2016

The Internet of Heirlooms and Disposable Things

Woodrow Hartzog
Boston University School of Law

Evan Selinger

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 17, ISSUE 4: MAY 2016

THE INTERNET OF HEIRLOOMS AND DISPOSABLE THINGS

Woodrow Hartzog*
Evan Selinger**

The Internet of Things ("IoT") is here, and we seem to be going all in. We are trying to put a microchip in nearly every object that is not nailed down and even a few that are. Soon, your cars, toasters, toys, and even your underwear will be wired up to make your lives better. The general thought seems to be that "Internet connectivity makes good objects great." While the IoT might be incredibly useful, we should proceed carefully. Objects are not necessarily better simply because they are connected to the Internet. Often, the Internet can make objects worse and users worse-off. Digital technologies can be hacked. Each new camera, microphone, and sensor adds another vector for attack and another point of surveillance in our everyday lives. The problem is that privacy and data security law have failed to recognize some "things" are more dangerous than others as part of the IoT. Some objects, like coffee pots and dolls, can last long after the standard life-cycle of software. Meanwhile cheap, disposable objects, like baby wipes, might not be worth outfitting with the most secure hardware and software. Yet they all are part of the network. This essay argues that the nature of the "thing" in the IoT should play a more prominent role in privacy and data security law. The decision to wire up an object should be coupled with responsibilities to make sure its users are protected. Only then, can we trust the Internet of Heirlooms and Disposable Things.

---

* Associate Professor, Samford University's Cumberland School of Law; Affiliate Scholar, Stanford Center for Internet and Society.

** Professor of Philosophy, Rochester Institute of Technology. The authors would like to thank Anne Klinefelter and Joe Kennedy. The authors would like to thank Anne Klinefelter, Sue Glueck, and Joe Kennedy and the participants of the North Carolina Journal of Law and Technology's Symposium: Privacy of the Home and the Internet of Things and the staff of the North Carolina Journal of Law and Technology.

I. INTRODUCTION

We have become drunk on our ability to connect anything to the Internet. Barbie dolls, baby monitors, coffee pots, refrigerators, clothes, watches, and cars—we have connected it all. It seems there is nothing we cannot improve by sticking a chip in it.

If you want a sense of just how mad we've become, look at the Twitter account "Internet of Shit" (@internetofshit), which satirizes what has come to be known as the "Internet of Things" ("IoT").[1] This account is a parade of dubious decisions to take an object, any object, and put a chip in it. Light switches, cooking pans, stuffed animals, basketballs, headbands, water bottles, rectal thermometers, and more are now all connected to the Internet and our mobile devices.[2] Japanese security researchers have already

[1] Internet of Shit, TWITTER, https://mobile.twitter.com/internetofshit (last visited April 17, 2016).

[2] *See, e.g.*, Internet of Shit, TWITTER, https://twitter.com/internetofshit/status/694526620795867136 (last visited Apr. 17, 2016); *Seed- The Smart Bottle That Never Forgets About You*, INDIEGOGO, https://www.indiegogo.com/projects/seed-the-smart-bottle-that-never-forgets-about-you#/; Cory Doctorow, *The Internet of Things In your Butt: Smart Rectal Thermometer*, BOINGBOING (Jan. 14, 2016), http://boingboing.net/2016/01/14/the-internet-of-things-in-your.html; Arielle Duhaime-Ross, *This Headband Analyzes Your Sweat to Improve Your Workout*, THE VERGE (Jan. 27, 2016), http://www.theverge.com/2016/1/27/10840680/sweat-wearable-analysis-real-time-berkeley.

hacked an IoToilet, giving them the ability to flush and squirt water at people. A literal "Internet of Shit."[3]

Of course, the IoT can be quite useful. Many devices are improved upon when they are connected. Automated cars could save millions of lives. Wearable technologies could detect health problems long before symptoms manifest. Toys connected to the Internet can be educational and therapeutic. Everyday technologies like TVs and books that are connected to the Internet can be configured to aid those living with disabilities. The IoT can make all of our lives easier and more pleasant. Of course, schlocky products might seem ridiculous. But consumer preferences vary and markets accommodate all kinds of tastes. They are not restricted to offering necessary items and well-made goods.

The problem is that we are not taking the decision to wire up an artifact to the Internet seriously enough. A chip-centric mentality has taken over—one that is guided by an overly simplistic principle: "Internet connectivity makes good objects great." Guided by this upgrade mentality, we seem to be in a rush to connect everything. Meanwhile seemingly none of us, including policy makers and regulators, have fully appreciated the significance of companies transforming from artifact and device "makers" to "service providers."

The digital transition should give us deep pause for thought. Objects are not necessarily better simply because they are connected to the Internet. Often, the Internet can make objects worse and users worse off. IoT objects only fulfill their designed purposes when their software works. But software that works today can crash tomorrow. Software needs upgrades to fix problems. Connectivity allows for regular updates. But it also provides an

---

[3] *See, e.g.*, Jasper Hamill, *Hackers take control of a Toilet using bog-standard computer skills*, MIRROR (Feb. 10, 2016) http://www.mirror.co.uk/tech/hackers-take-control-toilet-using-7342662. Wired magazine hosted sponsored content titled *The Toilet and Its Role in the Internet of Things*. Giles Crouch, *The Toilet and Its Role in the Internet of Things*, WIRED (Apr. 2014), http://www.wired.com/insights/2014/04/toilet-role-internet-things/.

attack vector for hackers and allows companies to render your IoT object inoperable whenever it likes. Consider how Google plans to shut down its Revolv hub designed to control lights, alarms, and doors.[4]

More fundamentally, the IoT requires adaptive design that thoughtfully attends to key features, including user functionality, security, and privacy. While the Federal Trade Commission ("FTC") requires reasonable data security from those collecting personal information, it has yet to grapple with all of these nuances and the systemic reasons why the IoT adds a host of vulnerabilities to our lives.[5]

Some IoT companies like VTech are washing their hands of responsibility. The company's IoT kids toys were hacked, leading to a massive data spill on Shodan (the search engine for the Internet of Things).[6] VTech's embarrassing data breach exposed personal data on 6 million children.[7]

---

[4] *Revolv Devices Bricked as Google's Nest Shuts Down Smart Home Company*, THE GUARDIAN, (Apr. 5, 2016), https://www.theguardian.com/technology/2016/apr/05/revolv-devices-bricked-google-nest-smart-home ("Against that background, losing customer trust could be a damaging move," Gilbert said. "I'm genuinely worried though. This move by Google opens up an entire host of concerns about other Google hardware. Which hardware will Google choose to intentionally brick next? . . . Is your Nexus device safe? What about your Nest fire/smoke alarm? What about your Dropcam? What about your Chromecast device? Will Google/Nest endanger your family at some point?").

[5] *See, e.g.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014); Brian Krebs, *IoT Reality: Smart Devices, Dumb Defaults*, KREBS ON SECURITY (Feb. 18, 2016), http://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/ [hereinafter Krebs, *Smart Devices, Dumb Defaults*].

[6] *See, e.g.*, *Lack of Database and Password Security Leaves Millions of Users Exposed*, DUO (Dec. 15, 2015), https://duo.com/blog/lack-of-database-and-password-security-leaves-millions-of-users-exposed; J.M. Porup, *'Internet of Things' Security is Hilariously Broken and Getting Worse*, ARS TECHNICA (Jan. 23, 2016), http://arstechnica.com/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/.

[7] Lorenzo Franceschi-Bicchierai, *Hacked Toy Company Vtech's TOS Now Says It's Not Liable for Hacks*, VICE (Feb. 9, 2016), http://motherboard.vice.com/read/hacked-toy-company-vtech-tos-now-says-its-not-liable-for-hacks.

In its Terms and Conditions for its software, VTech now includes the following ominous language in all-caps: "YOU ACKNOWLEDGE AND AGREE THAT ANY INFORMATION YOU SEND OR RECEIVE DURING YOUR USE OF THE SITE MAY NOT BE SECURE AND MAY BE INTERCEPTED OR LATER ACQUIRED BY UNAUTHORIZED PARTIES."[8] This reads more like fodder for a Saturday Night Live sketch than what we would expect out of a reasonable Terms of Use agreement.

Even when companies intend to keep their products safe and secure over the course of their use, the fact remains that they might not be around to see their commitment through.[9] "Here today, gone tomorrow" might as well be the epigram of Silicon Valley where the spirit of disruption drives innovation more than the ethos of sustainability.

Simply put, what's to stop a whole bunch of well-intentioned companies from producing IoT products that sell moderately or even poorly, but fail to be sufficiently profitable to prevent them from going out of business shortly after their goods hit the shelves? If that happens, they likely will not have the resources to provide further security work. And yet, if the products remain functional past the point of being serviced, consumers either must stop using them or take personal responsibility for security breaches via the "buyer beware" mentality. This makes many IoT objects more costly and risky than their "dumb" counterparts.

---

[8] *Id.*

[9] *See, e.g.*, Yash Kotak, *5 Reasons Why My IoT Startup Failed*, VENTUREBEAT (June 16, 2015), http://venturebeat.com/2015/06/16/5-reasons-why-my-iot-startup-failed/; Nat Garlin, *Quirky Files for Bankruptcy, Will Likely Sell its IoT Company Wink in the Next 60 Days*, THE NEXT WEB (Sept. 22, 2015), http://thenextweb.com/insider/2015/09/22/quirky-bankruptcy/.

II. "THINGS" ARE DIFFERENT AND MORE DANGEROUS THAN COMPUTERS

The IoT is rife with privacy and security problems.[10] But our debate has, up to this point, been focused more on the "Internet" part of the IoT rather than the "Things" that are connected. Our laws and rhetoric have failed to scrutinize the differing nature of "things," as if they all pose the same risks as computers and standard information technologies. But this is simply not true. Artifacts differ from computers and each other. The nature of an artifact and its design will influence a range of outcomes, including how we use it, where we put it, how much attention we pay to it, and how long we will keep it. In turn, these variables impact the extent to which vulnerabilities are created and persist.

Wiring a computer up to the Internet is not the same thing as wiring up an object that has non-processing uses like a doll or refrigerator. Computers that cannot connect to the Internet are of limited value in the age of cloud computing. The same cannot be said for the IoT, where Internet connectivity is often not essential to an object's core function. Dolls can be played with, clothes and diapers can be worn, coffee pots can still heat, and refrigerators can cool all without WiFi.

Some of these objects are likely to be used long after the vendor stops servicing them with critical security updates, known as "patches."[11] By contrast, objects like IoT diapers and shampoo bottles are meant to be quickly used and disposed of. These small, disposable objects are hard to service because of their limited bandwidth and storage capacities.[12] It is often too costly to invest in security for these disposable objects. Yet they remain persistent

---

[10] *See, e.g.*, Scott Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85 (2014).

[11] Institution Systems & Tech., *Why Patch?* MASS. INST. OF TECH., https://ist.mit.edu/security/patches (last visited Apr. 13, 2016).

[12] Parc Lawrence Lee, *How the 'Internet of Everyday Things' Could Turn Any Product into a Service*, VENTURE BEAT (Feb. 7, 2015), http://venturebeat.com/2015/02/07/how-the-internet-of-everyday-things-could-turn-any-product-into-a-service/.

risks in our home networks.[13] Security researcher Brian Krebs notes that poorly configured default settings for IoT devices are a security nightmare.[14] This is particularly true for devices that are costly to change, like many disposable and cheap IoT devices.

Some companies are even developing products like thin, adhesive films that will turn *any* object into an IoT artifact.[15] This

---

[13] *See, e.g.*, Krebs, *Smart Devices, Dumb Defaults*, *supra* note 5; Brian Krebs, *This is Why People Fear the 'Internet of Things*,*'* KREBS ON SECURITY (Feb. 18, 2016), https://krebsonsecurity.com/2016/02/this-is-why-people-fear-the-internet-of-things/; Kashmir Hill, *Article May Scare You Away from Internet of Things*, FORBES (May 27, 2016) [hereinafter Krebs, *This is Why People Fear the 'Internet of Things'*] http://www.forbes.com/sites/kashmirhill/2014/05/27/article-may-scare-you-away-from-internet-of-things/#3e6ec4ab23dd ("The reason why [Internet of Things] vendors are not doing security better is that it's cheaper not to do it. It's expensive to build security in. The shopper in Best Buy will buy the camera for $40 not the one that's $100. She doesn't know or care about the security. There will be more and more hacks, not just of cameras but of lots of things. Eventually it will make people care, and it will be more expensive to be insecure than secure.").

[14] *See, e.g.*, Brian Krebs, *The Lingering Mess from Default Insecurity*, KREBS ON SECURITY (Nov. 12, 2015), http://krebsonsecurity.com/2015/11/the-lingering-mess-from-default-insecurity/ ("As the Internet of Things grows, we can scarcely afford a massive glut of things that are insecure-by-design. One reason is that this stuff has far too long a half-life, and it will remain in our Internet's land and streams for many years to come . . . . Mass-deployed, insecure-by-default devices are difficult and expensive to clean up and/or harden for security, and the costs of that vulnerability are felt across the Internet and around the globe."); Krebs, *This is Why People Fear the 'Internet of Things'*, *supra* note 13.

[15] Rakesh Sharma, *A New Perspective On The Internet Of Things*, FORBES (Feb. 18, 2014), http://www.forbes.com/sites/rakeshsharma/2014/02/18/a-new-perspective-on-the-internet-of-things/#53652d3d267c ("As an example, Sutija points to Blue Tooth, which has low power requirements and transmits information over short distances. '(Using this approach) you can distribute intelligence broadly over a large number of simple devices (or, devices that are not IoT ready)' he says. Instead of big data, which relies on constant monitoring, such devices use small data or snippets of information at specific periods of time. For example, consumers can measure their vitals through temporary monitoring tests that use disposable electronics instead of conventional electronics. 'We want to add intelligence to ordinary objects that are also disposable,' says Sutija.").

might be the quickest way to scale the IoT in our homes. But every new IoT connection brings new risks. For example, it might take people a while to treat everyday objects with the same care they give to their computers. Until we change our mindsets, our daily routines will not include updating our coffee maker's operating system.

Krebs asserts that "[b]efore purchasing an 'Internet of things' (IoT) device . . . consider whether you can realistically care for and feed the security needs of yet another IoT thing."[16] According to Krebs, "there is a good chance your newly adopted IoT puppy will be chewing holes in your network defenses; gnawing open new critical security weaknesses; bred by a vendor that seldom and belatedly patches; [and] tough to wrangle down and patch."[17] Krebs quotes Craig Williams, the security outreach manager at Cisco, who has said:

> Compromising IoT devices allow unfettered access though the network to any other devices on the network . . . .To make matters worse almost no one has access to [an IoT's operating system] to notice that it has been compromised. No one wakes up and thinks, "Hey, it's time to update my thermostats [sic] firmware."[18]

This means that the Internet of Heirlooms and Disposable Things will stay likely stay compromised, giving hackers an ideal opening to laterally move through our networks.[19]

Bad defaults on IoT devices are common and most users cannot easily patch them. The process is usually complicated.[20]

What's worse is that the updating process for the IoT does not scale well. The typical lifetime of software is around 2 years. [21] But the estimated lifetime of some objects now connected to the

---

[16] Krebs, *This is Why People Fear the 'Internet of Things'*, *supra* note 13.
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] Krebs, *This is Why People Fear the 'Internet of Things'*, *supra* note 13.

Internet is often around 10 years.[22] Just think about how long coffee pots and refrigerators last. The "Internet of Things We Keep a Long Time" is a security nightmare.

Yet with few important exceptions,[23] the law has been largely agnostic regarding the decision to wire-up an artifact. The law is caught up in an information-centric approach to the regulation of data security. It abstracts away too many of the significant features of materiality—the very tangibility of things.[24] Companies are required to provide reasonable privacy and data security for the information they collect. But there is very little regulatory compliance cost for merely connecting artifacts to the Internet. This article suggests that there should be.

For example, the law might require more systemic consideration from IoT companies of the intended use and expected lifecycle of their artifacts. It could require companies provide appropriate protection for users that directly takes an object's lifecycle into account—an option we develop in greater detail below. Ultimately, a more measured approach to the IoT, such as this article is proposing, will help ensure the development and sale of safer technologies. It would alleviate some of the risk of harm faced by IoT users—users who have little knowledge of and ability to respond to the risks presented by the Internet of Heirlooms and Disposable Things.

---

[22] *Id.*

[23] *ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk,* FEDERAL TRADE COMMISSION (Feb. 23, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put; *FTC Approves Final Order Settling Charges Against TRENDnet, Inc.,* FEDERAL TRADE COMMISSION (Feb. 7, 2014), https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc.

[24] James Grimmelmann, *Privacy As Product Safety*, 19 WIDENER L.J. 793, 816 (2010) ("[T]he database-centric Fair Information Practice approach has been the basis for most of the information privacy law the United States actually has.").

III. MAYBE YOUR UNDERWEAR DOES NOT NEED TO BE CONNECTED TO THE INTERNET

"Vibrundies" are exactly what they sound like.[25] Not even your underwear is safe from the IoT. The website for the wearable tech states, "Using vibrations from our special undies power pack, Vibrundies monitors Twitter for brand mentions and shout-outs-giving you a very special feeling each time one hits . . . . [W]hen you can't look at your phone, there's a better way to feel the buzz of your social activity[.]"[26]

This is just one of the many kinds of things that you might be surprised are part of the IoT. They are all making us vulnerable. One general problem associated with the IoT is that it can be buggy, leaving us with inoperable or dysfunctional objects.[27] Because the IoT relies upon software and hardware, it is more complex than most non-digital technologies. The more moving parts a device has, the more that can go wrong. For example, a smart television apparently malfunctioned when it broadcast hardcore pornography during a funeral service for a father and his young son at a crematorium in Wales.[28]

The IoT has systemic problems surrounding the collection and use of personal information. Professor Scott Peppet has identified four major informational problems with the IoT: 1) discrimination, 2) privacy, 3) security, and 4) consent.[29] All four of these issues should give companies and lawmakers pause regarding the decision to wire up an artifact.

---

[25] VIBRUNDIES, http://www.vibrundies.com/ (last visited Apr. 5, 2016).

[26] *Id.*

[27] Lorenzo Franceschi-Bicchierai, *Smart Fridge Only Capable of Displaying Buggy Future of the Internet of Things,* MOTHERBOARD (Dec. 11, 2015, 11:33 AM), http://motherboard.vice.com/read/smart-fridge-only-capable-of-displaying-buggy-future-of-the-internet-of-things.

[28] Harry Yorke, *Grieving Family's Horror as Hardcore Pornography Played at Funeral for Father and Baby Son*, WALES ONLINE (Jan. 27, 2016, 6:55 PM), http://www.walesonline.co.uk/news/wales-news/grieving-familys-horror-hardcore-pornography-10797800.

[29] Scott Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent*, 93 TEX. L. REV. 85 (2014).

Regarding privacy, Peppet argues that sensor data are particularly hard to de-identify.[30] Consent to collecting and using information is also a true quagmire for the IoT.[31] Where exactly do you put the privacy policy for IoT underwear and IoToilets? The IoT is one of the most intimate technological movements ever, yet the mechanism for privacy permissions has never been more dysfunctional.

And the full version of the IoT is just getting warmed up. The "innovation at all costs" mantra of Silicon Valley repelled most meaningful privacy laws over the last twenty years, allowing the Internet surveillance economy to flourish. The surveillance tech industry is incredibly powerful. It has been quite helpful in limiting what technology is allowed to do and say about us when we're not looking.[32]

Consider, for example, the problem of cross-device tracking. SilverPush is an Indian startup company invested in identifying all your computing devices.[33] Schneier notes that, SilverPush uses inaudible sounds it embeds in webpages and television commercials to transmit that personal information back to SilverPush through the use of cookies.[34] This technique allows the company to track you across all your various devices. According to Schneier, SilverPush can associate the television commercials you watch with your web searches.[35] It can correlate your tablet activities with what you do on your computer.[36] Privacy and security research Bruce Schneier emphasizes, "Your computerized things are talking about you behind your back, and for the most

---

[30] *Id.*

[31] *Id.*

[32] Bruce Schneier, *The Internet of Things that Talk About You Behind Your Back*, SCHNEIER.COM (Jan. 16, 2016), https://www.schneier.com/blog/archives/2016/01/the_internet_of.html.

[33] *FTC Issues Warning Letters to App Developers Using 'Silverpush' Code,* FEDERAL TRADE COMMISSION (Mar. 17, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code.

[34] *Id.*

[35] *Id.*

[36] *Id.*

part you can't stop them -- or even learn what they're saying."[37] The FTC has already stated that consumers should be told about such technologies and practices.[38]

Then there's the billion-dollar IoT problem mentioned above: data security. Successful hacks on Internet of Things devices are legion. VTech and Fisher Price have been hacked.[39] Researchers discovered that an IoT doorbell was revealing users' WiFi keys.[40] Security flaws have been demonstrated in IoT Barbie Dolls, Samsung Refrigerators, Jeep Cherokees, and a WiFi enabled TrackingPoint sniper rifle (allowing for hackers to choose their own targets).[41] A GPS child tracker had a flaw that would let hackers act as a child's parents.[42] Andy Greenberg and Kim Zetter dubbed 2015 as "[t]he year of insecure internet things."[43] According to Cisco, there are more objects connected to the Internet than people.[44] Every new IoT device provides more attack surface for hackers.[45] Hewlett Packard recently estimated that 70

---

[37] *Id.*

[38] *Id.*

[39] Samuel Gibbs, *Toy Firm VTech Hack Exposes Private Data of Parents and Children,* THE GUARDIAN (Nov. 20, 2015), http://www.theguardian.com/technology/2015/nov/30/vtech-toys-hack-private-data-parents-children.

[40] John Leyden, *One Ring to Own them all: IoT Doorbell Can Reveal your Wi-Fi Key,* THE REGISTER (Jan. 12, 2016), http://www.theregister.co.uk/2016/01/12/ring_doorbell_reveals_wifi_credentials/.

[41] Andy Greenberg & Kim Zetter, *How the Internet of Things Got Hacked,* WIRED (Dec. 28, 2015), http://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/.

[42] Lorenzo Franceschi-Bicchierai, *A GPS Tracker for Kids Had a Bug That Would Let Hackers Stalk Them,* MOTHERBOARD (Feb. 2, 2016), http://motherboard.vice.com/read/a-gps-tracker-for-kids-had-a-bug-that-would-let-hackers-stalk-them.

[43] GREENBERG & ZETTER, *supra* note 41.

[44] Dave Evans, *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, CISCO (April 2011), http://share.cisco.com/internet-of-things.html.

[45] Omner Barajas, *How the Internet of Things (IoT) Is Changing the Cybersecurity Landscape*, SECURITY INTELLIGENCE (Sept. 17, 2014), https://securityintelligence.com/how-the-internet-of-things-iot-is-changing-the-cybersecurity-landscape/ (citing Evans, *supra* note 44); Daniel Miessler, *HP Study*

percent of IoT devices have serious security vulnerabilities.[46] Simply put, we have yet to figure out a way to keep the security of the IoT up to speed with the demand for IoT products.

Government intelligence and law enforcement services are also quite excited about the Internet of Things. IoT gives law enforcement another path to surveillance. And they are not shy about their intentions to exploit that sensor in your underwear or doll. For example, Director of U.S. National Intelligence James Clapper recently told a Senate panel as part of his annual "assessment of threats" against the U.S. that "[i]n the future, intelligence services might use the [internet of things] for identification, surveillance, monitoring, location tracking, and targetingfor recruitment, or to gain access to networks or user credentials."[47] Trevor Timm, a columnist for *The Guardian* and executive director of the Freedom of the Press Foundation, noted Clapper's testimony actually supports the claim by many that the FBI's recent claim that they are "going dark," or losing the ability to surveil suspects because of encryption, are largely overblown. There are more avenues for surveillance now than ever before.

This is why the design of our technologies matters. Companies' design decisions will impact the extent to which law enforcement and surveillance agencies can access your personal information. For example, Microsoft stores the full-disk version of the encryption key to Windows 10 in the cloud, providing it the ability to decrypt upon receiving a government demand for data.[48] Apple

---

Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack, HEWLETT PACKARD ENTERPRISE (July 29, 2014, 5:09 AM), http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.U_NUL4BdU00.

[46] *Id.*

[47] Trevor Timm, *The Government Just Admitted it Will Use Smart Home Devices for Spying*, THE GUARDIAN (Feb. 9, 2016, 3:29 PM), http://www.theguardian.com/commentisfree/2016/feb/09/internet-of-things-smart-devices-spying-surveillance-us-government.

[48] *Microsoft Stores Windows 10 Encryption Keys in the Cloud,* SECURITYWEEK (Dec. 30, 2015), http://www.securityweek.com/microsoft-stores-windows-10-encryption-keys-cloud.

has resisted the FBI's request to cripple its failsafe protective device on iPhones, which permanently encrypts data on the phone after a limited number of failed login attempts.[49] If we care about our privacy and the security of our personal information, we should care about the design and proliferation of the Internet of Things as unique and trusted parts of our daily lives.

IV. POSSIBLE LEGAL SOLUTIONS

We have argued that the law should better recognize the nature of "things" in the IoT. The good news is that the law recognizes that privacy and data security are context dependent.[50] Most data security rules require a broad, "reasonable," approach.[51] This makes most data security law nimble and adaptive to problems like those presented by the IoT. Courts and lawmakers can start by digging deeper.

Depending on the problem to be solved and how severe it is, lawmakers could take a soft, moderate, or robust approach. The soft approach would leverage concepts of notice and education efforts for both industry and users. For example, the government might help leverage efforts by organizations like "I Am The Cavalry" to implement best practices among companies and provide notice to users of the strength of privacy and data security design for the IoT.[52] I Am The Cavalry is a group of concerned

---

[49] *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/

[50] *Start with Security: A Guide for Business,* FEDERAL TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Apr. 5, 2016).

[51] *See, e.g.,* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230 (2015); Kristina Rozen, *How Do Industry Standards for Data Security Match Up with the FTC's Implied "Reasonable" Standards—And What Might This Mean for Liability Avoidance?*, IAPP (Nov. 25, 2014), https://iapp.org/news/a/how-do-industry-standards-for-data-security-match-up-with-the-ftcs-implied-reasonable-standards-and-what-might-this-mean-for-liability-avoidance.

[52] *About,* I AM THE CAVALRY, https://www.iamthecavalry.org/about/overview/ (last visited Apr. 5, 2016) ("The Cavalry is a grassroots organization

security researchers focused on critical infrastructure.[53] This group is working on a five-star rating system for consumer-facing IoT devices. The rating system will give consumers the "quick ability to check device security without having to understand the technical details."[54]

I Am The Cavalry has tentatively developed a set of criteria by which it will evaluate IoT products, which includes categories like "secure by default," "secure by design," "self-contained security" and "privacy."[55] Soft efforts would also help facilitate the

---

that is focused on issues where computer security intersect public safety and human life. The areas of focus for The Cavalry are medical devices, automobiles, home electronics and public infrastructure.").

[53] I AM THE CAVALRY, https://www.iamthecavalry.org/ (last visited Apr. 5, 2016).

[54] Porup, *supra* note 6.

[55] *Id*. The entire checklist is a good summary of sound design for the IoT:

Security

1. Secure by Default

a. No default passwords shared between devices, or weak out of the box passwords.

b. All passwords should be randomly created using high quality random number generators.

c. Advanced features used by small percentage of users should be turned off (VPN, Remote Administration, etc.).

2. Secure by Design

a. Firmware should be locked down so serial access is not available.

b. Secure Element (SE) or Trusted Protection Modules (TPM) devices should be used to protect access to the firmware and hardware.

c. All GPIO, UART, and JTAG interfaces on the hardware should be disabled for production versions.

d. NAND or other memory/storage mediums should be protected with epoxy, ball sockets (so the memory cannot be removed and dumped), or other methods to prevent physical attacks.

3. Self-contained security

a. The devices should not rely on the network to provide security. Rather, the device's security model should assume the network is compromised and still maintain protection methods. This can be done with prompts to the users to accept handshakes between devices trying to access other devices on their networks.

identification and reporting of security vulnerabilities and bugs. This might include backing away from the support for "digital rights management" ("DRM"),[56] in which presents security problems for the Internet of Things. DRM itself can be insecure, laws that protect DRM can hinder sound security research, and DRM limits your ability to protect your own devices.[57] Consider the Electronic Frontier Foundation's proposal to have the World Wide Web Consortium ("W3C"), the nonprofit body that maintains the Web's core standards, adopt rules that would minimize the risk of security researchers reporting bugs on DRM-protected software.[58] Perhaps the government could help facilitate some kind of market for servicing "walking dead" IoT devices, which are still in use years after the patches stop.

The moderate approach would involve data security mandates to embrace the nature of the object in how much data security will be provided. Generally speaking, most data security laws in the United States require "reasonable data security." For example, the FTC generally prohibits unreasonable data security practices "in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of

---

b. Communication between devices should be encrypted to prevent MitM attacks and sniffing/snooping.

Privacy

1. Consumer PII not shared with manufacturers or partners
2. Usage data on individual consumer is never shared with partners or advertisers.
3. Anonymous data for buckets of users on usage patterns is acceptable as long as it's proven to not be traceable back to the individual consumers.
4. Data collection policy, type of data collected and usage of data is clearly documented on site.

[56] Julia Layton, *How Digital Rights Management Works*, HOWSTUFFWORKS (Jan. 3, 2006), http://computer.howstuffworks.com/drm1.htm (explaining what a DRM is).

[57] Chris Hoffman, *Is DRM a Threat to Computer Security?*, MAKEUSEOF (June 12, 2014), http://www.makeuseof.com/tag/drm-threat-computer-security/.

[58] Cory Doctorow, *You Can't Destroy the Village to Save It: W3C vs DRM, Round Two*, ELECTRONIC FRONTIER FOUNDATION (Jan. 12, 2016), https://www.eff.org/deeplinks/2016/01/you-cant-destroy-village-save-it-w3c-vs-drm-round-two.

available tools to improve security and reduce vulnerabilities."[59] Almost ten states require reasonable data security practices, rather than a specific list of prohibited or mandatory actions.[60] Congress has also explicitly embraced a reasonableness approach to data security. The Fair Credit Reporting Act ("FCRA"),[61] the Health Insurance Portability and Accountability Act ("HIPAA"),[62] and the Gramm-Leach-Bliley Act ("GLBA")[63] all use reasonableness as a touchstone for determining the adequacy of data security measures.

The reasonableness standard is not perfect, but it is flexible and can account for new problems like those presented by the IoT. Lawmakers and courts might interpret "reasonable security" to include some minimum expectation for servicing IoT devices and a floor of data security for even disposable items. Imagine a system where companies told users how long they think a wired object will last and how long the company will commit to providing security patches. In the event that a company goes bankrupt before then, companies would work quickly to either notify users of its impending shut down or facilitate the responsibility for security patches to a third party. This would help us avoid the problem of "zombie" IoT devices.

A robust response, which should be judiciously deployed, might include liability for harms facilitated by poor data security or privacy design. It might also include a specific regulatory regime akin to the Food and Drug Administration's regulation of medical devices.[64] Robust regimes like this would be costly, given the

---

[59] *Commission Statement Marking the FTC's 50th Data Security Settlement,* FEDERAL TRADE COMMISSION (January 31, 2014), http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

[60] *See* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2246 n. 80-83 (2015), *available at* http://ssrn.com/abstract=2461096.

[61] 16 C.F.R. § 682.3(a) (2012).

[62] 45 C.F.R. §§ 164.308 –164.314 (2012).

[63] 16 C.F.R. §§ 314.3–314.4 (2012).

[64] *Overview of Device Regulation,* U.S. FOOD & DRUG ADMIN., http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ (last updated Aug. 14, 2015).

widespread availability and diversity of IoT devices. Legislators might create mandate specific service times based on lifecycles, rather than just lumping such obligations into the requirement to provide "reasonable data security." Although specific, timetables in the world of data security risk being both under- and over-inclusive in different contexts.

In short, the law should take the IoT more seriously, without pushing the courts and lawmakers to act too hastily. Law should build upon industry wisdom regarding data security and leverage existing legal mechanisms like notice, insurance, and flexible requirements to avoid creating an unreasonable risk of harm to people.

Regardless of which legal response is selected, industry should act to work with regulators to ensure that the IoT is safe and sustainable. In addition to helping clearly notify users of the downsides to wiring-up an artifact, it could also design its products (where possible) to become "dumb" once the security patches stop. Imagine certain products like dolls, coffee makers, refrigerators, and basketballs that do not need the Internet to function built with a connectivity "kill switch." Companies could design products so that when users decide they have had enough, the chip or antenna could easily be removed or a built-in switch could disable all of the object's network functionality. This sort of "severability" option would help people easily take risky devices out of circulation and far away from their networks while still making use of the object.

This short essay has argued that merely connecting something to the Internet does not automatically make it a better product. The calculus for whether it is a good idea to wire up an object is much more complicated than that. Sometimes Internet connectivity makes us more vulnerable for only minimal gain. One way to mitigate this problem is for people, lawmakers, and industry to be more conscientious about the nature of the object that is being connected. The Internet of Things can be revolutionary, but it needs nuanced boundaries to be safe and sustainable. If the Internet of Things ends up being too dangerous, people will probably just stick to their old, non-connected underwear.