Every smart door lock should offer a fallback allowing it to be opened with a physical key and should come with a switch that disables any other features.

A legacy switch would dramatically ameliorate if not entirely erase an IoT device's threats to privacy and security.[117] Once the user throws the legacy switch, the device would not only cease to track the user's behavior but would also no longer feed user input data into its machine learning algorithm.[118] The device would also stop transmitting data about individuals to the product manufacturer, allowing the homeowner to opt out of one small part of the system of surveillance capitalism.[119]

At the same time, disabling the device's connectivity—effectively removing the thing from the Internet of Things—would lead to greater security, both at the individual and collective level.[120] The device itself would be more

---

[114] Woody Hartzog wrote briefly about this proposal, citing one of us for the idea. HARTZOG, *supra* note 24, at 272. Chris Hoofnagle, Aniket Kesari, and Aaron Perzanowski briefly discussed a similar idea in a broader conversation about "tethered" devices. *See* Hoofnagle, Kesari & Perzanowski, *supra* note 22, at 868.

[115] Schneier, *Internet of Things*, *supra* note 87, at 3.

[116] Hoofnagle, Kesari & Perzanowski, *supra* note 22, at 868 (discussing kill switches for long-lived tethered devices).

[117] *See* CYBERSEC. UNIT, *supra* note 76, at 3 (outlining some threats posed by the use of IoT devices).

[118] To be clear, a legacy switch might still allow for machine learning processing, but only "on board" and not "in the cloud." Thus, a thermostat switched into its legacy mode might still collect and process data using its on-board processing, but it would not be permitted to collect or share the data or the model.

[119] *See* Hoofnagle, Kesari & Perzanowski, *supra* note 22, at 868–69.

[120] The Department of Homeland Security's "Strategic Principles for Security the Internet of Things" stresses the importance of what it calls "selective connectivity," meaning "controls . . . to disable network connections or specific ports when needed or desired" as a

secure from external cyber threats as it stops sending and receiving data packets over the Internet, thus making it harder to infect with a virus.[121] A disconnected device also reduces the overall attack surface[122] of a device, as it becomes much less likely to be enlisted in a botnet.[123] Legacy switches can therefore bring real improvement to the cybersecurity of broader society.

Legacy switches will protect physical safety, too. Remote attackers will lose the ability to entrap occupants during a fire, disable safety mechanisms on a furnace, or detect when a homeowner has left on vacation. Survivors of domestic abuse can switch off the vectors for harassment and stalking hard-wired into their homes by their abusers.[124]

Legacy switches can also help limit IoT's e-waste harm to the environment. Most importantly, devices with legacy switches will last longer; even after the manufacturer or developer stops supporting the device with software updates and patches, the device will continue to be able to carry out its basic function, be it locking doors, controlling the room's temperature, or keeping food cold.[125] Legacy switches would thus allow people to avoid having to purchase new versions of a product at the pace of consumer devices. It will therefore not only save consumers the frustration and hassle of the constant replacement cycle, but also save the environment from the aforementioned problem of the "Internet of Trash" as consumers purchase new devices less frequently.[126]

Finally, legacy switches can address the asymmetric power imbalance with platforms by restoring power and choice back to users. The ability to switch off a smart product's "smarts" not only benefits individual privacy and security, but also turns off the data spigot on which tech platforms rely.

In Part IV, we will delve more deeply into the details of this proposal. Government action is likely necessary to bring legacy switches into widespread usage, and we will identify a few specific agencies with the power and

---

means of increasing IoT device security. U.S. DEP'T OF HOMELAND SEC., *supra* note 1, at 12.

[121] *See* CYBERSEC. UNIT, *supra* note 76, at 1–3.

[122] An attack surface is "the set of ways in which an adversary can enter the system and potentially cause damage. Hence the 'smaller' the attack surface, the more insecure the system." *See* Pratyusa K. Manadhata & Jeannette M. Wing, *An Attack Surface Metric*, 37 IEEE TRANSACTIONS ON SOFTWARE ENG'G 371, 371 (May–June 2011), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5482589 [https://perma.cc/MC36-BG6M].

[123] *See* Bursztein, *supra* note 11.

[124] By allowing survivors of abuse to switch off the "smarts" without losing the normal functionality of the device, we can also prevent those survivors becoming further isolated, as often happens when survivors rip out smart thermostats from the walls or completely turn off their smart devices, making them useless. *See* Bowles, *supra* note 16.

[125] *See* Hoofnagle, Kesari & Perzanowski, *supra* note 22, at 868.

[126] *See* Higginbotham, *supra* note 100, at 17. Within the vast universe of consumer IoT devices, legacy switches will likely be most valuable to include in consumer products that have high inertia: namely, products that are large, expensive, or affixed to one's residence, such as smart televisions, refrigerators, laundry machines, thermostats, doorbells, or home security systems.

institutional competence to lead the charge. First, let us connect this proposal to the work and proposals of other scholars.

B. *Building Blocks*

Legacy switches build on three important themes in legal scholarship. Many have written about the intertwined problems of information privacy and platform power, focusing in part on how IoT devices feed a growing crisis of surveillance capitalism. They have recommended solutions that are compatible with our legacy switch proposal, although our solution diverges in a few important ways from the current conventional wisdom. Our work advances a growing literature around friction, which identifies the ways in which inefficiency can protect human values. Finally, it embraces those who focus on a turn to design; works that treat the design of technical systems as an underappreciated subject of study and object of regulation.

1. *Information Privacy and Platform Power*

Earlier, we pointed to a rich recent literature describing the problems with our emerging information society. Most importantly, Shoshana Zuboff's description of surveillance capitalism and Julie Cohen's framing of the biopolitical domain, best capture not only the rise of pervasive surveillance through technological advances including IoT, but also the ways in which our legal institutions are ill-suited to respond.[127]

The challenge is to build on this rich descriptive work—neither Cohen nor Zuboff purport to have detailed recommendations—to develop concrete, actionable proposals for reform.[128] In searching for other scholarship with concrete recommendations, there is much less prior work to which we can point; too many other good scholarly works written over the past two decades offer a compelling story of underappreciated privacy harm but then resolve into a tepid puddle of recommendations for impact assessments, increased enforcement power, or new takes on old torts.

Some of the better, newer work focuses on particular technologies with special harms. Woody Hartzog and Evan Selinger have proposed bans on facial recognition, for example.[129] Lauren Willis offers a creative new take on

---

[127] Zuboff's treatment is very long, and Cohen's text is very dense. *See generally* ZUBOFF, *supra* note 8; COHEN, *supra* note 9. A much more approachable introduction pitched for a lay audience is Neil Richards's compelling book. *See generally* RICHARDS, *supra* note 57.

[128] *See* ZUBOFF, *supra* note 8, at 524–25; COHEN, *supra* note 9, at 270–71.

[129] Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOY. L. REV. 101, 122 (2019) ("There is only one way to stop the harms of face surveillance. Ban it.").

consumer protection law, offering "performance-based" ways to hold companies accountable for the effects of their data collection practices.[130]

What we hope to bring to this work is a "nothing is sacred" approach to thinking about the present-day shape and design of our most important technologies. Embracing an "all artifacts have politics" approach, our goal is push the regulatory imagination around what should be changed, abandoned, or redesigned.[131]

2. *Friction and Desirable Inefficiency*

Our proposal advances a promising new approach for addressing the proliferating harms of the information age: friction.[132] For decades, Silicon Valley tech moguls have pursued the dream of frictionless platforms and services.[133] From Netflix's ability to start the next episode as soon as you've finished the last one, to Instagram's and TikTok's endless stream of social engagement, to Uber's reassuring display of available cars circling around your building, our economy has been oriented toward seamlessness, immediacy, and impulse.[134] Companies have deployed government lobbyists, academics, and captured regulators to elevate frictionlessness from mere technical desiderata to policy ambition and possibly even moral good.[135] Julie Cohen has connected this to a century-plus long experiment to center economic efficiency at the heart of our economy and government.[136] An insidious feature of this campaign is to deny that efficiency has a moral component, treating it instead like a natural

---

[130] Lauren E. Willis, *Performance-Based Consumer Law*, 82 U. CHI. L. REV. 1309, 1314–15 (2015).

[131] *See generally* LANGDON WINNER, THE WHALE AND THE REACTOR: A SEARCH FOR LIMITS IN AN AGE OF HIGH TECHNOLOGY (1986) (describing the notion that "all artifacts have politics," meaning all technological systems result from political processes and embed political preferences).

[132] *See* Ohm & Frankle, *supra* note 27, at 803–05; Goodman, *Digital Fidelity*, *supra* note 27, at 624–25; McGeveran, *supra* note 27, at 17.

[133] *See* McGeveran, *supra* note 27, at 20–21.

[134] *See How to Autoplay the Next Episode*, NETFLIX, https://help.netflix.com/en/node/121518 (on file with the *Ohio State Law Journal*); *Infinite Scroll*, ETHICAL SOC. MEDIA PROJECT, https://www.theethicalsocialmediaproject.com/infinite-scroll.html [https://perma.cc/57TG-67EM]; Sara Ashley O'Brien, *Uber: There Are No Ghost Cars in Our App*, CNN (July 30, 2015), https://money.cnn.com/2015/07/29/technology/uber-phantom-drivers/index.html [https://perma.cc/HZB8-925Z]; Esther Pomerantz, *Big Tech's Secret Weapon*, UX PLANET (Dec. 17, 2021), https://uxplanet.org/big-techs-secret-weapon-b9e7c9feb295 [https://perma.cc/KFG5-MSMG]; Shubham Agarwal, *Technology Is Easier Than Ever to Use—and It's Making Us Miserable*, DIGITALTRENDS (Oct. 25, 2020), https://www.digitaltrends.com/web/the-frictionless-internet/ [https://perma.cc/YD9K-XCTR].

[135] *See* McGeveran, *supra* note 27, at 26 (detailing Netflix's lobbying efforts to "weaken the consent requirements in the VPPA"); COHEN, *supra* note 9, at 194–95.

[136] COHEN, *supra* note 9, at 194–95.

feature of the world, a starting point or background presumption.[137] Proposals against efficiency or frictionless get framed as absurd or unnatural or perverse.

Observing what three decades of unchecked frictionlessness has wrought, we now can connect the dominance of frictionlessness and hyper-efficiency to a long and growing list of societal problems emanating from Silicon Valley. It is the unthinking and unchecked efficiency of our platforms that enables and feeds social media addiction, surveillance capitalism, misinformation and disinformation, and tech manipulation.[138] Efficient platforms prove to be tools for increasing income inequality, unchecked government surveillance, and autocratic rule.[139] Less efficient platforms place frictive hurdles in the way of problems like these.[140]

It is time to challenge the moral standing of efficiency. The hyper-efficiency of technology platforms is the root cause of some of the problems listed above, and it exacerbates the rest. Inefficiency, we argue, is an underappreciated and essential ingredient for making space for important human values to take root and flower.

Scholars have understood the importance of inefficiency in protecting human values. Julie Cohen wrote a decade ago about the need to inject systems with "semantic discontinuity," the gaps or seams that disrupt seamless information flows.[141] Mireille Hildebrandt writes of agonistic machine learning, meaning systems that "demand[] that companies or governments that base decisions on machine learning must explore and enable alternative ways of datafying and modeling the same event, person or action."[142]

The importance of friction and inefficiency has been identified within Silicon Valley itself. One of us has written previously about "desirable inefficiency."[143] We pointed out that many within the tech sector have realized the problem of unchecked efficiency and the way it interferes with human values.[144] We cited numerous examples of coders purposefully building

---

[137] *See* Kevin Roose, *Is Tech Too Easy to Use?*, N.Y. TIMES (Dec. 12, 2018), https://www.nytimes.com/2018/12/12/technology/tech-friction-frictionless.html [https://perma.cc/M6C4-LPCY].

[138] David R. Polgar, *Friction Tech Must Play a Bigger Role for Social Media to Get Better*, BUILTIN (May 25, 2021), https://builtin.com/software-engineering-perspectives/key-better-social-media-ecosystem-friction [https://perma.cc/D7HP-F28F]; Roose, *supra* note 137.

[139] Polgar, *supra* note 138.

[140] *See* Roose, *supra* note 137 (describing WhatsApp's efforts to create friction by "limit[ing] message forwarding" in the aftermath of riots in India stemming from forwarded misinformation and YouTube's revision of its ad revenue rules).

[141] JULIE E. COHEN, CONFIGURING THE NETWORKED SELF 239–41 (2012).

[142] Mireille Hildebrandt, *Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*, 20 THEORETICAL INQUIRIES IN L. 83, 106 (2019).

[143] Ohm & Frankle, *supra* note 27, at 782.

[144] *Id.* at 779.

inefficiencies into their code in order to protect essential human values.[145] Concrete real-world examples of desirable inefficiency include the smartphone password lockout mechanism and the captcha mechanism that often accompanies new account registration on websites.[146] A new stock exchange forces every trade to traverse thirty-eight miles of fiber optic cable to prevent certain types of "unfair" high-frequency trading.[147] The protocol at the heart of the Bitcoin cryptocurrency requires a costly "proof of work" step to bring about consensus and trust without centralized control.[148] All of these examples involve features that require the user to spend more time and energy than they otherwise would have to in order to obtain an output.[149] None are strictly essential for a service or product to operate, and more efficient designs clearly exist—smartphones could allow users to keep trying passwords without having to wait increasingly longer intervals between failed attempts; captchas could be eliminated so that web browsing could be made much faster; stock exchanges need not delay trades; and one could design a cryptocurrency without proof of work.[150] But these systems designers have baked inefficiency into their designs to protect the human values of security, fairness, trust, and consensus.

This Article marks a next step in this emerging research agenda. Once we establish the connection between inefficiency and human values—and challenge the dubious moral standing of efficiency—the next step is to find ways to intentionally inject friction into systems that have become too efficient or seamless in ways that jeopardize social order, prevent human flourishing, or otherwise interfere with important human values. Friction belongs in every policy conversation, inside corporate boardrooms, standards setting organizations, law enforcement agencies, regulatory bodies, and legislatures. Scholars and policy advocates need to investigate and elaborate friction to turn an admittedly vague overarching principle into actionable policy prescriptions. Our deep dive into legacy switches is an early attempt to undertake this work.

3. *Focusing on Design*

The past few decades have seen the rise of a new discipline studying the age-old process of design. The field of "design thinking" has tried to lend academic rigor to industrial processes focused on "how a system is architected, how it functions, how it communicates, and how that architecture, function, and communication affects people."[151]

---

[145] *See id.* at 781–82.
[146] *See id.* at 805.
[147] *Id.* at 793.
[148] *Id.* at 796–97.
[149] Ohm & Frankle, *supra* note 27, at 782.
[150] *See supra* notes 146–49 and accompanying text.
[151] HARTZOG, *supra* note 24, at 12.

In parallel to design thinking, scholars who study the social impacts of new technology have proposed "value sensitive design," asking how design choices impact human values.[152] Woody Hartzog has applied these concepts to information privacy, cataloging how the design of social networking platforms and IoT devices, among other things, manipulate consumers to hand over their information, perhaps against their stated wishes.[153] Hartzog urges policymakers to pay attention to the power of design, enacting laws and regulations that reshape technologies to avoid privacy harms and other problems.[154]

Some might criticize our proposal as needlessly in the weeds, or worse, an unwise intrusion into the protected province of the so-called "innovators."[155] The intrusion is the point. To tackle problems that go far beyond the privacy, security, and environmental consequences of IoT, we need to redefine who gets a say in the design of industrial products and services.[156] Many of the problems we document in this Article stem from the unsupervised design processes our governance structures presume;[157] what is needed is the public's involvement in the design process, through well-conceived regulatory interventions. To cure what ails us, we need methods for bringing out meaningfully participatory design.

We see this as a close cousin to the so-called "Right to Repair" movement, which stands in protest of manufacturers imposing various forms of restrictions against consumers repairing the products they have purchased.[158] Such products include not only cell phones and computers, but also farm equipment, home appliances, cars, and even medical devices.[159] The restrictions themselves can range from physical restrictions like adhesives, to limiting the availability of parts and making diagnostic software unavailable to independent repairers.[160] The Right to Repair movement has advocated for repair-friendly policies and

---

[152] BATYA FRIEDMAN & DAVID G. HENDRY, VALUE SENSITIVE DESIGN: SHAPING TECHNOLOGY WITH MORAL IMAGINATION 3–4 (2019).

[153] HARTZOG, *supra* note 24, at 260–75.

[154] *Id.* at 7–9.

[155] *See* ADAM THIERER, PERMISSIONLESS INNOVATION: THE CONTINUING CASE FOR COMPREHENSIVE TECHNOLOGICAL FREEDOM 7–8, 10 (2016).

[156] HARTZOG, *supra* note 24, at 9 ("We all have a role to play in the design of information technologies.").

[157] *See id.* at 268–69.

[158] Paola Rosa-Aquino, *Fix, or Toss? The 'Right to Repair' Movement Gains Ground*, N.Y. TIMES, https://www.nytimes.com/2020/10/23/climate/right-to-repair.html [https://perma.cc/VKQ3-V3AD] (Nov. 2, 2021).

[159] *Id.*

[160] FED. TRADE COMM'N, POLICY STATEMENT OF THE FTC ON REPAIR RESTRICTIONS IMPOSED BY MANUFACTURERS AND SELLERS (2021), https://www.ftc.gov/system/files/documents/public_statements/1592330/p194400repairrestrictionspolicystatement.pdf [https://perma.cc/HHB4-YFC3].

regulations in both the U.S. and abroad,[161] based on the simple argument that "You bought it, you should own it. Period."[162]

The movement has been gaining traction in recent years, with the European Commission announcing plans for new right to repair rules for smartphones, tablets, and laptops by 2021.[163] In a similar vein, the European Parliament has enacted legislation that will require all smartphones to have USB-C ports for charging by Fall 2024.[164]

The Right to Repair has had some traction in the United States as well. In 2021, the FTC announced it would "prioritize investigations" into manufacturers that impose certain repair restrictions.[165] In a victory for the movement, Apple recently announced that it would give customers access to official parts, tools, and documentation for repairing their own iPhones.[166]

The point is not to micromanage every detail of modern innovation. Both the Right to Repair and the legacy switch seek to inject important values into modern design but leave space for other forms of innovation and competition once those values are protected.

4. *A Complement, Not a Replacement, for Other Approaches*

Legacy switches do not make smart devices more private or secure. They make smart devices no longer smart and therefore less of a risk. This helps create a safer and more private home ecosystem, both for specific consumers and across the Internet, but a consumer who wants smart functionality and also privacy and security in a device will find no direct relief from our proposal.

Other scholars have written about how to enact new laws or promulgate new standards to reshape smart devices to respect privacy and protect security more.[167] California's SB-327, which took effect in 2020, requires IoT device manufacturers to implement modest security features.[168] The General Data

---

[161] Cody Godwin, *Right to Repair Movement Gains Power in US and Europe*, BBC (July 7, 2021), https://www.bbc.com/news/technology-57744091 [https://perma.cc/5M4B-JYWQ].

[162] *The Repair Association*, REPAIR.ORG, https://www.repair.org/ [https://perma.cc/T9YT-JZ4U].

[163] Rosa-Aquino, *supra* note 158.

[164] Press Release, European Parliament, Deal on Common Charger: Reducing Hassle for Consumers and Curbing E-Waste (June 7, 2022), https://www.europarl.europa.eu/pdfs/news/expert/2022/6/press_release/20220603IPR32196/20220603IPR32196_en.pdf [https://perma.cc/P8AC-2XTE].

[165] FED. TRADE COMM'N, *supra* note 160.

[166] Press Release, Apple, Apple Announces Self Service Repair (Nov. 17, 2021), https://www.apple.com/newsroom/2021/11/apple-announces-self-service-repair/ [https://perma.cc/SB3D-PQ7Y].

[167] *See, e.g.*, HARTZOG, *supra* note 24, at 269–75; *see also* Schneier, *Internet of Things*, *supra* note 87, at 120–23, 150–52.

[168] S.B. 327, 2017–18 Reg. Sess. (Cal. 2018) (codified at CAL. CIVIL CODE §§ 1798.91.04 to 1798.91.06 (West 2023)).

Protection Regulation (GDPR) and the California Consumer Privacy Act of 2018 (CCPA) already place restrictions on the ability of smart home device manufacturers to collect more information than needed or to sell information gathered to third parties.[169] We support these efforts to address some of the harms recited above. Even if legacy switches become widely adopted, smart home devices will pose security and privacy risks before their switches are flipped. New laws are needed to protect consumers using smart home devices as intended.

In addition, legacy switch mandates will complement these approaches. Giving consumers a method to opt out of all data collection if they so choose will increase incentives on manufacturers to avoid privacy and security fiascos. We anticipate that many consumers will flip their legacy switches in response to publicity about problems with particular devices or manufacturers. The threat of consumer exit created by legacy switches will tip the balance of power between manufacturer and consumer, creating a new credible threat that manufacturers may be held accountable for their poor privacy decisions.

Legacy switches will also give regulators an additional tool for consumer protection. In the face of evidence that a particular device has been rendered insecure, it can encourage the public to remove the devices from the Internet, effectively enacting a less expensive and less disruptive recall.

Ultimately, even the best new privacy laws will have trouble accounting for the expected lifespan of doorbells, refrigerators, doorknobs, and televisions. These infrastructural pieces of our homes have lasted decades in the past,[170] and the best privacy laws in the world will do no good after smart home manufacturers go out of business or otherwise stop supporting the millions of their devices hard-wired into the walls of homes around the world. Unless we accept the reality that devices like these no longer last decades and need to be replaced as often as they replace their smartphones—with the old carcasses filling our landfills with more e-waste—better privacy laws alone will not be enough.

C. *How Many People Will Use the Switch?*

If legacy switches were made available, how many people would use them? Will the benefits to those flipping the switch justify the investment in product redesign and reengineering they will require? Is there a critical rate of adoption—5%, 15%, 50%—at which these benefits will outweigh the costs? In addition to weighing costs and benefits in a conventional economic manner, focused primarily on price and consumer welfare, we analyze these tradeoffs more expansively, focused on how the very process of adopting legacy switches

---

[169] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016 O.J. (L 119) 1, 35–36; *e.g.*, California Consumer Privacy Act of 2018 § 3, CAL. CIV. CODE §§ 1798.100(b), 1798.110(c)(4), 1798.115(a)(2) (West 2018).

[170] *See* INTERNACHI, *supra* note 111.

could give rise to significant structural change and other non-economic benefits too. Consider the economic and structural/non-economic analyses in turn.

1. *Economic Costs and Benefits*

The rate of adoption for a particular legacy switch will vary based on how it is implemented as well as on other contextual details. Many of the relevant factors are considered in Part IV. As a preview, legacy switches are likelier to be used if they are easy to use and provide a simple choice.

Legacy switch usage for a particular device is likely to increase with time, as the risk of harm to security in particular increases. For example, as soon as a company declares a particular model of a particular device to be near or at its end of life, we expect a spike in usage.[171] We imagine that news stories about high-profile software vulnerabilities or data breaches involving a particular company or particular device might spur legacy switch use.[172] These triggering events will occur over time, so we cannot accurately measure the usage rate of a legacy switch until it has been available for a decade or longer.

In weighing costs and benefits, it is important to take account for how legacy switches—especially if imposed in response to a governmental mandate—will alter the market for IoT devices. Reengineering existing models to incorporate a legacy switch will increase the costs of engineering, distribution, support, and marketing.[173] Much of these costs are likely to be passed along to consumers, meaning higher prices for the products. Some manufacturers may be forced to exit the market due to the reduced profit margins. A legacy switch may thus end up making some categories of IoT devices too expensive for some consumers, disproportionately affecting those with less—a group we have cited as disproportionately vulnerable to some of the harms we are hoping to address.[174]

All of these costs and market impacts could still be justified if enough people benefit from the legacy switches. Those who flip the switch will be able to satisfy a preference for increased privacy and security. They will be at less

---

[171] Some companies specifically announce when certain products will be reaching their end-of-life at a certain year. *See, e.g.*, *Products Ending Support in 2021*, MICROSOFT (Jan. 14, 2022), https://docs.microsoft.com/en-us/lifecycle/end-of-support/end-of-support-2021 [https://perma.cc/7PGT-J7YN]; *End-of-Sale and End-of-Life Products*, CISCO, https://www.cisco.com/c/en/us/products/eos-eol-listing.html [https://perma.cc/U8JP-Y95Q]; *Security Updates*, SAMSUNG MOBILE SEC., https://security.samsungmobile.com/workScope.smsb [https://perma.cc/H8ZB-2TX6].

[172] *See, e.g.*, Casey Quackenbush, *Amazon and Ebay Are Among Retailers Dropping 'CloudPets' Smart Toys Amid Concerns About Hacking*, TIME (June 7, 2018), https://time.com/5304045/amazon-ebay-cloudpets-hacking/ [https://perma.cc/5ZCF-T2K9]; Leo Kelion, *Parents Urged to Boycott VTech Toys After Hack*, BBC (Feb. 10, 2016), https://www.bbc.com/news/technology-35532644 [https://perma.cc/6U63-VCNT].

[173] *See* HARTZOG, *supra* note 24, at 120–21.

[174] *See supra* note 23 and accompanying text.

risk of suffering a costly security or privacy breach. They will need to upgrade their devices less often, as legacy switches extend the usable lifespan of products. Our economic accounting should also consider people who may never use the switch but are persuaded to buy the devices because they value the option of the possibility of using the switch, treating them like insurance policies against future privacy and security risks and harms.

2. *Non-Economic Benefits*

It is not enough to focus solely on price and consumer welfare. The people who use the switch may experience significant nonfinancial benefits that justify the costs even if they are few in number. Consider again the victims of domestic abuse who have been stalked or terrorized by their abusers through IoT devices.[175] Permitting a small number of them to secure their homes easily may bring significant safety and peace of mind to a vulnerable population. Asking others who do not need a legacy switch to bear some of the cost of making it available to vulnerable people provides a pro-social benefit. Other users will enjoy psychic benefits both before and after they have flipped the switch. Legacy switches also reduce the cognitive burden of paying attention to confusing and rapidly changing information about reducing the security and privacy threats within one's home, a benefit in our information glutted times.[176]

Even if very few people end up using a legacy switch, the very process that leads to their adoption would itself be a significant benefit, one that might outweigh the costs. Say a company implements a legacy switch only because a new regulation requires it, rather than because of an independent assessment of market demand or social responsibility. The process that created such a regulation will result only after political pressure, civil society advocacy, and public debate. There is value in rallying and organizing the kind of participatory design forces we called for above. We need companies to increasingly envision design as a transparent process involving outside voices and influences more often than they have in the past. Every company that implements a legacy switch against its internal wishes is evidence of a productive opening of the broken insularity of modern technological design.

The sheer fact that a legacy switch mandate has been enacted may open the door to other pro-social interventions into the design of products and services. It might reveal a playbook for empowering external actors to help redesign social networking services to tamp down on misinformation or hate speech, redesign search engines to increase competition, or redesign gig economy services to improve labor standards, to name only three examples. Even if very few people would flip a legacy switch, the development of a playbook for other design interventions will help justify the costs of a mandate.

---

[175] Bowles, *supra* note 16; Holmstrand, *supra* note 16, at 226–28.

[176] *See generally* JAMES GLEICK, THE INFORMATION: A HISTORY, A THEORY, A FLOOD (Vintage Books 1st ed. 2012) (2011).

IV. IMPLEMENTATION

Although the basic idea of a legacy switch is simple and straightforward, there are many important implementation details. We address these in some depth, in part to present a fully realized proposal that anticipates important choices and likely objections. We hope this Article can serve as a roadmap for legislators or regulators interested in adopting a legacy switch mandate.

First, we explore several government institutions that might have the power, political will, institutional competence, and regulatory toolkits needed to create and enforce legacy switch mandates, focusing in particular on two U.S. federal agencies—the CPSC and FTC. Second, we delve into features that any good legacy switch (or legacy switch mandate) should provide: effectiveness, ease of use, and external verifiability. Finally, we explore two other features that can give rise to additional benefits for consumers or regulators, even if they are not always necessary: irreversibility and physical implementation.

A. *Federal Agencies*

We harbor no illusions that the tech industry will unilaterally adopt legacy switches to respond to market pressures or their own altruistic impulses. To bring these consumer protection design features into being, we recommend governmental action. There are numerous, state, local, and national government agencies empowered and competent to enact a legacy switch mandate or recommendation. Rather than exhaustively surveying the possibilities, we focus on two likely candidates at the national level in the United States that we think are especially well-suited for this work.

1. *Consumer Product Safety Commission*

With jurisdiction over thousands of types of consumer products and authority to regulate product safety in those products,[177] the CPSC is charged by the Consumer Product Safety Act:

> (1) to protect the public against unreasonable risks of injury associated with consumer products;
> (2) to assist consumers in evaluating the comparative safety of consumer products;
> (3) to develop uniform safety standards for consumer products and to minimize conflicting State and local regulations; and

[177] *See About CPSC*, U.S. CONSUMER PROD. SAFETY COMM'N, https://www.cpsc.gov/About-CPSC/ [https://perma.cc/2MFU-78ZX]. *See generally* Consumer Product Safety Act, 15 U.S.C. §§ 2051–2090.

(4) to promote research and investigation into the causes and prevention of product-related deaths, illnesses, and injuries.[178]

Due to its founding statute limiting the scope of the definition for "risks of injury" to risks of *physical* injuries,[179] the CPSC has remained largely uninvolved with the problematic space around IoT consumer products.[180] The Commission's jurisdiction only extends to those incidents where there is a physical manifestation of the harm caused by the IoT consumer product, and there simply haven't been many IoT safety incidents that have led to physical injuries.[181] For example, when a smart home device suffers a data breach, which then leads to unauthorized access to personal information of the device owner, such an incident would fall outside the CPSC's scope.[182] On the other hand, if a connected electric kettle were to be remotely tampered with so that it could

---

[178] *See* 15 U.S.C. § 2051(b).

[179] 15 U.S.C. § 2052(a)(14) ("The term 'risk of injury' means a risk of death, personal injury, or serious or frequent illness.").

[180] *See, e.g.*, Julie Y. Park, *CPSC Will Sharpen Its Focus on IoT in Upcoming Public Hearing About Internet-Connected Devices*, MORRISON FOERSTER: CLASS DISMISSED (Mar. 27, 2018), https://classdismissed.mofo.com/topics/cpsc-will-sharpen-its-focus-on-iot-in-upcoming-public-hearing-about-internet-connected-devices.html [https://perma.cc/D4AL-3PZ6] (With respect to potential regulation of IoT devices, "CPSC's focus remains where it has always been: on product hazards that cause physical injury or property damage"); ELLIOT F. KAYE & JONATHAN D. MIDGETT, U.S. CONSUMER PROD. SAFETY COMM'N, A FRAMEWORK OF SAFETY FOR THE INTERNET OF THINGS: CONSIDERATIONS FOR CONSUMER PRODUCT SAFETY 1 (Jan. 2019), https://www.cpsc.gov/s3fs-public/A_Framework_for_Safety_Across_the_Internet_of_Things_1-31-2019.pdf [https://perma.cc/KKY3-W9ZL]; A. Michael Froomkin, Phillip J. Arencibia & P. Zak Colangelo-Trenner, *Safety as Privacy*, 64 ARIZ. L. REV. 921, 957 (2022).

[181] *See, e.g.*, KAYE & MIDGETT, *supra* note 180, at 1; ADAM THIERER, JENNIFER HUDDLESTON SKEES & ANNE HOBSON, MERCATUS CTR. AT GEORGE MASON UNIV., THE INTERNET OF THINGS AND CONSUMER PRODUCT HAZARDS, 5 (June 2018), https://www.mercatus.org/media/66731/download?attachment [https://perma.cc/Q2J9-82NV] ("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."); *see also* JAMES ANDREW LEWIS, CTR. FOR STRATEGIC & INT'L STUD., MANAGING RISK FOR THE INTERNET OF THINGS 6 (Feb. 2016), https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/160217_Lewis_ManagingRiskIoT_Web_Redated.pdf [https://perma.cc/NCU8-RQ4A] ("Most of the vulnerabilities found in IoT devices lead to events that would qualify as pranks.").

[182] *See* U.S. CONSUMER PROD. SAFETY COMM'N, STATUS REPORT ON THE INTERNET OF THINGS (IOT) AND CONSUMER PRODUCT SAFETY 2 (Sept. 2019) [hereinafter CPSC STATUS REPORT], https://www.cpsc.gov/s3fs-public/Status-Report-to-the-Commission-on-the-Internet-of-Things-and-Consumer-Product-Safety.pdf [https://perma.cc/XSL4-N3ZE] ("CPSC does not consider personal data protection and privacy to be consumer product hazards that we would address, absent an associated unreasonable risk of injury."). *But see* Froomkin, Arencibia & Colangelo-Trenner, *supra* note 180, at 958 (arguing that privacy risks posed by IoT devices "fall tidily" within the scope of CPSC authority).

potentially explode and cause serious burns or other injury to someone nearby,[183] the CPSC would presumably investigate to understand whether the kettle's poor security features made it pose an unreasonable risk of injury to the user.

In more recent years the CPSC has started to take steps to define its role and increase its involvement in tackling the consumer IoT problem. In 2018, the Commission held a public hearing on the IoT, requesting information and feedback from stakeholders on the "potential safety issues and hazards associated with internet-connected consumer products."[184] In early 2019, CPSC Commissioner Elliot Kaye released a paper outlining a safety framework for the IoT, recommending that manufacturers conduct risk assessments and implement a variety of countermeasures for safety risks.[185] These countermeasures included certification of components according to industry standards and best practices, parental controls, user authentication for added security, redundant safeguarding (with physical safeguards preferred to software safeguards), and transparent disclosures about component tracking, data collection, and expected lifespan.[186]

Later that same year in September, CPSC staff submitted a status report to the Commission describing the CPSC's work on IoT issues since the 2018 public hearing.[187] The CPSC report stated that its staff is working on defining consumer product safety in terms of the IoT, and how "[its] traditional risk management approaches apply to connected products," following the observation that CPSC's mission of keeping consumers safe from unreasonable risks from consumer products intersects closely with data security in the current reality of IoT.[188] To further expand its involvement in addressing the safety of Internet-connected consumer products, the CPSC staff will be "[d]eveloping staff expertise and in-house capabilities for Internet-connected products (education/workforce development); [p]articipating in and developing voluntary consensus standards (domestic and international); [and c]ollaborating with other federal agencies, foreign governments, and with a wide range of stakeholders."[189] The report also described the various project work that CPSC

---

[183] This is not a random hypothetical; In a chilling live demonstration at a European Commission conference in 2018, a computer security expert showed how this precise scenario could play out. *See* Conference Agenda, European Commission, International Product Safety Week 2018: Connecting Safety (Nov. 12, 2018), https://commission.europa.eu/system/files/2018-11/ipsw-programme_2018_web.pdf [https://perma.cc/86KZ-LCSF].

[184] The Internet of Things and Consumer Product Hazards, 83 Fed. Reg. 13,122, 13,122 (Mar. 27, 2018) (explaining the reasoning for a notice of public hearing and request for written comments).

[185] KAYE & MIDGETT, *supra* note 180, at 2–6.

[186] *Id.* at 4–6.

[187] CPSC STATUS REPORT, *supra* note 182, at 2.

[188] *Id.* at 2, 6–7.

[189] *Id.* at 15.

staff was implementing, including the development of a methodology for assessing how software and firmware updates to connected products impact the product's safety.[190]

The CPSC's move to step into a larger role in IoT consumer product issues is a welcome development. The Commission has often been overlooked in policy conversations about IoT safety, even though it likely has the most relevant mandate among federal agencies to protect people from harms and hazards of IoT devices, and also has greatest expertise in evaluating the safety of products that touch the lives of everyday people.[191] The CPSC itself admitted in its report that despite its "product safety jurisdiction over the vast majority of connectable consumer products, there has been little recognition, to date, from Congress of CPSC's role in government-wide cybersecurity policy."[192] At the same time, the CPSC expects for this to change as it takes on greater leadership in working with other agencies and engaging stakeholders to address IoT product safety issues.[193] We share in this optimism and envision the CPSC taking center stage as policymakers and regulators take on the wide variety of issues arising from the ability of digital connectedness to affect physical change in the real world.

2. *Federal Trade Commission*

The Federal Trade Commission was established to promote fair competition and commerce; nowhere in the statute that established the FTC is data privacy or security mentioned.[194] The FTC started becoming more directly involved in protecting consumers on the Internet in 1990, when the Commission added policing of electronic commerce and privacy to its scope.[195] For policing poor digital security practices, the FTC often opens investigations into companies for unfair and deceptive practices, using its authority to regulate false advertising against manufacturers that misrepresent the security of their products.[196]

As the Internet of Things grew in prominence and ubiquity in everyday life in the past decade, so has the FTC's interest in the IoT as an area where consumer protection became increasingly needed. The agency hosted a workshop in November 2013 to discuss the various consumer benefits and risks

---

[190] *Id.* at 16.

[191] *See* Consumer Product Safety Act §§ 4–5, 15 U.S.C. §§ 2053–2054.

[192] CPSC STATUS REPORT, *supra* note 182, at 10.

[193] *Id.* at 2, 10.

[194] *See Federal Trade Commission*, USA.GOV, https://www.usa.gov/federal-agencies/federal-trade-commission#:~:text=The%20Federal%20Trade%20Commission%20works,and%20avoid%20scams%20and%20fraud [https://perma.cc/WC3G-DNSL]; Federal Trade Commission Act, 15 U.S.C. §§ 41–58.

[195] *See* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 67 (2016).

[196] *See id.* at 216–17.

borne by the IoT and published a report in early 2015 presenting key findings from the workshop.[197] The FTC has also frequently weighed in as an active stakeholder in various forums involving the discussion of security risks in the IoT.[198]

The FTC has also brought action against IoT manufacturers for poor security practices. In 2017, it brought claims against smart home product maker D-Link, whose Wi-Fi routers and Internet-connected cameras "left its wireless routers and Internet cameras vulnerable to hackers and put U.S. consumers' privacy at risk."[199] 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.[200] As part of its settlement with the FTC, D-Link agreed to abide by the court's orders to implement a comprehensive software development program, continuously monitor its systems for security flaws, and allow itself to be subject to third-party assessments of its software security program by FTC-approved auditors.[201]

More recently, the FTC settled with Tapplock, a smart lock manufacturer that was allegedly deceiving consumers by falsely claiming that its locks were "unbreakable" and that it took reasonable steps to secure personal information it collected from users.[202] As a result of the settlement, Tapplock will also be required to undergo regular third-party assessments of its information security program.[203]

Traditionally, the FTC has focused more on its enforcement toolkit rather than its rulemaking power, owing in part to special, burdensome procedural requirements placed by Congress upon the agency's rulemaking authority.[204]

---

[197] FED. TRADE COMM'N, *supra* note 13, at i–ii.

[198] The FTC's IoT-related activities have included providing comments for other agencies' requests for information, see, for example, Fed. Trade Comm'n, *supra* note 43, and publishing its own guidance on IoT security, see, for example, FED. TRADE COMM'N, *supra* note 68, at 1–10.

[199] Press Release, FTC, 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 [https://perma.cc/79RU-639L].

[200] Lesley Fair, *D-Link Settlement: Internet of Things Depends on Secure Software Development*, FED. TRADE COMM'N: BUSINESS BLOG (July 2, 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/07/d-link-settlement-internet-things-depends-secure-software [https://perma.cc/GN4V-7RNS].

[201] *Id.*

[202] Press Release, FTC, Canadian Maker of Smart Locks Settles FTC Allegations That It Deceived Consumers About Its Security Practices (Apr. 6, 2020), https://www.ftc.gov/news-events/press-releases/2020/04/canadian-maker-smart-locks-settles-ftc-allegations-it-deceived [https://perma.cc/L8Q9-MHR2].

[203] *Id.*

[204] HOOFNAGLE, *supra* note 195, at 334.

The FTC can therefore serve as an invaluable partner and resource to the CPSC, which is not burdened by these limits on its rulemaking power, as it continues to grow its own capacity and expertise to better handle issues related to IoT consumer products. For example, the FTC offered a comment to CPSC describing the ways that poor IoT security can lead to safety risks.[205]

B. *Mandatory Implementation Details*

We propose three principles to guide the design of legacy switches in order to ensure that they serve their intended purposes. All legacy switches must be (1) effective, (2) easy to use, and (3) externally verifiable.

1. *Effectiveness' Definitional Challenges: What Is a Thermostat?*

Effectiveness poses definitional challenges, because it forces the regulator to identify the smart features that must be disabled when the switch is engaged. Any law mandating a legacy switch must address a difficult, ontological, and almost metaphysical question: what exactly is a smart device? If we are to separate the "dumb" features from the "smart" ones, we need to write a definition that draws a line between separate categories of functionality, precisely delineating the features that make a device a smart device.

What must happen when a consumer flips a legacy switch? This reads like a postmodern riddle: what is the essence of a thermostat? The positive approach is to focus on the essential functionality we expect from the device: a doorbell sounds an audible chime when pressed; a thermostat switches an HVAC system on or off depending on the temperature; a refrigerator keeps things cold.[206] The negative approach is to list the harms we are trying to avoid, such as the harms to security, privacy, and the environment described earlier. These harms in turn come from specific device features, discrete bits of functionality added to a legacy product (thermostat, doorbell, refrigerator) that feed surveillance capitalism, increase a device's attack surface, provide mechanisms to threaten security or privacy, or hasten a device's obsolescence, for example.[207]

---

[205] Press, Release, FTC, *supra* note 76.

[206] *See* HARTZOG, *supra* note 24, at 267 (noting that IoT devices often have a "core function" that is unrelated to the "smart" addition); *see also, e.g.*, SCHNEIER, CLICK HERE, *supra* note 86, at 108–09 ("Users should be able to turn off all incoming and outgoing network connections while still being able to use the device. For example, an Internet-connected refrigerator should keep things cold even when not connected to the Internet.").

[207] *See* Hoofnagle, Kesari & Perzanowski, *supra* note 22, at 809–28, 868.

a. *An Institutional Design Approach to Defining Effectiveness*

Rather than answer this question exhaustively for every type of smart device, we will focus instead on the institutions that are best positioned to provide an answer and the types of procedures they might create or use to develop the answer.[208] Let's first dispense with two appealing but unworkable procedures for defining the smart features a legacy switch ought to disable, one at each end of the spectrum, from detailed and prescriptive to vague and deferential. First, Congress or a state legislature itself could spell out in statute and detail the precise features that ought to be disabled. Imagine a law that said, when enabled, a legacy switch should disable any smart device's network connection, screen, microphone, and camera. This approach would unacceptably overprotect and underprotect. A smart speaker without Bluetooth or a smart camera without a camera is a worthless lump of circuitry and plastic. Legislatures lack the institutional competence to undertake this work with specificity, and legislation is the wrong vehicle for spelling out nuanced requirements.

Second, a law could issue a vague standard and nothing more: a legacy switch should disable any feature that poses a significant threat to privacy or security that is not outweighed by the benefits the feature provides.[209] This approach would lead to different approaches by different manufacturers. It would require monitoring and enforcement, either externally by a government agency or internally by a self-enforcement mechanism, which would be costly and time consuming. It would water down the protection, giving manufacturers the power to cling to the most profitable features, even if they pose risks. All of this would lead to consumer confusion.

We prefer a middle way between these two extremes. A statute mandating legacy switches could list the harms that legacy switches must be designed to address and then prescribe administrative procedures for connecting these harms to specific device features that must be disabled by a legacy switch for a particular type of device. For example, the statute might mandate legacy switches in smart home devices that disable features that lead to harms to privacy or security, further directing the CPSC or FTC to engage in public rulemakings to define the lists of features. The agency assigned would then progress through three steps, engaging with public stakeholders along the way: first, it would more precisely elaborate the specific harms the legacy switch is meant to prevent. The lists should include surveillance, security (both

---

[208] We will focus on government institutions and procedures, although these definitions may come from non-governmental sources such as standards-setting bodies too. *See* HARTZOG, *supra* note 24, at 270 (noting efforts by standards bodies to establish privacy and security design standards for IoT devices).

[209] *Cf.* 15 U.S.C. § 45(n) (limiting the FTC's unfairness authority to acts or practices that "cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition").

cybersecurity and protection of personal safety), invasions of privacy, and undue restrictions of consumer choice, but certain devices might raise other concerns. Second, the group should identify the features that increase the risk of the particular harm. Microphones pose risks to privacy, speakers provide avenues for harassment, and network connections pose risks to cybersecurity and privacy. Finally, the group would publish a list of features that must be disabled in a legacy state.

This approach might be supported by rigorous threat modeling and assessment approaches from the field of computer security. In the past, we have urged legal scholars and policymakers to borrow these approaches into debates about privacy and security.[210]

At the end of this process, rather than announce a list of features to be disabled, it might be more efficient, if a bit less tailored, to announce a temporal line—a specific date or even model number that represents the start of "smart" functionality that needs to be disabled. The agency or standards body could study product histories from various vendors to track when various features were introduced. They could identify a critical moment in time when products in the category first became subject to a significant risk of the harms the legacy switch is meant to avoid. It could choose that date or model number as the critical moment in time—any feature introduced after that date or model would be on the list of features disabled by a legacy switch.

A temporal approach has the typical benefits of a rule over a standard.[211] The bright-line choice of a single moment of time is simple to apply and easy for those charged with enforcement to verify. The downside of this approach is also typical of a rule. A temporal approach is not directly tethered to the harm we are trying to avoid, so it is likely to overprotect and may also underprotect. Some recent innovations in thermostat technology might raise substantial benefits without contributing much to the risk of harm, yet a temporal rule would throw out those innovations along with the harmful pieces.

b. *Smart Features a Legacy Switch Might Enable*

To make our prescription even more concrete, consider the following features that are associated with smart/IoT technology. These are the kind of

---

[210] *See* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1172–79 (2015); NATHANIEL KIM, TREY HERR & BRUCE SCHNEIER, ATL. COUNCIL, THE REVERSE CASCADE: ENFORCING SECURITY ON THE GLOBAL IOT SUPPLY CHAIN, 1–2 (June 15, 2020), https://www.atlanticcouncil.org/wp-content/uploads/2020/06/Reverse-Cascade-Report-web.pdf [https://perma.cc/QX76-LS94].

[211] *See* HARTZOG, *supra* note 24, at 121–23 (arguing for standards over rules for governing design to protect privacy). *See generally* Michael Coenen, *Rules Against Rulification*, 124 YALE L.J. 644 (2014); Cass R. Sunstein, *Problems with Rules*, 83 CALIF. L. REV. 953 (1995); Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557 (1992); Pierre Schlag, *Rules and Standards*, 33 UCLA L. REV. 379 (1985).

features a rule ought to require a legacy switch to disable, as well as the risks of harm the features have introduced. Consider this a starting point, one to be refined and improved through the rulemaking or standards-setting processes described above.

Wi-Fi: Wi-Fi connects IoT devices to the outside world. The network connectivity Wi-Fi permits the exfiltration of information about the interior of the home to those outside the home, and they permit people on the outside to control the operation of the device on the inside.[212] These outside actors receiving information and sending controls can be the vendors themselves, third-parties authorized by the vendors, or malicious interlopers exploiting vulnerabilities in the system.[213] They can be participants in the surveillance economy, bad actors looking to steal or exploit information, or both.[214] Wi-Fi is a source of significant potential security harm and privacy harm.

Wi-Fi is the feature we believe most often should be disabled by a legacy switch. The connection to the outside world—both in-bound and out-bound—is a critical enabler of most of the harms described earlier. In-bound networking empowers remote control by bad actors.[215] Out-bound networking provides the pathway to leak information about private behavior inside the home.[216]

Importantly, "dumb" devices that predated the newer smart versions never relied on anything like Internet connectivity. This suggests that these devices—thermostats, doorbells, smoke alarms—can operate perfectly well without the ability to send or receive packets to the Internet.

Microphones and cameras: Smart devices often come with embedded cameras and microphones.[217] These are used to provide functionality—for example, to enable smart assistants like Siri or Alexa—and they drive more surprising and potentially unwelcome features—such as allowing your smart

---

[212] Aliza Vigderman & Gabe Turner, *What Is Home Automation and How Does It Work?*, SECURITY.ORG (May 12, 2022), https://www.security.org/home-automation/ [https://perma.cc/7GE4-59SV].

[213] *See* Andrew Rens, *Who Is in Charge Here? The Internet of Things, Governance and the Global Intellectual Property Regime*, 23 UCLA J.L. & TECH i, 21 (2019); Beale & Berris, *supra* note 6, at 167.

[214] *See* Rens, *supra* note 213; Donnell Holloway, *Explainer: What Is Surveillance Capitalism and How Does It Shape Our Economy?*, CONVERSATION (June 24, 2019), https://theconversation.com/explainer-what-is-surveillance-capitalism-and-how-does-it-shape-our-economy-119158 [https://perma.cc/ET3M-DL4F].

[215] *See* Nicole Smith, Note, *Protecting Consumers in the Age of the Internet of Things*, 93 ST. JOHN'S L. REV. 851, 859–61 (2019).

[216] *See id.* at 861–64.

[217] *E.g.*, Herb Weisbaum, *The Downside of Connected Tech: Are the Smart Devices in Your Home Spying on You?*, NBC NEWS: BETTER (Dec. 16, 2019), https://www.nbcnews.com/better/lifestyle/downside-connected-tech-are-smart-devices-your-home-spying-you-ncna1101906 [https://perma.cc/VS7E-SFSQ].

television to hear ultrasonic squeals from your computer, enabling powerful and invasive ad tracking.[218]

Speakers: Increasingly, our IoT devices talk to us. The primitive beeps and clicks that once emanated from our refrigerators, smoke alarms, and thermostats, have been replaced by computer voices speaking complete sentences. Many devices double as portals for smart assistants such as Apple's Siri, Amazon's Alexa, or Google's Assistant, who engage us in conversation.[219]

Speakers are also vectors for privacy and security harms. Abusive ex-partners use speakers to harass or to make their victims think they are hearing voices.[220] Strangers talk to children over the speakers built into nanny cams left open to the Internet.[221] Tones emanated at frequencies outside the range of normal hearing can transmit information to the microphones in other devices. For these reasons and more, the CPSC, FTC, or other standards-setting body might conclude that legacy switches in some devices should disable any speakers.

It does not make sense, however, to shut off a speaker for some devices. Speakers that are intrinsic to the utility of the device should not be subject to a legacy switch. One giveaway are categories of devices that have long had speakers, dating back before the rise of the IoT. Televisions and radios are examples. No legacy switch should silence these devices. So too with today's so-called smart speakers, often paired with smartphones to playroom-filling amplified music or podcasts.

Bluetooth: Bluetooth differs from Wi-Fi in an important way: Bluetooth is intended for data exchange across relatively short distances, while Wi-Fi is often used as a portal to communications with the Internet.[222] Bluetooth is commonly used, for example, to connect a keyboard or mouse to a computer; to transmit audio from a smartphone to a speaker or headphones, or to communicate sensor data to a smart home hub.[223] There are many flavors and versions of Bluetooth,

---

[218] The CDT described SilverPush as an example of this kind of cross-device tracking through audio beacons in its response to the FTC's request for comments. *See* Letter from Chris Calabrese, Vice President, Katherine L. McInnis, Privacy & Technology Fellow, G.S. Hans, Policy Counsel & Director, & Greg Norcie Staff Technologist, Center for Democracy & Technology, to Federal Trade Commission, Re: Comments for November 2015 Workshop on Cross-Device Tracking (Oct. 16, 2015), https://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf [https://perma.cc/E3R9-79AS].

[219] Parker Hall, *The Best Smart Speakers with Alexa, Google Assistant, and Siri*, WIRED (Sept. 27, 2022), https://www.wired.com/story/best-smart-speakers/ [https://perma.cc/Y5Z2-U9HD].

[220] Bowles, *supra* note 16.

[221] Wang, *supra* note 18.

[222] *See* Jeremy Laukkonen, *Bluetooth vs. Wi-Fi: What's the Difference?*, LIFEWIRE (Feb. 24, 2020), https://www.lifewire.com/bluetooth-vs-wi-fi-4088218 [https://perma.cc/84KM-LHW4] ("[T]he range of a Wi-Fi network is typically larger than a Bluetooth connection.").

[223] *Id.*

but all tend to have smaller effective transmission ranges than other wireless communications protocols, commonly less than ten meters.[224]

For these reasons, Bluetooth is often more intrinsic to the operation of a smart device and would render the device much less useful if not unusable if disabled. A wireless headset without Bluetooth simply serves no purpose. For the same reason, the kinds of information usually transmitted via Bluetooth are not as directly connected to the harms to privacy and security described above. There are notable exceptions, devices that use Bluetooth for networked communications, as a replacement for Wi-Fi.[225] A similarly named but distinct technology called Bluetooth Low Energy (BLE) is increasingly used for sensors,[226] which again might be too important to an IoT device to disable it. But BLE is also increasingly used to track user and device location and movement, which might be a reason to add it to the list to be disabled.[227]

Smartphone app integration: Most smart home IoT devices interact with apps on user smartphones.[228] Since many IoT devices lack screens, an app is often the best way to make rich controls available for monitoring, configuring, and troubleshooting the device.[229] Often, these apps are poorly designed and maintained.[230] They may suffer from security problems that widen the overall attack surface of the device.[231]

---

[224] *See id.*; John Fuller & Chris Pollette, *How Bluetooth Surveillance Works*, HOWSTUFFWORKS (Oct. 20, 2021), https://electronics.howstuffworks.com/bluetooth-surveillance.htm [https://perma.cc/QVC9-YPV4] (describing Bluetooth's range as a "10-meter (33-foot) circle around [the user]").

[225] *See, e.g.*, Melanie Uy, *How to Get Internet with a Bluetooth-Enabled Cell Phone*, LIFEWIRE (May 10, 2022), https://www.lifewire.com/internet-on-laptop-with-a-bluetooth-enabled-cell-phone-2377930 [https://perma.cc/89B6-AZNT].

[226] *See* Elliot Nesbo, *What Is BLE (Bluetooth Low Energy) and How Does It Work?*, MAKE USE OF (Dec. 27, 2021), https://www.makeuseof.com/what-is-ble-bluetooth-low-energy/ [https://perma.cc/9T3C-H6FS].

[227] *Id.*

[228] *See* T.J. OConnor, Dylan Jessee & Daniel Campos, *Through the Spyglass: Toward IoT Companion App Man-in-the-Middle Attacks*, 14 PROC. CSET 58, 58 (2021), https://dl.acm.org/doi/pdf/10.1145/3474718.3474729 [https://perma.cc/FV5P-MSTV].

[229] *Id.* at 3–4.

[230] *Id.* at 4 (revealing critical cryptographic flaws in smartphone apps for popular smart home devices); *see also* Haotian Chi, Qiang Zeng, Xiaojiang Du & Jiaping Yu, *Cross-App Interference Threats in Smart Homes: Categorization, Detection and Handling*, 50 IEEE/IFIP INT'L CONF. ON DSN 411, 411 (2020), https://cs.gmu.edu/~qzeng2/papers/2020-dsn-homeguard.pdf [https://perma.cc/2569-RM36] (demonstrating that home automation apps can still cause security risks when they interact with each other, even if they are individually secure); Kaushal Kafle, Kevin Moran, Sunil Manandhar, Adwiat Nadkarni & Denis Poshyvanyk, *A Study of Data Store-Based Home Automation*, 29 PROC. ACM CONF. ON DATA & APPLICATION SEC. & PRIV. 73, 82 (2019), https://dl.acm.org/doi/pdf/10.1145/3292006.3300031 [https://perma.cc/87SR-7DES] ("The security of the smart home indirectly depends on the smart phone (apps).").

[231] OConnor, Jessee & Campos, *supra* note 228, at 2.

As with Bluetooth, the problem is that many of these devices would be hard or impossible to use without the associated app. Regulators may conclude, after study, notice, and comment, that app integration is too important to require it to be disabled with a legacy switch, at least for some categories of products. Or they may conclude that because app integration poses such risks that it must be disabled with the legacy switch, manufacturers may be obligated to build in a redundant subset of the controls provided by the app into the device itself. For example, a smart thermostat without a screen might require a rudimentary set of physical switches and a small screen for use after legacy switches have been thrown.

c. *A Tricky Case Study: Smart Security Systems*

To demonstrate some of the pitfalls that enter the effectiveness analysis, and to highlight the need for expert regulatory attention, consider smart security systems. The home security industry has been transformed in the past few decades from a service industry that once required expensive and permanent installations and pricey round-the-clock monitoring to cheaper do-it-yourself solutions built on IoT technologies.[232] Product lines like SimpliSafe and Ring Alarm allow untrained individuals to install contact sensors on doors and windows, motion sensors, security cameras, glass-break audio monitors, and more in the form of small, plastic IoT devices that use standard wireless protocols to communicate with one another.[233] Today's homeowner has a cheaper and simpler alternative to the professional service model, which still exists for those willing to pay more for less individual hassle.[234]

To implement a legacy switch solution for systems like SimpliSafe or Ring Alarm, we need to resolve some tricky questions. First, does every device in a security system need a legacy switch, or should a single legacy switch control the entire security system? Although an agency process could conclude otherwise, we see a good argument to require a single switch for the entire system rather than one on each device. It's unclear what a legacy switch would mean for a single door contact sensor, for example. Such a sensor would have

---

[232] *See* Parks Associates, *Home Security: A Redefined Market*, PARKS PERSPS. (May 19, 2021), https://www.parksassociates.com/blog/article/home-security--a-redefined-market-[https://perma.cc/5TZG-BJVE]; *The Definitive History of Home Security Systems*, HOMEWATCH GRP. (Feb. 28, 2021), https://www.homewatchgroup.com/the-definitive-history-of-home-security-systems/ [https://perma.cc/L7L6-CD5P].

[233] *See generally* SIMPLISAFE, https://simplisafe.com/ [https://perma.cc/TSG9-JHHU]; RING, https://ring.com/security-system [https://perma.cc/GJ42-H3DM]; *Glass Break Detector*, SLOMIN'S, https://www.slomins.com/product/audio-glass-break-detector/ [https://perma.cc/X6TE-RQCU].

[234] *See Home Security System Buying Guide*, CONSUMER REPS., https://www.consumerreports.org/home-garden/home-security-systems/buying-guide/ [https://perma.cc/F2FT-CDAA] (July 1, 2022) (comparing DIY and professionally installed home security systems).

two functions: (1) detect when the door has been opened, and (2) send a signal to a monitoring system in the home or across the Internet. Disabling either function would render a door switch no longer useful.

Second, and more fundamentally, should a legacy system cut off a home security system from communication with the outside world? Opening a door when an alarm system has been armed will usually trigger an audible siren loud enough to alert residents, scare off intruders, and possibly alert people outside the building. Depending on how the system is configured, and possibly on whether the homeowner pays a recurring fee, it might also notify a security monitoring service, the local police department, or both.[235] Since Wi-Fi and Internet communication tend to be a major vector for security threats, one might conclude that a legacy switch on a security system should disable all communications outside the residence, perhaps limiting the system to generating audible alarms.

The ontological, "what is a home security system?" analysis might conclude that a home security system that cannot alert a central monitor is no longer a viable home security system. More practically speaking, providing a switch that prevents the police from knowing about break-ins raises a significant risk of harm to individuals due to consumer confusion. On the other hand, some consumers might benefit from and value a legacy switch that retains the audible alarms but loses central monitoring, in exchange for less susceptibility to being hacked or hijacked by outsiders. Once again, we would want an expert agency to work through these issues with participation from the public.

The difficulties in this case study seem particular to security systems. We focus on it to highlight the need for expert agencies—not the legislature—to elucidate the rules. We think the process will be far clearer and simpler for most other IoT devices: smart refrigerators, televisions, and thermostats will raise far fewer difficult and nuanced questions.

2. *Easy-to-Use and Externally Verifiable*

A second mandatory requirement is that every legacy switch should afford a simple, clear mechanism for disabling all smart technology and connectivity in the device. It should offer a single, binary choice: "smart and connected" or "dumb and disconnected." We imagine something quite similar to the physical mute switches that Google and Amazon have added to their smart speakers,[236] except the legacy switch would likely turn off more than just the device's

---

[235] *See id.*

[236] Chaim Gartenberg, *The Google Home Mini's Mute Switch Makes Privacy Deliberate*, VERGE (Aug. 23, 2019), https://www.theverge.com/circuitbreaker/2019/8/23/20828854/google-home-mini-mute-switch-button-privacy-microphones [https://perma.cc/MM5C-XRKP]; Charles Radclyffe, *The Deliberate Design Flaw In Every Amazon Echo*, FORBES (Aug. 29, 2018), https://www.forbes.com/sites/charlesradclyffe/2018/08/29/the-deliberate-design-flaw-in-every-amazon-echo/?sh=16756ada31b0 [https://perma.cc/UP7L-6RMB].

microphone, depending on the line drawn by the agency promulgating the rules. For example, it might also disable the virtual assistant and disconnect the speaker from the Internet, turning the device into just another set of wireless speakers. The user should not have to choose from a complex menu of dozens of granular preferences, like disabling the video camera while continuing to enable the microphone on a smart doorbell. Even if finer grained options must be tolerated, they should not interfere with the user's ability to find the one choice that says, "disable all smart functionality."

Because smart home devices have specifically been used by domestic abusers to stalk and terrorize their victims,[237] legacy switches should be accessible even to those without ordinary control over the device. In other words, even one without a device password or authenticated app on their smartphone should be able to disable the device.

Finally, legacy switches must be externally verifiable; that is, there should be an easy way to prove that a smart device has been rendered dumb. One possibility is to build the verification function into home Wi-Fi routers. The router can report to the user—via the router webpage typically used to configure router settings, or through an interactive screen directly on the router—that an IoT device that once connected to the Internet through the router has stopped sending and receiving packets. It may also be in the interest of manufacturers to notify the user when the legacy switch is thrown and they cease to receive any data from a previously communicative device, if only to check whether it was done by accident. Either way, the notification could easily serve as external verification that the legacy switch worked as intended.

3. *Might Legacy Switches Make Devices Less Secure and Less Reliable?*

Especially if implemented poorly, a legacy switch might introduce new security and reliability problems. On balance, these risks might make the cure worse than the disease, so we should take care to design procedures to reduce them.

The security problem is, again, the attack surface. Although attackers sometimes try to hijack a device to spy on a target, in other cases the goal is to disable or shut off the device.[238] Because a legacy switch will introduce a way

---

[237] Bowles, *supra* note 16.

[238] Cybersecurity experts would refer to these types of attacks as confidentiality and availability attacks, respectively, which are part of the information security triad of confidentiality, integrity, and availability. *See, e.g.*, Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 997–98 (2018). Bruce Schneier's example illustrates the differences well:

> [W]hile I am worried that someone will hack into the car and eavesdrop on my conversations through the Bluetooth connection (a confidentiality threat), I am much more worried that they will disable the brakes (an availability threat) or modify the

to shut off some key functionality of a device, an attacker might learn to flip the legacy switch remotely, disabling the smart features against the owner's wishes.

To reduce the attack surface, legacy switches should not be accessible from outside the IoT device's network. They should not, for example, be controlled by settings on a manufacturer's cloud server. Permitting remote control would give attackers a powerful vector for an attack. Remote control would also introduce the possibility of government-mandated use of an individual's legacy switch. Imagine the police seek permission in a search warrant to remotely disable a target's smart security devices using legacy switch settings before a judicially approved raid on their property. Civil liberties groups,[239] security experts,[240] political leaders,[241] and others have explained the problems with giving the government control over so-called "Internet kill switches," often pointing out the way the Egyptian government tried to disable Internet access during the Arab Spring to squelch protest and speech.[242]

Another security risk introduced by a legacy switch is the way it might make it impossible to update the software on a device switched to its legacy state. Because legacy switches will often remove a device from the Internet, they will take away the ability for the device to "phone home" to download critical security patches.[243]

Legacy switches may make devices less reliable. Regardless of how they are implemented, they will require the manufacturer to design an entirely new mode of operation for their device. The manufacturer will need to subject the switch to extensive testing to ensure the other mode operates reliability.

> parameters of the automatic lane-centering and following-distance systems (an integrity threat). The confidentiality threat affects my privacy; the availability and integrity threats can kill me.

SCHNEIER, CLICK HERE, *supra* note 86, at 79.

[239] *See, e.g.*, CYBERSECURITY AND CIVIL LIBERTIES: THE "KILL SWITCH," ACLU 1 (Feb. 2012), https://www.aclu.org/sites/default/files/field_document/aclu_one_pager_kill_switch.pdf [https://perma.cc/72HU-9BQF].

[240] *See, e.g.*, Bruce Schneier, *I've Seen the Future, and It Has a Kill Switch*, WIRED (June 26, 2008), https://www.wired.com/2008/06/securitymatters-0626/ [https://perma.cc/9782-EADU].

[241] *See, e.g.*, Press Release, Rand Paul, United States Senator, Sens. Paul, Wyden, and Peters, Reps. Gabbard and Massie Launch Bipartisan, Bicameral Push to Unplug Internet 'Kill Switch,' Protect Civil Liberties (Sept. 23, 2020), https://www.paul.senate.gov/news-sens-paul-wyden-and-peters-reps-gabbard-and-massie-launch-bipartisan-bicameral-push-unplug/ [https://perma.cc/4W5Z-5CDM].

[242] *See* Declan McCullagh, *Internet 'Kill Switch' Bill Gets a Makeover*, CNET (Feb. 18, 2011), https://www.cnet.com/tech/services-and-software/internet-kill-switch-bill-gets-a-makeover/ [https://perma.cc/F6FB-S7TZ]; Emily Banks, *Egyptian President Steps Down Amidst Groundbreaking Digital Revolution*, CNN (Feb. 11, 2011), https://www.cnn.com/2011/TECH/social.media/02/11/egyptian.president.digital.mashable/index.html [https://perma.cc/5Z7Y-LBBN].

[243] *See* Hoofnagle, Kesari & Perzanowski, *supra* note 22, at 792.

All of these problems will be exacerbated by the incentives on manufacturers. Because legacy switches might be treated like compliance burdens rather than demand-driven features, manufacturers might devote inferior human and engineering resources—their so-called "B Team"—toward their development.

We need to take these concerns seriously and calibrate the incentives to address them. At the very least, legislation mandating a legacy switch should require manufacturers to consider and minimize the security and reliability risks introduced by the legacy switch, and it should empower the regulating agency to monitor compliance with these requirements and to penalize violations. The agency should have the right to test the way this requirement gets implemented, and the power to mandate fixes for poor implementations and in extreme cases, the ability to recall devices that cannot be fixed remotely.

A well-implemented legacy switch will counteract the security and reliability risks it introduces, so we ought not exaggerate the scale of this concern. For example, while a IoT device with a disabled Internet connection might lose the pathway for downloading security updates, a truly disabled Internet connection should also have a dramatically reduced attack surface, by taking away the most important vector for attacks.[244] A device with a glaring security hole that nobody on the Internet can exploit is arguably more secure than another device without that specific security hole but connected to the Internet.

We must also remember to ask, "compared to what?" The new vulnerabilities introduced by a legacy switch should be balanced against the unsecure, intrinsically nonprivate devices being sold today, devices that are difficult to patch, insufficiently secured, and shuffled rapidly into an early "end of life" zombie state.[245] Compared to the status quo, the risk that a legacy switch will be the cause of insecurity or unreliability rather than the cure perhaps seems less serious and more easily reducible.

C. *Discretionary Implementation Proposals*

All legacy switches must have the three features described above: effectiveness, ease-of-use, and external verifiability. In addition, manufacturers may embrace or regulators may require two other features to give rise to additional benefits to consumers: First, some legacy switches should be

---

[244] Richard Barrus, *Stop What You're Doing and Get Every Possible IoT Connected Device Off the Internet . . . NOW*, PIVOTPOINT SEC. (Mar. 23, 2017), https://www.pivotpointsecurity.com/blog/iot-connected-device-security/ [https://perma.cc/249A-H9H2] ("Taking all possible systems and connected devices off the Internet is an essential step in battening down your network and minimizing your attack surface.").

[245] *See generally* Woodrow Hartzog & Evan Selinger, *The Internet of Heirlooms and Disposable Things*, 17 N.C. J.L. & TECH. 581 (2016) (describing the ever-growing wave of IoT devices that are cheap, insecure, and soon obsolete); Hoofnagle, Kesari & Perzanowski, *supra* note 22, at 810–28 (outlining IoT-related harms to consumers).

irreversible—once they are flipped, they should not be permitted to be flipped back. Second, regulators might insist that some legacy switches be implemented with a physical switch rather than as a software option. We explain the advantages of these options below.

1. *Irreversibility*

We might require some legacy switches to operate only in one direction, able to turn a device from smart to legacy without being able to reverse the decision. To implement irreversibility, manufacturers might use technology out of a spy novel. There are chips that can physically erase themselves when a current is applied in the right way.[246] Or if the smart and dumb halves sit on circuit boards, a user can literally remove the wire traces that connect the two halves by scratching them off, or applying acid to them, or breaking the circuit board in the right place. Focusing beyond the smart home for a moment, imagine deploying hard-hatted workers across a smart city, instructing them to grip the circuit board of a smart traffic light or bus stop marquee with pliers, snapping clean at the pre-scored boundary layer, flipping the legacy switch in a particularly visceral way, with an audible, satisfying, "crack."

Irreversibility is most important to address the security threat from outdated, end-of-life hardware. To revisit a metaphor, permitting a legacy switch to be reversed and put back in smart operation resumes the security time bomb's ticking countdown. An insecure device that is removed from a network on day zero will only be more vulnerable to exploit on day thirty or day sixty.

As a means for combatting some of the other harms we have discussed, irreversibility may not be a good idea. For victims of domestic abuse, a legacy switch might provide temporary relief when the threat of abuse is highest. The victim can switch off a smart camera her abuser is using to spy, but a reversible switch would return the full functionality of the camera once the abuser has been forced or persuaded to give up control of the camera.

Reversible legacy switches also protect against accidental use. Those in households with children might be frustrated to irreversibly lose the smart functionality of an expensive television or refrigerator due to their toddler's curiosity. A reversible legacy switch will avoid this frustration.

Clever engineering may provide the benefits of both irreversibility and reversibility by rendering switches easy to flip and difficult to revert. For example, some switches might lock in place into the "engaged" position, requiring a physical key (or other part) to flip back to disengage. This will add

---

[246] *See, e.g.*, Nicole Casal Moore, *A Self-Erasing Chip for Security and Anti-Counterfeit Tech*, UNIV. OF MICH. NEWS (Sept. 24, 2020), https://news.umich.edu/a-self-erasing-chip-for-security-and-anti-counterfeit-tech/ [https://perma.cc/MKW9-33TM]; Tia Ghose, *This Computer Chip Will Self-Destruct in 5 Seconds*, LIVESCIENCE (Oct. 6, 2015), https://www.livescience.com/52397-self-destructing-chip-secures-data.html [https://perma.cc/T894-DG7E].

friction to the return to a smart state, without taking that possibility away forever.

2. *Most Legacy Switches Should Be Physical Switches*

We predict that many manufacturers will opt to implement legacy switches in software, giving users a virtual slider switch in an app connected to the device or on the tiny screen of the device. In most cases, legacy switches should be physical switches instead; a simple, physical slider or lever that flips from "smart" to "legacy." This supports all three principles described above: ease-of-use, effectiveness, and verifiability.

Physical switches are very easy to use. They afford a visible, binary setting—on or off. We first encounter physical switches early in childhood and interact with them every day of our lives. They require less accurate motor skills and eyesight than swiping on a tiny device screen, and they require less technical know-how than installing and interacting with an app on a smartphone.

Physical switches reduce the attack surface. Malevolent hackers, disgruntled ex-partners, and government officials will not be able to flip a physical switch remotely.

Physical switches foster ease of use by working regardless of authorization, access rights, or passwords. This supports victims of domestic abuse living in a space full of devices installed and controlled by their abuser. This also supports people who have simply forgotten their password or no longer own the smartphone on which they installed the associated app, solving likely problems consumers will encounter revisiting devices they installed a few years prior.

Finally, physical switches are a paradigm of external verifiability. It indicates to anyone near the device that it has been ordered into the legacy state.

V. BEYOND LEGACY SWITCHES

Legacy switches are no panacea for the fundamental, structural problems wrought by new technology. We see them as a piece of a broader project of redesigning public and private governance institutions to address these harms. Scholars like Cohen, Zuboff, and Hartzog have begun to sketch what a radically redesigned governance looks like.[247] Let us highlight how prescriptions like legacy switch mandates should play a role in these efforts.

---

[247] *See* COHEN, *supra* note 9, at 270–71; ZUBOFF, *supra* note 8, at 521–25; HARTZOG, *supra* note 24, at 157–93.

A. *Legacy Switches and the Problems with Consent Solutions*

Much recent scholarly writing about information privacy refutes approaches based on consent or control.[248] Legacy switches might be seen as yet another misguided control approach, a solution premised on the idea that users can decide for themselves when to opt-out of the risks inherent in IoT devices. While we agree wholeheartedly with the critics of control, we think legacy switches might be a rare example in which control can still do some important work.

The now canonical critique of control is Dan Solove's notion of "privacy self-management."[249] Solove decries the way consent-based approaches to privacy bombard the typical consumer with an endless parade of consent dashboards of increasingly complicated design.[250] Consumers are too busy to attend to their privacy in this kind of fine detail, especially because the true costs and benefits of any choice are obscured beneath technical complexity.[251] Consumers are seriously outmatched by sophisticated technology platforms that can harness the power of design and choice architecture to exploit the stickiness of default choices.[252] Tech companies employ behavioral scientists harnessing the latest advances in methods for shaping human decisions, using A/B testing and manipulative dark patterns.[253] No sophisticated privacy scholar writing today holds out hope for solutions premised on giving consumers increased choice and control.

In the face of this universal condemnation, we understand that our proposal may seem retrograde or counterproductive. We embrace the critiques of control and agree that solutions based on consent and control should not play a central role in strategies to increase privacy. Still, we can never take the user or the market out of our considerations. We need new rules to protect consumers from predatory manufacturers, but we also need to strengthen ways to empower the consumer. Our proposal serves as a rare exception to the privacy self-management critique for several reasons.

First, while critics have focused on the problems of control for questions of privacy or consumer protection, they have said less about control as a tool to protect security, or the environment. To protect security, specifically, we cannot abandon end-user self-management. The best security is "Defense in Depth,"

---

[248] *E.g.*, Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880–82 (2013).

[249] *Id.* at 1880.

[250] *See id.* at 1898–99.

[251] *See id.* at 1885, 1890.

[252] *See id.*

[253] Hannah Fry, *Big Tech Is Testing You*, NEW YORKER (Feb. 24, 2020), https://www.newyorker.com/magazine/2020/03/02/big-tech-is-testing-you [https://perma.cc/VT3N-DDYM]; Sara Morrison, *Dark Patterns, the Tricks Websites Use to Make You Say Yes, Explained*, VOX (Apr. 1, 2021), https://www.vox.com/recode/22351108/dark-patterns-ui-web-design-privacy [https://perma.cc/2ZBD-W4H3].

meaning a multi-layered approach, one which inevitably requires attention and participation by the user.[254] For example, we rely heavily on giving end users control mechanisms to protect digital networks, such as passwords and two-factor authentication.[255]

Second, for most people, the number of IoT devices they control is far less than the number of apps on their smartphone or websites they visit.[256] The physicality of IoT puts a constraint on the number of devices we can have in our home. These things take up space. We need to have them shipped to our homes, installed in our walls, and wired up to our powerlines. IoT devices are not given away for free, the way many smartphone apps are, even if many are sold at a loss.[257] This caps the number of devices that may have legacy switches, and thus the number of choices legacy switches put before a user. The decision of whether to flip a legacy switch will not come up often, and in many cases, consumers will flip the switch once and never think of it again. Staunch critics of control should understand that control must continue to play a role in privacy law; the goal is to reduce the number of situations governed by control to a much smaller, much more human-manageable number.[258]

---

[254] *See* U.S. DEP'T OF HOMELAND SEC., RECOMMENDED PRACTICE: IMPROVING INDUSTRIAL CONTROL SYSTEM CYBERSECURITY WITH DEFENSE-IN-DEPTH STRATEGIES 2 (Sept. 2016), https://www.cisa.gov/uscert/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf [https://perma.cc/5QCA-STDW].

[255] *See, e.g.*, Don Malloy, *Back to Basics: What's Multi-Factor Authentication—and Why Should I Care?*, NAT'L INST. OF STANDARDS & TECH.: CYBERSEC. INSIGHTS, https://www.nist.gov/blogs/cybersecurity-insights/back-basics-whats-multi-factor-authentication-and-why-should-i-care [https://perma.cc/A7ZB-V7N2].

[256] *See, e.g.*, Press Release, Deloitte, Consumers Benefit from Virtual Experiences, but Need Help Managing Screen Time, Security and Tech Overload (Aug. 3, 2022), https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/connectivity-and-mobile-trends.html [https://perma.cc/6D9E-LAY3] ("On average, U.S. households now have a total of 22 connected devices, down from 25 in 2021."); Maitrik Kataria, *App Usage Statistics 2022 That'll Surprise You (Updated)*, SIMFORM, https://www.simform.com/blog/the-state-of-mobile-app-usage/ [https://perma.cc/F427-KVBE] (Jan. 4, 2023) ("[A]n average person has 40 apps installed on his phone."); Nicola Bleu, *27 Latest Website Statistics for 2023: Data-Backed Facts and Trends*, BLOGGINGWIZARD (Jan. 1, 2023), https://bloggingwizard.com/website-statistics [https://perma.cc/D7JT-XMZJ] ("On average internet users in the US visit over 130 web pages per day.").

[257] *See* Bret Kinsella, *Why Tech Giants Are So Desperate to Provide Your Voice Assistant*, HARV. BUS. REV. (May 7, 2019), https://hbr.org/2019/05/why-tech-giants-are-so-desperate-to-provide-your-voice-assistant [https://perma.cc/K3X3-XCFG]; Nash Riggins, *Smart Marketing: Losing Money to Make Money*, NEW ECON. (Dec. 13, 2013), https://www.theneweconomy.com/strategy/smart-marketing-losing-money-to-make-money [https://perma.cc/WPC8-SRAK].

[258] *E.g.*, HARTZOG, *supra* note 24, at 67 ("Privacy regimes should seek to preserve control for when it can be the most effective, and leave the rest to other concepts, like privacy-friendly design.").

Third, the implementation details we presented in Part IV attempt to reduce the complexity and cognitive burden associated with privacy self-management. Legacy switches will not serve their purpose if they are bogged down with sub-choices and sub-sub-choices. They should present a binary choice: a device can be "smart" or it can be put into its legacy "dumb" state, presented as a simple option in a setting screen or, better yet, as a physical switch.

We think these factors make our proposal a rare exception to the modern understanding that solutions around control and consent have failed and ought to be disfavored. We are not trying to breathe new life into this marginalized approach. Instead, we see our proposal as a narrow exception designed to address the specific and unusual features of IoT and the harms it produces. It serves as a reminder, too, that while we search for solutions that improve on control and consent, we can never abandon control and consent entirely.

B. *The Virtue of Rough Design*

Legacy switches might become little blemishes on the otherwise smooth uniformity that marks the prevailing aesthetic ideal of our day. People like Steve Jobs and Elon Musk have established in our culture the ideal of curvy, streamlined, seamless perfection.[259] A physical legacy switch is a pockmark of human values, a pimple of privacy, or a blemish of choice. It will drive some designers crazy to have to accede to this externally imposed ugliness, and it will remind consumers that these are not just the products of single minds. We like the way the struggle for the right to design might be revealed to the casual observer.

This connects, once again, to movements like the Right to Repair. Some modern devices are difficult to repair not only as a way for the manufacturers to capture repair revenue but because the seamless design aesthetic is easier to achieve if you can secure parts together with permanent glue instead of removable screws.[260] Easy-to-repair devices might tend to be a little larger,

---

[259] *See, e.g.*, Ryan Ayers, *Lessons from Apple on Why Aesthetic Innovation Is Important*, INNOVATION MGMT. (June 22, 2017), https://innovationmanagement.se/2017/06/22/lessons-from-apple-on-why-aesthetic-innovation-is-important/ [https://perma.cc/Z29Q-L3WL]; Matthew DeBord, *The Secret to How Tesla Gets Its Cars to Look Absolutely Fantastic*, BUS. INSIDER (Dec. 29, 2017), https://www.businessinsider.com/how-tesla-designs-cars-to-look-so-good-2017-11 [https://perma.cc/M2S6-PD4G]; Faiz Siddiqui, *Tesla Is Like an 'iPhone on Wheels.' And Consumers Are Locked into Its Ecosystem*, WASH. POST (May 14, 2021), https://www.washingtonpost.com/technology/2021/05/14/tesla-apple-tech/ [https://perma.cc/H9LF-6SWD] ("Like Apple, Tesla built its brand on exclusivity and aspirational products . . . . [B]oth companies have integrated software with hardware in a way that revolutionized their industries . . . .").

[260] *See* Thorin Klosowski, *The Framework Laptop Could Revolutionize Repairability. We Hope It Does*, N.Y. TIMES: WIRECUTTER (Oct. 13, 2021), https://www.nytimes.com/

heavier, and less sleek.[261] Some might view this as a regrettable side effect of repairability, but maybe we ought instead to embrace this as a badge of products that have been subjected to participatory design.

We also connect this also to a burgeoning movement called "The Maintainers."[262] Science and technology studies scholars Lee Vinsel and Andrew Russell argue that our society overvalues so-called "innovation" in the form of sleek-and-shiny products that are designed to fail after a few years.[263] As a counterweight, we should instead celebrate activities like maintenance, infrastructure, and repair.[264]

Lumpy, awkward legacy switches will remind consumers that design is a conversation, and that a product has been influenced by someone other than Silicon Valley masterminds.

C. *Modular Design for Legacy Switches*

We believe that a new governance agenda needs to highlight participatory design, breaking the monopoly manufacturers have in designing technical products and services. To embark in a new project of publicly influenced private design, we need to identify both micro-scale fixes like legacy switches but also the macro-scale design principles that are advanced by those fixes. An important principle advanced by legacy switches is the idea of modular design.

One way to create a legacy switch is to design a smart device in two halves: a "dumb" core that provides only the basic functionality of the device, attached to a "smart" half that controls the intelligent behaviors of the device. Engineers can create a simple, dumb version of their device, one which controls the core functionality of the thermostat, doorbell, or door lock. Separately, they can engineer a smart circuit that can control the dumb half using a pre-defined arrangement of wires and connectors that transmit specific electronic and electrical signals. The design of a system as discrete, separate parts that communicate with one another across a clearly delineated boundary is known as "modular design," with each part called a "module," and the control circuitry and logic called an "interface."[265] The technical literature abounds with descriptions of the benefits of modularity.[266] The Internet itself was designed

---

wirecutter/reviews/framework-laptop/ [https://perma.cc/74MW-8GAQ] (speculating that manufacturers use glue to allow for "impossibly thin-and-light" devices).

[261] *See id.*

[262] *About*, MAINTAINERS, https://themaintainers.org/about/ [https://perma.cc/Q85K-3XB6].

[263] *See* LEE VINSEL & ANDREW L. RUSSELL, THE INNOVATION DELUSION: HOW OUR OBSESSION WITH THE NEW HAS DISRUPTED THE WORK THAT MATTERS MOST 12–13, 141–42 (2020).

[264] *See id.* at 12–15.

[265] *See* Chun-Che Huang & Andrew Kusiak, *Modularity in Design of Products and Systems*, 28 INST. ELEC. & ELECS. ENG'RS 66, 66 (1998).

[266] *See, e.g.*, J.H. Saltzer, D.P. Reed & D.D. Clark, *End-to-End Arguments in System Design*, 2 ACM TRANSACTIONS ON COMPUT. SYS. 277, 278 (1984).

with modularity as a core precept, and some point to its modularity as a fundamental part of its success.[267]

Modular design can be implemented in different ways. Earlier, we described irreversible legacy switches that can be "flipped" by scratching wire traces off of a circuit board or snapping off half of a board. The two halves of such a board are modules in a modular design. Modular design can be implemented less destructively. Single-board computers allow for plug-in expansion boards, sometimes called expansion cards, daughterboards, or shields.[268] These circuit boards expand the functionality of the computer, communicating through a well-defined interface such as GPIO, PCI, or USB.[269] Regulators could mandate a plug-in design, in which all of the "smart" functionality is carried in a plug-in board, meaning the legacy functionality should reside on a single "main board," one that provides basic functionality when nothing is connected.

One important smart home product category has already been implemented in modular fashion: Smart TVs. Thanks to standards like HDMI, manufacturers such as Roku, Google, and Amazon manufacture small "dongles," little hockey-puck or USB-stick style devices designed to be plugged directly into a television to give it additional smart functionality.[270] When these devices reach their end-of-life, or when newer versions from the same manufacturer or a competitor introduce new desirable features, a consumer can unplug and upgrade this tiny and relatively smart device, while not needing to upgrade the bigger, more expensive components of the television screen.

Legal scholars have explored how modular design can advance public policy in addition to technical goals.[271] Some have written about the benefits of modular, technical systems such as network protocols to innovation and

---

[267] *See, e.g.*, JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 31, 41 (2008).

[268] *See* JUNE J. PARSONS ET AL., COMPUTER CONCEPTS & MICROSOFT OFFICE 365 & OFFICE 2016, at 38 (2016). *See generally* Mel Hawthorne, *What Is a Daughterboard*, TECHNIPAGES (Aug. 8, 2022), https://www.technipages.com/what-is-a-daughterboard?utm_source=rss&utm_medium=rss&utm_campaign=what-is-a-daughterboard [https://perma.cc/SAC2-BYLY].

[269] PARSONS, *supra* note 268, at 30.

[270] *See* Corey Gaskin, *Chromecast, Fire TV Stick, or Roku: What's the Best Streaming Stick for ~$50?*, ARS TECHNICA (Feb. 2, 2022), https://arstechnica.com/gadgets/2022/02/4k-streamer-showdown-chromecast-vs-amazon-fire-tv-stick-vs-roku-streaming-stick/ [https://perma.cc/T9CU-QQET].

[271] Some scholars have imported modular design beyond technology to the design of legal instruments, focusing for example on modular contracts, see generally Henry E. Smith, *Modularity in Contracts: Boilerplate and Information Flow*, 104 MICH. L. REV. 1175 (2006), property rules, Thomas W. Merrill, *Property as Modularity*, 125 HARV. L. REV. F. 151 (2012), and environmental regulation, and Jody Freeman & Daniel A. Farber, *Modular Environmental Regulation*, 54 DUKE L.J. 795 (2005).

competition.[272] Consider how IoT devices with a modular legacy switch can open up possibilities for competition, transparency, and regulation.

If the interface between an IoT device's two halves is published in full, it might give rise to competition, as other companies could supply their own smart module to replace the original. The market for add-on smart TV dongles is a great example. Companies could compete on privacy, selling daughterboards that allow for smart devices with less exfiltration of data and bans on using the data for marketing, as DuckDuckGo has tried to compete with Google on search engines or Mozilla has tried to compete on web browsers.[273] Other companies could target end-of-life devices, selling cheaper daughterboards that preserve a few small bells-and-whistles, adding features back to legacy state devices, coupled with that company's promise to support and update the devices.[274] We could even imagine a regime modeled on expired patents and generic drugs, in which companies are permitted a few years of sales without daughterboard competition, after which they must publish the full interface specification, unleashing a market for "generic" smarts.[275] In fact, we could imagine some manufacturers focusing on the "smart platform" market, marketing only a legacy-core device designed for others to extend in smart ways, publishing a well-designed public interface for competition in the add-on market. This might be an attractive and lucrative market segment for companies with a long tradition in building pre-IoT versions of these devices, such as Honeywell for thermostats or GE for smoke alarms.

Modular design will create a boundary between "smart" and "legacy," demarcating a literal and physical frontier of innovation. This will, in turn, create new opportunities for transparency and regulation, by both formal government agencies and informal consumer protection organizations. For example, the physical boundary of modular design produces a single point of transparency and observation. It requires engineers to run literal wires on a circuit board between the "thinking" and "doing" halves of the device.

---

[272] *See generally* Christopher S. Yoo, *Modularity Theory and Internet Regulation*, 2016 U. ILL. L. REV. 1; Joseph Farrell & Philip J. Weiser, *Modularity, Vertical Integration, and Open Access Policies: Towards a Convergence of Antitrust and Regulation in the Internet Age*, 17 HARV. J.L. & TECH 85 (2003).

[273] Matt Burgess, *Google Got Rich from Your Data. DuckDuckGo Is Fighting Back*, WIRED (Aug. 6, 2020), https://www.wired.co.uk/article/duckduckgo-android-choice-screen-search [https://perma.cc/524P-3XBH]; *Comparing Firefox Browser with Google Chrome*, MOZILLA, https://www.mozilla.org/en-US/firefox/browsers/compare/chrome/ [https://perma.cc/84A5-QGGL].

[274] On the other hand, the secondary market might exacerbate the problems, if third parties sell cheap and poorly support "smart" alternatives that raise their own security and privacy problems.

[275] *Cf.* Linda Gorman, *Patent Expiration and Pharmaceutical Prices*, NAT'L BUREAU OF ECON. RSCH. (Sept. 2014), https://www.nber.org/digest/sep14/patent-expiration-and-pharmaceutical-prices [https://perma.cc/3XZF-5N6W] ("When a drug's U.S. patent expires, manufacturers other than the initial developer may take advantage of an abbreviated approval process to introduce lower-priced generic versions.").

Government auditors or nonprofit consumer testing labs can probe and test those wires to observe stimuli-reaction relationships. The modules on either side of the interface may be black boxes, but the interface will reveal otherwise hidden or obfuscated functionality, conduct, design, and intent. A testing lab will not need to reverse-engineer what is happening inside the "smart" black box if it could simply verify that nothing is flowing from the dumb side (where all the sensors live) to the smart side (where data processing and exfiltration occurs). This would give the auditors access to details about what a device is doing that would be otherwise very difficult or impossible to probe in an integrated smart/dumb circuit board.

Given the significant advantages for competition and transparency afforded by modular design, we might mandate modularity for some legacy switches.

VI. CONCLUSION

Legacy switches will allow consumers to build and maintain the smart homes of their dreams on their own terms. A consumer can choose which of their smart home devices to replace rather than render dumb—say their smart televisions and smart speakers—while flipping the switches on other devices—such as their doorbells and thermostats. Each can walk the innovation path best suited to their individual preferences, resources, and circumstances.

Smart home device manufacturers might even welcome legacy switch requirements, as legacy switches may liberate them from needing to continue supporting devices that are decades old. Legacy switches will also provide an alternative path to costly recalls after vulnerabilities are found, perhaps decreasing the cost of responding to future lawsuits or safety commission investigations. They might increase the attractiveness of corporate acquisitions, allowing the acquirer to buy a IoT company's personnel and intellectual property without necessarily needing to shoulder the support obligations for the entire installed base.[276]

Finally, creating and administering a legacy switch requirement will help legislatures and government agencies embrace a different, more involved, and more proactive approach to governing technology companies than they have adopted in the past. They need more often to see themselves as co-designers, along with the tech companies, of the devices and services that both enrich our lives and create new risks of harm. A society in which "they design, we react" has led to social networks full of misinformation, toxic services full of misogyny and hate, generations of people addicted to their smartphones, and cratering democratic institutions. Our thirty-year experiment in letting Silicon Valley design alone has failed, and we need to reconceptualize who gets to participate in design.

---

[276] *See* David Gewirtz, *Revolv Is Dead. Google Killed It. Long Live Innovation*, ZDNET (June 20, 2016), https://www.zdnet.com/article/revolv-is-dead-google-killed-it-long-live-innovation/ [https://perma.cc/HLF9-PZ8U].