2019

Freedom to Hack

Ido Kilovaty

FREEDOM TO HACK

Ido Kilovaty[1]

Abstract

The proliferation of Internet-connected smart devices (the "Internet of Things") has become a major threat to privacy, user security, Internet security, and even national security. These threats are manifestations of externalities primarily resulting from a market failure in the Internet of Things industry, in which vendors do not have an incentive to implement reasonable security in the software embedded in devices they produce, thus creating cheap and unsecure devices. This Article argues that law and policy have a central role to play in making this digital ecosystem more secure – not only through direct regulation of this industry, but primarily through allowing individual security researchers to hack for security – or "ethical hacking." At present, laws that prohibit hacking, such as the Computer Fraud and Abuse Act and the Digital Millennium Copyright Act, are adopting a strict liability approach to hacking, which criminalizes almost any form of hacking, regardless of motivation or potential benefits. This Article rejects this outdated approach in the wake of ubiquitous cyber-attacks, imperfect software, and the emerging Internet of Things ecosystem.

This Article argues that law and regulatory agencies should accommodate hacking for security purposes to allow security researchers to discover possible vulnerabilities while shielding them from copyright infringement or criminal liabilities. While security research into software and hardware is desirable, the law by and large restricts such research. This results in a reality of highly unsecure Internet-of-Things devices and could potentially lead to serious harms to security and privacy. Such a legal accommodation should be supported by other legal adaptations, mainly involving regulatory oversight and enforcement, consistent rules for

[1] The author is a Cyber Fellow at the Center for Global Legal Challenges and a Resident Fellow at the Information Society Project, Yale Law School. I wish to thank The Center for Cyber Law & Policy at the University of Haifa for its generous support, which made this project possible. I would also like to thank Rosa Brooks, Oona Hathaway, Scott Shapiro, Robin West, Taisu Zhang, Molly Brady, Rebecca Crootof, Claudia Haupt, the ISP fellows' workshop, Data & Society fellows, and the Georgetown Law fellows' workshop. This article is forthcoming in the OHIO STATE LAW JOURNAL in 2019.

vulnerability disclosure, and clear distinctions between ethical and malicious hackers.

Contents

INTRODUCTION

Everyday devices and appliances are becoming more sophisticated, computerized, and software-backed. Cars, thermostats, door locks, smart watches, and even toasters are now powered by code and connected to the Internet, which offers a variety of online features that allow users to remotely monitor and control their devices. These objects are collectively referred to as the "Internet of Things" (IoT) to denote that Internet is no longer exclusively a platform for people to communicate with each other; it is now also a network for "things" to communicate amongst themselves and at times to collect and transmit user data to corporations and state authorities.[2]

The proliferation of IoT devices in personal, business, and public environments is part of a technological shift from hardware to software.[3] Physical objects are being supplemented, and even replaced, by software.[4] By 2020, it is expected that IoT will reach as many as 20 billion connected devices, compared to 8 billion today,[5] with other estimates extending to as much as 50 billion devices.[6] The future worth of the IoT industry is also estimated in the hundreds of billions of dollars should its trajectory remain as projected.[7] This shift is preceded by a phenomenon of embedding processors into everyday "things." In the past, this would have been immensely expensive and inefficient, whereas today, microprocessors are widely available and affordable, and Internet

[2] *See* Bruce Schneier, *Security and the Internet of Things*, SCHNEIER ON SECURITY (Feb. 1, 2017) https://www.schneier.com/blog/archives/2017/02/security_and_th.html (arguing that data collected about us and the things we do is available to both corporations and governments).

[3] Paul Ohm & Blake Reid, *Regulating Software When Everything Has Software*, GEO. WASH. L. REV. 1672, 1673 (2016).

[4] *Id.*

[5] *See Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*, GARTNER (Feb. 7, 2017) http://www.gartner.com/newsroom/id/3598917.

[6] INTERNET OF THINGS – PRIVACY & SECURITY IN A CONNECTED WORLD, FTC STAFF REPORT i (Jan. 2015).

[7] Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security*, 31(2) BERK. TECH. L. J. 997, 1009 (2016).

speeds are constantly increasing, meaning that it is easier to manufacture "smart" objects that operate smoothly.[8]

Software, however, is not the only emerging technological feature in everyday objects. The uniqueness of IoT is its Internet connectivity, which makes it part of the global network grid, with all the pertaining conveniences and dangers.[9] The IoT trend will most likely continue to grow and pose serious challenges in the future, both legally and technically. Some argue that the IoT development may signal "the end of ownership,"[10] since copyright may stifle any modification to the software of these devices, but copyright law is also in a way a form of information censorship.[11]

However, I argue that unless a broad freedom to hack these devices for security purposes is recognized, at least until regulatory agencies catch up, IoT technology could also be the end of security

---

[8] *See* BROADBAND COMMISSION FOR DIGITAL DEVELOPMENT, BROADBAND DRIVES THE INTERNET OF THINGS, http://www.broadbandcommission.org/Documents/Media%20Corner%20Files%20and%20pdfs/Broadband%20drives%20the%20Internet%20of%20Things.pdf ("Broadband represents the vital final piece of the puzzle. The need for always-on bandwidth combined with potentially huge numbers of networked objects – some estimate many billion individually connected devices – imply an immense data throughput on networks"). *See also* LOPEZ RESEARCH, AN INTRODUCTION TO THE INTERNET OF THINGS (IOT) 2 (Nov. 2013), *available at* http://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf (identifying the many features of today's tech world allowing the proliferation of IoT: IPv6, battery life, decreased cost of wireless networks, and broadband speeds).

[9] *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 ["With its insecure devices with multiple points of data access, user applications that routinely exfiltrate our sensor data, activity logs and personal contacts, and a Sisyphean uphill struggle required to exert any control over who knows what about us, the Internet of things does more than create whole new cyber-security attack surfaces. It is so riddled with metastasising points of vulnerability that you begin to sense that these are not bugs, but features."]

[10] *See* Pamela Samuelson, *Freedom to Tinker*, 17 THEORETICAL INQ. L. 563, 589 (2016) (quoting AARON PERZANOWSKI & JASON SCHULTZ, THE END OF OWNERSHIP (2016)).

[11] *See* Susan Brenner, *Complicit Publication: When Should the Dissemination of Ideas and Data be Criminalized*? 13 ALB. L. J. SCI. & TECH. 101, 348–56 (2003).

and privacy, broadly speaking.[12] This is particularly true considering that the complexities of IoT software will necessarily mean tradeoffs in terms of security, and vendors creating complex IoT software will have to test it for every possible attack or compromise, which is essentially impossible.[13] Even if it were possible, experts argue that software engineers cannot predict future methods of attack,[14] and software testing would also not solve the social engineering threat that targets the unwitting cooperation of users,[15] which involves "opening an infected file, clicking on a malicious hyperlink, sending personal information to a phishing Web site, or manually adjusting security settings."[16] However, it is still believed that the vast majority of security breaches are caused by flaws in software.[17]

While embedding access to the global network within ordinary objects offers many advantages – it makes devices more dynamic, customizable, user-friendly (to an extent), and, generally, smarter – it also poses a series of security challenges that, if they remain unaddressed, may represent actual threats to the "digital order" in the form of rampant security breaches and privacy violations.

The major problem with today's unsecure IoT environment is that it is largely a result of a market failure. The market failure manifests itself in multiple ways. First, the industry is not legally bound by any particular guidelines on security and privacy; a sizable number of devices are therefore unsecure, offering an opportunity for criminals and other exploiters to commit malicious cyber-attacks against innocent users. This could even go further; IoT can also be used as a proxy for larger attacks against critical infrastructure,

---

[12] *See* Samuelson, *supra* note 10, at 589.

[13] Trevor A. Thompson, *Terrorizing the Technological Neighborhood Watch: The Alienation and Deterrence of the "White Hats" Under the CFAA*, 36 FLA. ST. U. L. REV. 537, 543 (2009).

[14] Capers Jones, *Software Defect-Removal Efficiency*, 29 COMPUTER 94, 94–95 (1996).

[15] *See* Thompson, *supra* note 13, at 545 ("Even when software performs as intended, software cannot fully protect users from themselves.") *See also Immunizing the Internet, Or: How I Learned to Stop Worrying and Love the Worm*, 119(8) HARV. L. REV. 2442, 2449 (2006) ("[I]t is much harder to 'patch' a person than a computer.").

[16] *See* Thompson, *supra* note 13, at 547.

[17] *See* Derek Bambauer & Oliver Day, *The Hacker's Aegis,* 60 EM. L. REV. 1051, 1060 ("Gartner calculates that 75% of security breaches result from software flaws.").

including the very backbone of the Internet – an externality that neither vendors or IoT users necessarily care about, because they do not directly experience the adverse effects of those externalities.[18] Second, IoT vendors have no economic incentive to offer security as a feature in their products, primarily because consumers are not showing strong preferences toward security and privacy as higher priorities than lower prices. At the very least, informational gaps between vendors and consumers lead to an uninformed and inefficient choice by consumers.[19] The Senate has recently recognized this particular market failure and has proposed IoT industry-focused legislation.[20]

Ransomware attacks[21] are only one example of malicious activity that criminals or nation-states may use against unsecure IoT devices, and reports indicate that ransomware against IoT is already taking place at present.[22] Distributed denial-of-service (DDoS)

---

[18] *See Dyn Statement on 10/21/2016 DDoS Attack*, https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/ (explaining how an IoT-enabled denial-of-service attack against DNS provider Dyn made it impossible for Internet users on the East Coast to reach various websites). *See also* Bruce Schneier, *Your WiFi-connected Thermostat Can Take Down the Whole Internet. We Need New Regulations*, WASHINGTON POST (Nov. 3, 2016), https://www.washingtonpost.com/posteverything/wp/2016/11/03/your-wifi-connected-thermostat-can-take-down-the-whole-internet-we-need-new-regulations/ ("An additional market failure illustrated by the Dyn attack is that neither the seller nor the buyer of those devices cares about fixing the vulnerability. The owners of those devices don't care. They wanted a webcam—or thermostat, or refrigerator—with nice features at a good price. Even after they were recruited into this botnet, they still work fine—you can't even tell they were used in the attack.").

[19] *See* RICHARD SPINELLO, CYBERETHICS: MORALITY AND LAW IN CYBERSPACE 152 (2006) (explaining that the loss of privacy is a market failure).

[20] *See* Senators Mark Warner, Cory Gardner, Ron Wyden, and Steve Daines, *Internet of Things Cybersecurity Improvement Act of 2017 – Fact Sheet*, https://www.warner.senate.gov/public/_cache/files/8/6/861d66b8-93bf-4c93-84d0-6bea67235047/8061BCEEBF4300EC702B4E894247D0E0.iot-cybesecurity-improvement-act---fact-sheet.pdf.

[21] *See* Kim Zetter, *What Is Ransomware? A Guide to the Global Cyberattack's Scary Method*, WIRED (Apr. 5, 2017), https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise (explaining that ransomware is malware that prevents access to data resident on a target computer by encrypting data files, without the user being able to access them until he or she pays the ransom).

[22] *See* Dan Bilefsky, *Hackers Use New Tactic at Austrian Hotel: Locking the Doors*, N.Y. TIMES (Jan. 30, 2017) (explaining that computer systems responsible

attacks,[23] data breaches, and surveillance[24] are all possible threats to IoT users if its security problem remains unaddressed.[25]

Recently, Bruce Schneier, leading cybersecurity and cryptography expert, referred to the increasing prevalence of IoT devices as a "World-sized Web,"[26] denoting that this ubiquitous network of devices will benefit corporations seeking to maximize profits, open new vulnerabilities[27] for criminals to exploit, and aid totalitarian regimes throughout the world. It is almost a cliché in the information security community that IoT devices are very often unsecure and relatively easy to hack[28] due to an abundancy of software flaws, unpatched vulnerabilities, and even an inability to "patch" these devices' flaws once they are discovered.[29] This is

for the electronic key system was hit with ransomware). *See also* Nathaniel Mott, *Ransomware Didn't Lock People in Their Hotel Rooms,* TOM'S HARDWARE (Jan. 30, 2017), http://www.tomshardware.com/news/ransomware-didnt-lock-hotel-rooms,33528.html (claiming that the Austrian hotel ransomware was not quite as reported, but a regular ransomware affecting generation of new keys).

[23] *See* Anonymous, *Immunizing the Internet, Or: How I Learned to Stop Worrying and Love the Worm,* 119(8) HARV. L. REV. 2442, 2444 (2006) (DDoS attacks are "self-propagating worms [who] take control of vulnerable computers . . . the attackers then command the computer to flood the targeted systems with requests for information, preventing legitimate traffic from getting through.").

[24] *See generally* Andrew Ferguson, *The Internet of Things and the Fourth Amendment of Effects,* 104 CAL. L. REV. 805 (2016).

[25] *See generally* Michael Covington & Rush Carskadden, *Threat Implications of the Internet of Things,* 5th INT'L CONF. CY. CONFLICT (2013).

[26] *See* Bruce Schneier, *The Internet of Things Will be the World's Biggest Robot,* SCHNEIER ON SECURITY (Feb. 4, 2016), https://www.schneier.com/blog/archives/2016/02/the_internet_of_1.html.

[27] For the purposes of this Article, "vulnerability" is broadly defined as "a set of conditions that may compromise the confidentiality, integrity, or availability of an information system. It is often a simple oversight or weakness in a computer's software that lets the hacker manipulate computer data." Edward Freeman, *Vulnerability Disclosure: The Strange Case of Bret McDanel,* 16 INFORMATION SYSTEMS SECURITY 127, 127 (2007).

[28] *See* Bruce Schneier, *IoT Teddy Bear Leaked Personal Audio Recordings,* SCHNEIER ON SECURITY (Mar. 15, 2017), https://www.schneier.com/blog/archives/2017/03/iot_teddy_bear_.html.

[29] Patchability – the ability to release security updates to fix vulnerabilities, is still unavailable in many IoT devices, *see* Bruce Schneier, *The Internet of Things is Wildly Insecure – And Often Unpatchable,* WIRED (Jan. 6, 2014), https://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-

largely enabled by market forces, which pressure vendors to create cheaper devices at the cost of disregarding security and privacy.[30] In other words, this reality is enabled by the tech industry's drive to innovate at an accelerated pace,[31] while working under the assumption that embedding cybersecurity could stifle this rapid innovation rate.[32]

To address the abovementioned market failure, this Article argues that outsourcing some of the vulnerability discovery to third-party actors – security researchers – would bolster IoT security. These researchers essentially employ hacking techniques for the purpose of enhancing security – in other words, they think and act like a hacker *for* the company in order to ward off future criminal hacking.

Currently, federal law imposes significant limitations on unsolicited hacking for security research through both civil penalties and criminalization of certain hacking activities, leading to fears of legal jeopardy among members of the cybersecurity community.[33]

---

things-and-thats-a-huge-problem/ ("[I]t's often impossible to patch the software or upgrade the components to the latest version.").

[30] *See* CONNECTED WORLD: EXAMINING THE INTERNET OF THINGS: HEARING BEFORE THE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION, UNITED STATES SENATE, ONE HUNDRED FOURTEENTH CONGRESS, FIRST SESSION, S. Hrg. 114–237, 119 ("The computer chips that power these systems are often cheaply produced, rarely updated or patched, and highly susceptible to hacks . . . . These devices will be cheap, even disposable, and the incentives for the manufacturer to provide regular security updates will be minimal.").

[31] *See* Schneier (*The Internet of Things Is Wildly Insecure – And Often Unpatchable) supra* note 29 (giving an example of how some of the tech industry operates – "The chip manufacturer is busy shipping the next version of the chip, and the ODM is busy upgrading its product to work with this next chip. Maintaining the older chips and products just isn't a priority. And the software is old, even when the device is new. For example, one survey of common home routers found that the software components were four to five years older than the device").

[32] *See* Adam Thierer, Andrea O'Suillivan, *Leave the Internet of Things Alone*, U.S. NEWS (Jun. 12, 2017), https://www.usnews.com/opinion/economic-intelligence/articles/2017-06-12/dont-stifle-the-internet-of-things-with-regulation (arguing that heavy security regulation on IoT will place an undue burden on the IoT industry).

[33] UC Berkeley School of Information, *Cybersecurity Research: Addressing the Legal Barriers and Disincentives*, at 1 (Sept. 28, 2015), *available at*

Exceptions to these legal sanctions, if they exist, are typically very narrow and would still put benign actors under the threat of legal consequences from vendors, thus limiting the amount of overall security research as well as the ability to present such research in an academic setting for further study and development.[34]

In order to enhance IoT security, the law, as well as the institutions creating, interpreting, and applying the law, should allow hacking for the purpose of security research. Such "benign" hacking would reveal flaws and weaknesses in software that, if exploited by malicious actors, could affect not only individuals' personal security and privacy but even US national security.[35] This approach will increase the efficiency of vulnerability disclosure and patching because there will be no chilling effect on the activity of revealing software vulnerabilities.[36] To be clear, security research is only one part of the overall cybersecurity concoction, which should include, in Lawrence Lessig's words, an optimal balance between "public law and private fences."[37] There is a race between benevolent and malicious actors in cyberspace, and the argument advanced by this paper seeks to empower actors who wish to improve the overall security and privacy of IoT.

---

https://www.ischool.berkeley.edu/sites/default/files/cybersec-research-nsf-workshop.pdf.

[34] *See* Derek Bambauer, Oliver Day, *The Hacker's Aegis,* 60 EM. L. REV. 1051, 1054 (2011) (arguing that IP laws stifle critical security research and blocks or limits the ability to share information relating to security flaws) (citing Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974 (2006)).

[35] *See* Melissa Hathaway, *Cyber Security: An Economic and National Security Crisis*, 16 INTELLIGENCER 31 (2008). Also, *see* U.S. Department of Defense, *DOD Announces Digital Vulnerability Disclosure Policy and "Hack the Army" Kick-off* (Nov. 21, 2016), https://www.defense.gov/News/News-Releases/News-Release-View/Article/1009956/dod-announces-digital-vulnerability-disclosure-policy-and-hack-the-army-kick-off (where then-Secretary of Defense, Ash Carter, underscores that "We want to encourage computer security researchers to help us improve our defenses. This policy gives them a legal pathway to bolster the department's cybersecurity and ultimately the nation's security.").

[36] *See* Malena Carollo, *Influencers: Lawsuits to Prevent Reporting Vulnerabilities Will Chill Research,* CHRISTIAN SCIENCE MONITOR (Sep. 29, 2015) (providing data that 75% of leading experts (referred to as "the Influencers") believe that lawsuits against vulnerability disclosure in public will have chilling effects on security research).

[37] *See* LAWRENCE LESSIG, CODE 2.0 170 (2006).

The underlying hypothesis of this paper is that advancing IoT technologies will transform our lives entirely by becoming a substantial part of our society. The ubiquity of sensors, the physicality of most IoT devices, and the absence of reasonable default security standards could lead to major threats to individual and collective security and privacy. The rapid development of this field has already led to regulatory inefficiency and a serious market failure, enabling vendors to manufacture and sell unsecure IoT devices globally. Providing an incentive for the broader security community to become involved in fixing this ecosystem without fear of legal jeopardy will make individual users safer while also protecting critical infrastructure, such as hospitals, power plants, and the Internet backbone, from IoT externalities.[38]

This paper will proceed in four parts. In Part I, I will discuss the phenomenon of IoT – "the world of hackable things" – and provide an overview of the market failures at play. These market failures are at the crux of this Article's argument because they allow threats to individual users and third-parties to flourish as a result of unsecure IoT devices. Part II will be dedicated to introducing the security research environment, in which different types of hackers and motivations are shaping reality. In Part III, I will focus on the legal hurdles impeding "the freedom to hack" – mainly the federal prohibition of circumvention of technological protection measures (TPMs) and criminal liability for unauthorized access to protected computers. Finally, Part IV will propose a concrete framework for creating a normative, technical, and institutional environment in which security researchers can achieve their goal of making software more secure by distinguishing benevolent from malicious actors, strengthening regulatory oversight and enforcement, clarifying statutory boundaries, regulating *patchability*, creating a consistent procedure for disclosure of vulnerabilities, and tackling security by obscurity.

I. Internet of *Hackable* Things

[38] *See* Anonymous, *Immunizing the Internet, Or: How I Learned to Stop Worrying and Love the Worm*, 119(8) HARV. L. REV. 2442, 2443 (2006) ("Not only does current policy create the wrong incentives regarding cybercrime, it does too little to encourage computer hackers and computer users to contribute actively to Intern.").

It was probably unimaginable at the conception of the Internet that one day it would be used to connect everyday "things" to it. The development of this phenomenon allowed for machine-to-machine communication, the "communication between . . . entities that do not necessarily need any direct human intervention."[39] Whether through a smart thermostat that learns a user's temperature-setting patterns,[40] a bracelet that tells a user how well she exercises and sleeps,[41] a webcam that can wirelessly transmit photos and videos,[42] a smart toaster offering the perfect toast,[43] or a car that has the ability to connect to the Internet and offer navigation services, self-diagnosis tools, and remote control through widely used smartphones,[44] such machine-to-machine networks abound.

There is a growing understanding that "things with computers embedded in them" are becoming "computers with things attached to them."[45] This means that a whole set of legal issues traditionally pertaining to computers are transposed into the area of ordinary daily objects, but those ordinary daily objects now have a few extra features that make questions of legality tremendously challenging. For example, previously, if a toaster malfunctioned, it would have been mainly a consumer protection problem, whereas today, it might as well be a telecommunications problem, involving a whole set of

---

[39] Roberto Minerva, Abyi Biru & Domenico Rotondi, *Towards a Definition of the Internet of Things (IoT)*, IEEE INTERNET INITIATIVE, 12 (May 27, 2015), http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things _Revision1_27MAY15.pdf

[40] Nest, *Meet the Thermostat,* https://nest.com/thermostat/meet-nest-thermostat.

[41] *See* Andrew Meola, *Wearable Technology and IoT Wearable Devices,* BUSINESS INSIDER (Dec. 19, 2016), http://www.businessinsider.com/wearable-technology-iot-devices-2016-8.

[42] *See* Haley Edwards, *How Web Cams Helped Bring Down the Internet, Briefly*, TIME (Oct. 25, 2016), http://time.com/4542600/internet-outage-web-cams-hackers.

[43] Joel Hruska, *The Internet of Things Has Officially Peak Stupid, Courtesy of This Smart Toaster*, EXTREME TECH (Jan. 5, 2017), https://www.extremetech.com/electronics/242169-internet-things-officially-hit-peak-stupid-courtesy-smart-toaster-griffin-technology.

[44] *See* Thilo Koslowski, *Forget the Internet of Things: Here Comes the 'Internet of Cars',* WIRED (Jan. 4, 2013), https://www.wired.com/2013/01/forget-the-internet-of-things-here-comes-the-internet-of-cars.

[45] *See* Bruce Schneier, *Security and the Internet of Things,* SCHNEIER ON SECURITY (Feb. 1, 2017), https://www.schneier.com/blog/archives/2017/02/security_and_th.html.

challenges pertaining to privacy and security and, in more extreme circumstances, national security.[46]

While the general phenomenon of IoT is somewhat intuitive in today's hyperconnected world, there is no official or widely adopted definition of the technology. One definition is "the ability of everyday objects to connect to the Internet and to send and receive data,"[47] a feature that was previously nonexistent in everyday "things." Another definition provides that IoT is "a network of items—each embedded with sensors—which are connected to the Internet"[48]; another similar definition characterizes IoT as a "system where the Internet is connected to the physical world via ubiquitous sensors."[49] While Internet connectivity is itself quite intuitive, often missing in defining IoT is an emphasis on the sensors, actuators, and CPUs, or cloud computers,[50] that often comprise the IoT ecosystem.

Unlike personal computers (desktop, laptops, smartphones, and the like), IoT devices often lack a user interface, or at least one that allows control over security and privacy features.[51] IoT should also be contrasted from popular operating systems, which are supported by large tech companies who constantly offer updates to the software. This largely means that the degree of user control over the configuration of a device is significantly limited and is usually

---

[46] *See* Mike Orcutt, *Security Experts Warn Congress That Internet of Things Could Kill People,* M.I.T. TECH. REV. (Dec. 5, 2016), https://www.technologyreview.com/s/603015/security-experts-warn-congress-that-the-internet-of-things-could-kill-people.

[47] INTERNET OF THINGS – PRIVACY & SECURITY IN A CONNECTED WORLD, FTC STAFF REPORT i (Jan. 2015).

[48] *See* Kathy Pretz, *Smart Sensors,* THE INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS (Mar. 14, 2014), http://theinstitute.ieee.org/technology-topics/internet-of-things/smarter-sensors.

[49] Roberto Minerva, Abyi Biru, and Domenico Rotondi, *Towards a Definition of the Internet of Things (IoT),* IEEE INTERNET INITIATIVE, 10 (May 27, 2015), http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things _Revision1_27MAY15.pdf.

[50] The fact that many IoT devices are supported by cloud computing creates and additional risk to privacy, since data stored on the cloud could potentially become the target of a data breach against the cloud itself. *See* Bambauer, *supra* note 34, at 1059 (providing an example of cloud weakness that led to a security breach against Twitter).

[51] FTC IOT REPORT, *supra* note 6, at v.

controlled by the vendor, if at all. It is expected that the vendor will provide reasonable security already built into the device – "security by design" – but unfortunately, the current state of affairs in IoT has proven otherwise.[52]

Understanding the physicality of IoT is crucial if we are to create solutions to the wide range of resulting legal challenges. IoT insecurity is not merely a theoretical threat – it is an actual danger to our very homes. Typically, an IoT device is comprised of three components – a sensor, a CPU (or cloud computer), and an actuator.[53] While a sensor collects data about its users and environment,[54] the CPU (or "the cloud") processes that data and potentially commands the actuator to take appropriate actions. These two components are essential for controlling the actuator, which is an "output device[] that implement[s] decisions."[55] For example, a sensor could be a thermostat used to monitor the temperature, with a connected CPU tasked with determining whether the air conditioner should be turned on or off, which would be accomplished through the actuator, the actual object that this whole system was built to control. In a way, sensors are the "eyes and ears" of the Internet, and the actuators are "hands and feet." The CPUs, in this analogy, would be the brain, since they process data and react to it according to certain predetermined software-based rules.[56]

Since a typical user has little to no control over the security features (and many other features) of their specific device, enhancing the security of the device will necessarily require the user to tinker with the software, which could violate the anti-circumvention rules of the Digital Millennium Copyright Act

---

[52] *See* Symantec, *An Internet of Things Reference Architecture* (2016) ("Most IoT devices are "closed." Customers can't add security software after devices ship from the factory. Often, such tampering voids the warranty. For such reasons, security has to be built into IoT devices so that they are "secure by design." In other words, for IoT, security must evolve from security just "bolted onto" existing systems such as servers and personal computer (PC) laptops and desktops. Security must evolve to security that is "built in" to the system before the system leaves the factory.").

[53] *See* Schneier, *supra* note 2.

[54] *Id.*

[55] *See* Poudel, *supra* note 7, at 1003.

[56] *See* Schneier, *supra* note 2.

(DMCA), unless the user is explicitly exempt from legal liability.[57] In addition, security researchers who might want to probe specific IoT devices for vulnerabilities might encounter threats of criminal liability and prosecution if the manner in which they access these devices is unauthorized – which includes virtually any form of hacking.[58]

Therefore, users often have to rely on vendors' practices of vulnerability patching and security by design, which do not always exist in a market of accelerated innovation and competition, particularly in cheaper devices.[59] In many instances, a vendor's decision whether to provide vulnerability patches is a question of risk assessment and market forces – and market forces, particularly in the tech industry, do not always work in favor of consumers (if we assume that privacy and security are in the interest of consumers).[60] This is perhaps more alarming considering that the

---

[57] *See* Aaron Alva, *DMCA Security Research Exemption For Consumer Devices*, Tech@FTC (Federal Trade Commission), https://www.ftc.gov/news-events/blogs/techftc/2016/10/dmca-security-research-exemption-consumer-devices.

[58] *See* 18 U.S.C. § 1030(a)(2). *See also* Erin Fleury, *Is It Illegal to Test Websites For Security Flaws? Heartbleed & The CFAA*, MINN. J. L. SCI. & TECH. F. (Dec. 30, 2014), http://editions.lib.umn.edu/mjlst/is-it-illegal-to-test-websites-for-security-flaws-heartbleed-the-cfaa (arguing that the discovery of the OpenSSL Heartbleed security flaw, which allowed intercepting encrypted information, caused systems "to send back far more than what is intended. Of course, the CFAA is meant to target people who use exploits such as this to gain unauthorized access to computer systems, so it would seem that using Heartbleed is clearly within the scope and purpose of the CFAA. The real problem arises, however, for people interested in independently (i.e. without authorization) testing a system to determine if it is still susceptible to Heartbleed or other vulnerabilities").

[59] *See* Rapid7's Comment to NTIA's call for public comments on "*The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*", *available at* https://www.ntia.doc.gov/files/ntia/publications/rapid7_comments_to_ntia_iot_rfc_-_jun_2_2016.pdf ("Since IoT devices are highly diversified and include very inexpensive items manufactured by companies with limited security experience, the result can be a considerably more exploitable environment than the status quo.").

[60] *See* Keynote Remarks of FTC Commissioner Terrell McSweeny, "Consumer Protection in the Age of Connected Everything" 3 (New York Law School, Feb. 3, 2017) *available at* https://www.ftc.gov/system/files/documents/public_statements/1070193/mcsweeny_nyls_iot_sympoisum.pdf ("Consumer concern is heightened by business practices that often leave them in the lurch: IoT products may not have patch

cost of security breaches to users in aggregate is significantly higher than the cost to vendors, which could explain the gap in expectations between vendors and users.[61] In other words, "systems are particularly prone to failure[] when the person guarding them is not the person who suffers when they fail."[62]

a. The Economics of IoT

Many assume that the market will eventually solve the security and privacy problems of the IoT ecosystem. But this may not be accurate given that these problems are themselves a result of a market failure. The unlikelihood of a market solution is particularly stark when examined in terms of the costs associated with cyber-attacks on IoT, which are often experienced by third parties and are therefore considered externalities.[63] Because such externalities involve a wide variety of sectors and actors, with varying degrees of costs and benefits, the prospect of an efficient transaction is unlikely.

When it comes to externalities in software, it is often believed that software vulnerabilities are "inevitable externalities" because flawless software[64] does not yet exist. This is further exacerbated by the pressure on vendors by competition to release software to the market as fast as they can.[65] While this trend is generally true, it is

support or the same life expectancy as other connected products, and these limitations are not always communicated clearly to consumers… Consumers are repeatedly saying that data security is a top barrier to purchasing connected devices.").

[61] *See* Bambauer, *supra* note 34, at 1059 ("[U]sers face greater harm than vendors do, especially overall. While precise figures are difficult to ascertain, reliable estimates of the worldwide economic damage caused by digital attacks in 2003 range from $12.5 billion for worms and viruses, and $226 billion for all attacks, to $157–$192 billion on Windows PCs alone in 2004. Losses to vendors from security breaches, such as from increased support costs, reputational harm, and declines in share price, are also uncertain, but likely considerably smaller. Vendors, therefore, have less incentive to fix bugs than is socially optimal.")

[62] Anderson & Moore, *The Economics of Information Security*, 314 SCIENCE 610, 610 (2006).

[63] *See* Schneier, *supra* note 2.

[64] *See* JOHN VIEGA, THE MYTHS OF SECURITY 142–44 (Mike Loukides ed., 2009). *See also* Jay Pil Choi et al., *Network Security: Vulnerabilities and Disclosure Policy*, 58 J. INDUS. ECON. 868, 869 (2010).

[65] See Micah Schwalb, *Exploit Derivatives & National Security*, 9 YALE J. L. & TECH. 162, 168–69 (2007).

still possible to make software better through constant fixing of vulnerabilities, therefore reaching a socially optimal level of security.

Furthermore, companies who decide to enter the IoT market do not always have the experience needed to implement security features in their devices.[66] There is a sizable degree of opportunism when it comes to new players in the IoT industry, making unsecure IoT devices pervasive.

In addition, IoT devices are largely inexpensive and disposable, which precludes most costly security features.[67] The literature identifies additional reasons for ubiquitous unsecure IoT devices – lack of experience in data security among vendors, absence of processing power in most IoT devices for "robust security measures such as encryption," and unforeseen threats,[68] given that the attackers are humans who constantly adapt and change their methods.[69] The recurring theme is the inability of vendors to fully solve the potential security flaws in IoT devices on their own.

At the same time, the users themselves are often unaware of the risks; IoT architecture is often driven by vendors attempting to reduce costs, and the individual consumer is typically interested in a product's features, rather than its security settings.[70] Whereas computers have been hackable since their conception, the IoT ecosystem increases the stakes to a far greater state of urgency. This is largely enabled by the physicality of IoT, which can cause serious physical harms, and the ubiquitous sensors, which pose a privacy concern to users.[71] This notion is further supported by the

---

[66] FTC IOT REPORT, *supra* note 6, at 13.

[67] FTC IOT REPORT, *supra* note 6, at 13.

[68] *See* Poudel, *supra* note 7, at 1015 (citing Scott Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent*, 93 TEX. L. REV. 85, 135–36 (2014)).

[69] NIELS FERGUSON & BRUCE SCHNEIER, PRACTICAL CRYPTOGRAPHY 5, 11–12 (2003).

[70] *See* FTC IOT REPORT, *supra* note 6, at i–ii.

[71] *See* Schneier, *supra* note 2 ("All computers are hackable. This has as much to do with the computer market as it does with the technologies. We prefer our software full of features and inexpensive, at the expense of security and reliability. That your computer can affect the security of Twitter is a market failure. The industry is filled with market failures that, until now, have been largely ignorable.

unwillingness of certain tech companies to patch their software if it does not yield an effective cost-benefit analysis.[72] Furthermore, while security and privacy are certainly important to consumers, it is unclear whether consumers will agree to pay more for a product that is more secure, even if current vendor–user informational gaps are decreased.[73] This suggests that even if informing users of the risks is unlikely to solve the problem of unsecure IoT.

The classic solution to externalities resulting from market failures is government intervention in the form of legislation and regulation.[74] This Article takes another approach – legislation and regulation of the IoT industry are certainly required, but they could be far more efficient in conjunction with the lifting of burdens constraining security researchers. In other words, the market failure described in this subchapter can be mitigated by security researchers improving software quality through ethical hacking.

b. The Technology of IoT

IoT offers a convenience not previously available in offline objects. First, the user has some remote control over certain features of the device, often from a smartphone or personal computer. She has the ability to customize and monitor the functionality of her appliances, though this is often limited through the user interface provided by the vendor.[75] Second, IoT technology equips vendors

---

As computers continue to permeate our homes, cars, businesses, these market failures will no longer be tolerable. Our only solution will be regulation, and that regulation will be foisted on us by a government desperate to "do something" in the face of disaster.").

[72] *See* Andrew Aurenheimer, *Forget Disclosure – Hackers Should Keep Security Holes to Themselves*, WIRED (Nov. 29, 2012), https://www.wired.com/2012/11/hacking-choice-and-disclosure ("[T]he vendor may decide not to release a patch because a cost/benefit analysis conducted by an in-house MBA determines that it's cheaper to simply do . . . nothing.").

[73] *See* Jay Kesan & Carol Hayes, *Bugs in the Market: Creating A Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities*, 58 ARIZ. L. REV. 753, 781–82 (2016).

[74] *See* Eli Dourado & Jerry Brito, *Is There a Market Failure in Cybersecurity?*, 106 MERCATUS ON POLICY (2012), p. 2.

[75] *See* Nick Feamster, *Who Will Secure the Internet of Things?* FREEDOM TO TINKER (Jan. 19, 2016), *available at* https://freedom-to-tinker.com/2016/01/19/who-will-secure-the-internet-of-things ("Manufacturers of consumer products have little interest in releasing software patches and may

with the ability to optimize and improve their products through processing user data generated by the devices. However, this comes at a cost, since consumer data may also be used in negative ways, such as aggressive advertising, sale to third parties, or enhancement of surveillance capabilities.[76] Third, IoT technology offers interoperability between devices, which, though it is yet to be fully developed, allows devices to communicate with each other.[77] These benefits may sometimes even relate to the health, quality of life, and wellbeing of the user. Insulin pumps and pacemakers are examples of IoT applications in healthcare that revolutionized diagnosis and medical treatment, making these patients' health much more manageable.[78]

Cybersecurity risks and threats existed long before the advent of IoT, and the argument made by this Article could apply equally to IoT and non-IoT environments, since software will have flaws regardless of the platform on which it runs. However, the IoT ecosystem creates a serious challenge and shakes up some basic cybersecurity assumptions – it significantly broadens the attack surface that hackers can use, and the level of harm to autonomy is also far greater, thus trivializing hacking in general but also making it more personal.[79] This will result in more opportunistic hacking,

---

even design the device without any interfaces for patching the software in the first place.").

[76] *See generally* Andrew Ferguson, *The Internet of Things and the Fourth Amendment of Effects,* 104 CAL. L. REV. 805 (2016).

[77] *See* Charles McLellan, *M2M and the Internet of Things: A Guide,* ZDNet (Jan. 10, 2013), http://www.zdnet.com/article/m2m-and-the-internet-of-things-a-guide.

[78] *See* FTC IOT REPORT, *supra* note 6, at 8. ("connected health devices can "improve quality of life and safety by providing a richer source of data to the patient's doctor for diagnosis and treatment[,] . . . improve disease prevention, making the healthcare system more efficient and driving costs down[,] . . . [and] provide an incredible wealth of data, revolutionizing medical research and allowing the medical community to better treat, and ultimately eradicate, diseases.").

[79] Oliver Tavakoli, *The Unintended Attack Surface of the Internet of Things*, DARK READING (Sept. 29, 2015), www.darkreading.com/vulnerabilities---threats/the-unintended-attack-surface-of-the-internet-of-things/a/d-id/1322393 ("[T]he combination of poorly written code and infrequent updates will surely lead to a broader and less manageable attack surface."). *See also* FTC IOT REPORT, *supra* note 6, at 11 ("[A]s consumers install more smart devices in their homes, they may increase the number of vulnerabilities an intruder could use to compromise

whereby users' security or privacy may be compromised for potential criminal ends.[80]

Law and regulation will find it increasingly difficult to address IoT hacking, due to its immense pervasiveness, volume, and trans-border effects and origins. This will leave the most trivial hacking activities unaddressed from a law enforcement perspective.[81] The argument in this Article, therefore, proposes enhance security by fixing vulnerabilities through a legal system that legitimizes the activities undertaken by security researchers. These researchers employ hacking and reverse-engineering techniques for the purpose of identifying security flaws and reporting them to the respective vendor and, eventually, the public.

The following sub-sections elaborate on why the IoT ecosystem is particularly challenging in the cybersecurity context – sensors are everywhere, processors are operating physical objects, and the distinctions between software and hardware are eroding. These IoT-specific challenges are creating a particularly vulnerable environment.

1. The Ubiquity of Sensors

The IoT ecosystem is creating a world of ubiquitous sensors.[82] These sensors are the eyes and ears of the Internet, collecting data

---

personal information."); La Marca & Paez, *The Internet of Things: Emerging Legal Issues for Businesses*, 43 N. KY. L. REV. 29, 46 (2016) ("As the number of Internet-connected objects expands, so too does the potential attack surface. The loT faces serious security issues because it is based on interoperability and interdependence: more interactions among devices lead to more areas of vulnerability.").

[80] Mihai Lazaresu, *Hacked by Your Fridge: the Internet of Things Could Spark a New Wave of Cyber Attacks*, THE CONVERSATION (Oct. 7, 2016), https://theconversation.com/hacked-by-your-fridge-the-internet-of-things-could-spark-a-new-wave-of-cyber-attacks-66493.

[81] Scholars recognize the limits of law enforcement in the world of computer crime. *See* Anonymous, *Immunizing the Internet, Or: How I Learned to Stop Worrying and Love the Worm*, 119(8) HARV. L. REV. 2442, 2445 (2006) ("[C]ybercrime cannot be effectively combated solely with traditional law enforcement tools.").

[82] *See* Arkady Zaslavsky, *Internet of Things and Ubiquitous Sensing*, COMPUTER (Sept. 2013), https://www.computer.org/web/computingnow/archive/september2013 ("With billions of ICOs [Internet-connected objects] and a diverse abundance of sensors, the IoT will be an enabler of ubiquitous sensing.").

about the environment and processing and possibly transmitting that data elsewhere.[83] These sensors are working continuously, and they are everywhere. IoT devices enable not only data about direct computer use but also data about driving, home heating and cooling, food stored in a refrigerator, pulse and blood pressure, sleep patterns, and much more.

These distributed data can tell a lot about a specific person. The most private and nonintuitive pieces of information about a user are constantly collected by IoT devices and may enable misuse for criminal, business, law enforcement, and other purposes.[84] The richness of data within the IoT ecosystem has also led to law enforcement finding this space appealing for surveillance.[85]

2. Physicality

A significant characteristic of IoT is its physicality. Processors embedded in IoT devices are tasked to operate actual, physical equipment, with tangible consequences in the physical world. Think of a smart thermostat, which learns about the preferences of the user but is also tasked to turn on or off a piece of equipment – the AC or furnace – when certain conditions are met. In this way, the IoT device commands the actuator, meaning that any meddling with IoT could have physical ramifications due to actuators malfunctioning, at times posing danger to physical security. Examples include a

---

[83] *See* Hakima Chaouchi & Thomas Bourgeau, *Internet of Things: From Real to Virtual World*, in NAVEEN CHILAMKURTI, SHERALI ZEADALLY, HAKIMA CHAOUCHI (EDS.), NEXT-GENERATION WIRELESS TECHNOLOGIES: 4G AND BEYOND 161, 173 (2013) (listing some examples of data collected by sensors – "mechanical data (position, force, pressure), thermal data (temperature, heat flow), electrostatic or magnetic field, radiation intensity (electromagnetic, nuclear), chemical data (humidity, ion, gas concentration), and biological data (toxicity, presence of bio organisms)").

[84] *See* Symantec, *Internet Security Threat Report* Vol. 21, 16 (Apr. 2016), https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

[85] *See* Andrew Ferguson, *The Internet of Things and the Fourth Amendment Effects*, 104 CAL. L. REV. 805, 810 (2016) ("The Internet of Things offers new surveillance possibilities that do not involve any physical intrusion into the object. As currently designed, these objects radiate data trails quite useful for law enforcement tracking.").

vehicle not responding to its driver's actions, a disabled insulin pump, and a garage door that won't open.

In other words, today's everyday objects are creating telecommunications problems that challenge notions of security and privacy. These challenges are similar whether we talk about healthcare equipment, household objects, or transportation. The effects, however, may be tremendously different – a malfunctioning pacemaker could lead to death, whereas a disabled wearable smartwatch is a matter of inconvenience or, at most, a privacy violation.

3. Software and Hardware Distinction

Although the growing role and share of software in the overall IoT environment cannot be overstated, hardware also poses a host of challenges to the security and privacy associated with IoT.[86] For example, researchers at the University of Michigan have recently learned that a CPU manufactured in China had a backdoor built by design into the CPU.[87] This enables a small portion of the CPU to be used as an entryway for malware, which can then obtain control over the device. Since IoT devices have CPUs embedded in them, this represents an actual threat to the integrity and resilience of IoT.

From a security and privacy perspective, both the software and the hardware need to be regulated and monitored for potential vulnerabilities that could affect the normal functioning of a device. Regulatory agencies in the U.S. are increasingly focusing their efforts on software, which many believe will be "eating the world" and taking over the digital sphere. But even if this prediction is accurate, hardware may still be designed in a way that allows exploitation, particularly if it is under-regulated due to the appeal of software regulation. Hardware represents an even bigger "black-

[86] *See* Andy Greenberg, *Forget Software – Now Hackers Are Exploiting Physics*, WIRED (Aug. 31, 2016), https://www.wired.com/2016/08/new-form-hacking-breaks-ideas-computers-work ("The trick works by running a program on the target computer, which repeatedly overwrites a certain row of transistors in its DRAM flash memory, "hammering" it until a rare glitch occurs: Electric charge leaks from the hammered row of transistors into an adjacent row. The leaked charge then causes a certain bit in that adjacent row of the computer's memory to flip from one to zero or vice versa. That bit flip gives you access to a privileged level of the computer's operating system.").

[87] *See* Kaiyuan Yang, Matthew Hicks, Qing Dong, Todd Austin, Dennis Sylvester, *A2: Analog Malicious Hardware*, 2016 IEEE SYMPOSIUM ON SECURITY AND PRIVACY, *available at* http://ieeexplore.ieee.org/document/7546493.

box" problem, since it is extremely time consuming and complicated to determine how a specific computer component works, whereas software is relatively easier to grasp – as security researchers have demonstrated recently. Therefore, the analysis provided by this Article, while focusing mostly on software, could still be applicable to security research into hardware.

c. The Threats of IoT

The characteristics of sensor abundancy and general physicality of IoT lead us to a third attribute, which is particularly alarming. IoT devices are not typically manufactured with robust or even minimal security standards (technical, and possibly mechanical). The IoT market failure results in vendors not implementing security in their IoT devices, mostly due to competition – in other words, in order to reduce manufacturing costs and offer a cheaper product. On the other hand, the average consumer does not typically demand strong security features, most likely due to informational gaps.

This suggests that IoT unsecurity is a global problem, since the same security-lacking devices would be present in the U.S. just as in other parts of the world. Regardless, the U.S. has an important role to play from a legal perspective by setting robust standards and best practices for the rest of the world to follow, including the ethical hacking of IoT devices advanced by this paper. In addition, many IoT vendors are based in the U.S. and so fall under the jurisdiction of U.S. laws and regulations, and so ethical hacking within the U.S. would secure both domestic devices as well as those that are exported to elsewhere in the world.

The IoT revolution comes with a price. While the ability of everyday objects to connect to the Internet offers a broad range of advantages, it also poses a set of specific challenges, stemming from the vulnerabilities that these devices have almost by default. The literature generally identifies three major threats with today's IoT ecosystem – privacy, individual user security, and third-party security.[88]

[88] *See* Sir Mark Walport, *The Internet of Things: Making the Most of the Second Digital Revolution*, UK GOV'T OFF. FOR SCI., 15 no. 3 (Dec. 2014), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/ 14-1230-internet-of-things-review.pdf. Also, *see* FTC IOT REPORT, *supra* note 6, p. 10 – (Where the FTC identifies these three threats, providing that

First, since IoT sensors collect data about their respective users and their environment, unauthorized actors may attempt to access that personal information for a variety of reasons. Having security features within an IoT device could make it much harder for these unauthorized actors to access personal information. However, privacy breaches could then still be committed by vendors and other third parties who seek to monetize the collected data, which could also be labeled as a privacy risk.

Second, malicious actors may try to hack into IoT devices and meddle with the functionality of the device. For example, hackers may decide to shut down a car's engine,[89] lock a hotel room while demanding ransom,[90] or disable a pacemaker.[91] These are security risks confined to the user.

Third, IoT devices may be used individually (a single IoT device) or collectively (an "army" of compromised IoT devices) to facilitate an attack or breach targeting another computer system.[92] In this case, the IoT is used merely as a proxy, which allows the hacker to have more disruptive power (if multiple IoT devices are used for a specific attack) and to mask her or his identity. This is the manifestation of the externalities discussed *supra*. For example, a hundred thousand compromised IoT devices were used to mount a distributed denial of service (DDoS) attack against Domain Name

---

unsecure IoT is – "(1) enabling unauthorized access and misuse of personal information, (2) facilitating attacks on other systems, and (3) creating physical safety risks.")

[89] *See* Craig Timberg, *Hacks on the Highway*, WASHINGTON POST (July 22, 2015), http://www.washingtonpost.com/sf/business/2015/07/22/hacks-on-the-highway.

[90] *See* Josephine Wolff, *The Ransomware Attack That Locked Hotel Guests Out of Their Rooms*, SLATE (Feb. 1, 2017), http://www.slate.com/articles/technology/future_tense/2017/02/the_ransomware_attack_that_locked_hotel_guests_out_of_their_rooms.html.

[91] *See* Morie Moe, *Go Ahead, Hackers. Break My Heart*, WIRED (Mar. 14, 2016), https://www.wired.com/2016/03/go-ahead-hackers-break-heart.

[92] *See* FTC IoT Report, *supra* note 6, at 12. ("[A] compromised loT device could be used to launch a denial of service attack. Denial of service attacks are more effective the more devices the attacker has under his or her control; as loT devices proliferate, vulnerabilities could enable these attackers to assemble large numbers of devices to use in such attacks. Another possibility is that a connected device could be used to send malicious emails.").

System (DNS) provider Dyn.[93] The Dyn attack made it impossible for Internet users to access websites like Twitter, Netflix, and Reddit.[94] This is a security risk against third parties – against the Internet.

1. *User Privacy*

IoT devices often generate data about the consumer, which raises the risk of these data being compromised. Many consumers would not be able to differentiate between an Internet-connected object and its offline counterpart in terms of the potential privacy implications. Data collected by IoT devices may pose a host of privacy concerns. For example, in the case of an IoT device used to measure blood alcohol – the Breathometer – collected data may impact "employment decisions, criminal liability implications, and health, life, car insurance ramifications."[95] The data collection, retention, and disposal policies of a specific manufacturer are not always communicated to the consumer in a transparent and accessible manner.[96] This is of course not unique to the Breathometer, as other IoT devices collect sensitive personal data as well.

These problematic uses of personal information are not the end of the story. Certain devices might require the use of payment methods and passwords, which could be accessed and misused by cyber criminals seeking financial gain.[97] If this sensitive information is not properly secured, the number of vulnerabilities and

---

[93] *See* Scott Hilton, *Dyn Analysis Summary of Friday October 21 Attack*, VANTAGEPOINT DYN COMPANY NEWS, https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.

[94] *See* Schneier, *supra* note 2.

[95] *See* Scott Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Conesnt*, 93 TEX. L. REV. 85, 90 (2014).

[96] *See* Peppet, *supra* note 95, at 90 ("[M]any 'things' have little in their external form that suggests they are connected to the Internet. When you grab an Internet-connected scarf from the coat rack or sit on an Internet connected chair, should you have some obvious sign that data will be transmitted or an action triggered?") (citing ADRIAN MCEWEN & HAKIM CASSIMALLY, DESIGNING THE INTERNET OF THINGS 294 (2014)).

[97] *See* Roey Tzezana, *Scenarios for Crime and Terrorist Attacks Using The Internet Of Things*, 4(18) EUROPEAN JOURNAL OF FUTURES RESEARCH 17 (2016).

compromises will increase, exposing personal information to malicious actors.

Another major problem that is currently emerging in the privacy law scholarship is sensor fusion[98] – when innocuous and seemingly insignificant data collected by an individual IoT sensor could be used to make inferences about the user when paired with data collected from other IoT sensors. Collectively, the data could be used to make near-certain inferences about the user, though the individual pieces of data would have no meaning on their own. This could be used to make powerful inferences about the user. For example, data from a smartphone's gyroscope could be used to determine the driving habits of a user; when paired with an IoT pacemaker, the combination of these data can yield an inference about the emotional state and mood of the user.[99] Scholars identify a long list of inferences that would be possible under the emerging IoT ecosystem of data collection – "a user's mood; stress levels; personality type; bipolar disorder; demographics (e.g., gender, marital status, job status, age); smoking habits; overall wellbeing; progression of Parkinson's disease; sleep patterns; happiness; levels of exercise; and types of physical activity or movement."[100] Considering how personal and sensitive some of these data are, IoT devices should allow for stronger security to prevent breaches that could be devastating to users.

Daniel Solove calls this problem "data aggregation" and argues that, "[v]iewed in isolation, each piece of our day-to-day information is not all that telling; viewed in combination, it begins to paint a portrait about our personalities."[101] The bottom line is that malicious actors have many methods of abusing private information

---

[98] *See* Peppet, *supra* note 95, at 118–24 ("Sensor fusion is the combining of sensor data from different sources to create a resulting set of information that is better than if the information is used separately.").

[99] *See* Poudel, *supra* note 7, at 1013.

[100] *See* Peppet, *supra* note 7, at 113.

[101] *See* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1185 (2002) ("Viewed in isolation, each piece of our day-to-day information is not all that telling; viewed in combination, it begins to paint a portrait about our personalities. The aggregation problem arises from the fact that the digital revolution has enabled information to be easily amassed and combined. Even information in public records that is superficial or incomplete can be quite useful in obtaining more data about individuals. Information breeds information.").

they collect without authorization, particularly if they can collect that information across multiple IoT devices.

It must be noted that many of the data described in this sub-section would not be considered personally identifiable information (PII), which, if compromised, imposes notification responsibilities on vendors. However, PII does not typically include sensor data, or anonymized data, which is often re-identifiable.[102] This difficulty seems to suggest that the focus at present should be on enhancing IoT security until federal and state regulations address the full breadth of data that ought to be protected by vendors. At present, relying on state laws regulating notification of data breaches would not necessarily solve the problem of sensor fusion.

2. *User Security*

Vulnerabilities in a specific device may facilitate potential exploitations against that specific device and, consequently, its user. The primary target in this case is not the data in the device but rather the device's functionality. For example, a hacker may decide to attack a thermostat using a ransomware method, meaning that the user will be unable to use the thermostat until she or he pays the ransom.[103] The data are not the primary interest for the hacker here – whereas disrupting the normal functioning of the device is. This hack is also enabled by weak security standards and vulnerabilities in software.

Recently, an Austrian hotel suffered a ransomware attack targeting its smart-locks. The attack locked up hotel rooms until the hotel gave up and paid the ransom in order to restore the functioning of the locks. In that case, hackers did not care about who used the locks, or how, or when.[104]

---

[102] *See* Alexander Tran, *The Internet of Things and Potential Remedies in Privacy Tort Law*, 50 COLUM. J. L. SOC. PROB. 263, 275-276 (2017) (arguing that many state laws are not dealing with sensor data, which may be re-identifiable, with Texas' statute being one of the only exceptions, providing a broad definition to "sensitive personal information").

[103] *See* Dan Raywood, *#DefCon: Thermostat Control Hacked to Host Ransomware*, INFO SECURITY (Aug. 7, 2016), https://www.infosecurity-magazine.com/news/defcon-thermostat-control-hacked.

[104] *See* Wolff (Slate), *supra* note 90.

User security may take a more serious form if the target is a life-sustaining IoT device such as the pacemaker. In fact, security researchers revealed recently that pacemakers have 19 security vulnerabilities and are plagued with as many as 8,600 security flaws.[105] In addition, security researchers were able to hack into insulin pumps and disable their medicine delivery settings.[106] Potentially, a hacker exploiting one or more of these vulnerabilities could cause a life-threatening situation, ranging from a serious bodily harm to the user or, in extreme situations, even death.[107]

Vulnerable IoT devices could also be used to access the network through which they connect to the Internet, which would expose other devices on the network to potential compromise. Even if a specific vendor employs the strictest security features for their IoT devices, that would not necessarily protect *all* IoT devices within a household, as there are many vendors with varying degrees of IoT security implementations.[108] This is analogous in a way to the Target breach, which surprisingly was directed not at Target's computer network but rather at a contractor who had weaker data-protection standards. That hack resulted in forty million credit cards being stolen in one of the biggest data breaches in recent years.[109]

The bottom line is that a compromise to user security can range in its effects from inconvenience, such as the device being slowed

---

[105] See Swati Khandelwal, *Over 8,600 Vulnerabilities Found in Pacemakers*, THE HACKER NEWS (Jun. 5, 2017), http://thehackernews.com/2017/06/pacemaker-vulnerability.html. *See also* Keith Collins, *Pacemakers Have Thousands of Vulnerabilities Hackers Can Exploit, Study Finds*, QUARTZ (June 3, 2017), https://qz.com/997803/pacemakers-have-thousands-of-vulnerabilities-hackers-can-exploit-study-finds/.

[106] *See* FTC IOT REPORT, *supra* note 6, at 12.

[107] *See* Lily Newman, *Medical Devices Are The Next Security Nightmare*, WIRED (Mar. 2, 2017), https://www.wired.com/2017/03/medical-devices-next-security-nightmare ("That in turn could mean the theft of sensitive medical records, or a devastating ransomware attack that holds vital systems hostage until administrators pay up. 'The entire extortion landscape has changed,' says Ed Cabrera, chief cybersecurity officer at the threat research firm Trend Micro. 'You do get into this life or death situation potentially.'").

[108] *See* Poudel, *supra* note 7, at 1015.

[109] Paul Ziobro, *Target Breach Began with Contractor's Electronic Billing Link*, WALL ST. J. (Feb. 6, 2014). *See also* Brian Krebs, *Email Attack on Vendor Set Up Breach at Target*, KREBS ON SECURITY (Feb. 14, 2014), https://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target.

down, to complete disruption of the device, to a life-threatening situation, depending on the targeted device, motivation, and the method of exploitation employed.

3. *Third-Party Security*

The proliferation of IoT creates an environment of potentially millions of vulnerable devices. This enables hackers to create enslaved IoT devices that can be used as a proxy for attacking third parties – commonly referred to as "botnets."[110] Botnets are essentially armies of Internet-connected devices compromised through a malware that infects them and allows the attacker (the "bot master") to command that group of devices. The most intuitive form of third-party security risk due to IoT botnets is a DDoS attack. The key in a DDoS attack (as opposed to a DoS attack) is in the overwhelming volume of requests, which essentially shuts down the target due to its unavailable bandwidth for responding to legitimate requests of service.

In October 2016, a malware named Mirai created a botnet out of a hundred thousand compromised IoT devices used it to mount a DDoS attack against a Domain Name System (DNS) service provider, Dyn.[111] DNS is the basic protocol that translates alphanumerical addresses (www.nytimes.com, for example) to numerical IP addresses (like 192.168.1.182), which are then translated into a computer's binary language in blocks of eight bits (11000000 10101000 00000001 10110110). The Internet's TCP/IP protocol works with binary addresses, which it "understands," whereas alphanumerical addresses are a convention that enables humans to conveniently browse the Internet without having to memorize a list of numerical IP addresses. This structure is an easy target for a malicious actor who wishes to shut down portions of the World Wide Web and make it impossible for the average user to access websites and services online.

II. THE SECURITY RESEARCH ENVIRONMENT

[110] A botnet that recently caused significant unrest is Mirai, which is also the name of the malware that allowed the organization of this botnet. *See* Lily Hay Newman, *The Botnet That Broke the Internet Isn't Going Away,* WIRED (Dec. 9, 2016), https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away.

[111] *See* Dyn Statement, *supra* note 18.

In cybersecurity, it is essential to understand the enemy in order to resolve the threats and challenges that exist largely due to certain forms of hacking. Hacking tends to have a negative connotation – it frequently implies malevolent, possibly illegal, activity in relation to computers and networks.[112] But hacking culture is more diverse than that. Criminally motivated hackers, or "black hat hackers," are only a subset of the larger group of hackers – in fact, a tiny proportion, only about 1%.[113] Hackers tend to have different motivations, purposes, and incentives, ranging from seeking a thrill or challenge, or resolving and fixing vulnerabilities, to extorting a user, disrupting the functioning of computers and networks, stealing data and credentials, and potentially selling the data or vulnerabilities in a designated marketplace on the Internet.

Similarly, people tinker with their devices for a variety of reasons – for fun, to study, or to fix vulnerabilities and weaknesses, but also for criminal and destructive purposes.[114] More importantly, hackers have a clear advantage over vendors when it comes to finding vulnerabilities.[115] While a vendor may be focused on other tasks, hackers can dedicate their time to further study a specific system and identify its flaws. Hackers also tend to have the cutting-edge knowledge that allows them to reveal vulnerabilities in creative ways. Considering that it is far easier to attack than to defend in cyberspace – the attacker needs to know of only one vulnerability, while the defender has to defend against all possible attacks – provides yet another argument in favor of ethical hacking for security purposes.[116] Efficient cyber-defense strategies, therefore, have to rely on a robust cybersecurity research environment, which involves hacking.[117]

---

[112] *See* Cassandra Kirsch, *The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law*, 41 N. KY. L. J. 383, 385 (2014) (explaining that "not all hacking is created equal").

[113] *See* Robert Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J. L. & PUB. POL'Y 283, 296 (2006).

[114] *See* Samuelson, *supra* note 10, at 564. *See also* William W. Fisher III, *The Implication for Law of User Innovation*, 94 MINN. L. REV. 1417, 1455–72 (2010).

[115] *See* Bambauer, *supra* note 34, at 1062.

[116] *See* LILLIAN ABLON ET AL., MARKETS FOR CYBERCRIME TOOLS AND STOLEN DATA: HACKERS' BAZAAR 31 (2014).

[117] *See* Kesan, & Hayes, *supra* note 73, at 786.

This section will explain the three main categories of hackers, which may assist in the further analysis of the "freedom to hack." These categories are typically assigned a color – white, gray, or black. These colors reflect the morality of the hacking – which may also suggest its legality, though the two are not mutually dependent.[118] As this section demonstrates, the boundary between legitimate and illegitimate hacking is somewhat fuzzy,[119] given that both ethical and criminal hackers are utilizing the same techniques, and at first blush, in the absence of context, it is hard to differentiate between the two.[120] Law enforcement and courts are not always well equipped to make this normative determination,[121] and this Article therefore argues that differentiating between ethical and unethical hackers depends on whether the hacker in question exploited a vulnerability and whether procedures of vulnerability disclosure were followed. This will be further discussed in Section IV.

a. White Hat

White-hat hackers are security researchers whose main motivation is to improve software and hardware by revealing vulnerabilities and security flaws and disclosing them in a way that will ensure they are patched. White-hat hackers, when not employed by the vendors themselves, are motivated only sometimes by financial gain (the expectation of being monetarily rewarded); more often they are motivated by the challenge, or by the genuine belief that improving the quality of software and hardware will make Internet security stronger.

For an illustration of how white hats are improving the security of the broader Internet infrastructure, we can look to Mike Lynn, a security researcher then affiliated with Internet Security Systems, who discovered a serious software flaw in Cisco's

---

[118] *See* Kesan & Hayes, *supra* note 73, at 769–70 (suggestingethics and morality axes for hackers).

[119] *See* Thompson, *supra* note 13, at 556.

[120] *See* Nancy Gohring, *Digital Vigilantes: Hacking for a Good Cause*, PCWORLD (Dec. 25, 2007), http://www.pcworld.com/article/140731/article.html (explaining how a Trojan horse was used to uncover child-porn activities).

[121] In section IV, I will propose certain recommendations that could alleviate some of the difficulties introduced in the current section.

routers.[122] Although Lynn reported the vulnerability to Cisco, he was still threatened with legal action because he planned on presenting some of the information to his peers at a security conference.[123] The gravity of this flaw was characterized then as a ticking bomb endangering the very backbone of the Internet.[124]

Certain commentators believe that the notion separating white hats from other hackers is that white hats act under authorization.[125] Another distinction made in literature is based on disclosure: hackers disclosing vulnerabilities directly to the vendor are white hats, while those who publicize vulnerabilities to the broader public are considered gray or black hats.[126]

Given that white hats' motivation is primarily the drive to enhance security, it seems unreasonable to subject these individuals to legal liability, assuming that cybersecurity is in the interest of the broader public and possibly the international community. It would be best, therefore, to define white hats as hackers who seek to improve security while minimizing possible harm to the vulnerable target by neither exploiting the vulnerability nor selling it to malicious actors.[127]

b. Black Hat

Black-hat hacking is the exact opposite of the white-hat approach. Indeed, black hats are hackers motivated by mischief or profit rather than by actually fixing vulnerabilities and security flaws.[128] The ability to anonymize one's identity on the Internet allows for the proliferation of black hat hackers (or "cybercriminals"), which lowers the risks of detection and

---

[122] *See* Bambauer, *supra* note 34, at 1053.

[123] Bruce Schneier, *Cisco Harasses Security Researcher*, SCHNEIER ON SECURITY (July 29, 2005), http://www.schneier.com/blog/archives/2005/07/cisco_harasses.html.

[124] *See* Kim Zetter, *Router Flaw Is a Ticking Bomb*, WIRED (Aug. 1, 2005), https://www.wired.com/2005/08/router-flaw-is-a-ticking-bomb.

[125] *See* Thompson, *supra* note 13, at 557.

[126] *See* Thompson, *supra* note 13, at 557.

[127] *See* Thompson, *supra* note 13, at 558.

[128] Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud & Abuse Act*, 18 BERK. TECH. L. J. 909, 919-921 (2003).

prosecution compared to the physical world.[129] Data suggest that law enforcement is usually reluctant to investigate, apprehend, and prosecute cybercriminals, given that hackers often reside overseas, which presents challenges with regard to jurisdiction and gathering evidence.[130]

Certain commentators make the argument that even though black hats are essentially cybercriminals, the law should still allow them to operate freely, since they can expose flaws and vulnerabilities that could have been exploited in more harmful ways, such as through terrorism or state-sponsored attacks.[131] However, the analysis in this Article will exclude black-hat hackers, since their primary intention is not enhancing security.

c. Gray Hat

Hackers' ethics and motivations are not binary but rather could be placed somewhere on the black–white continuum. The gray area in which hackers operate with unclear motivations is fittingly labeled as "gray hat."[132] As an example, gray hats will still identify vulnerabilities, but, rather than disclosing them to the vendor, they might sell them to governments, intelligence agencies, or law enforcement authorities.[133] The buyer, in turn, uses the vulnerability for a variety of purposes, such as for espionage, military, or law enforcement ends.[134] The primary intention of gray hats is not necessarily enhancing security, although that could be one motivation – it is the desire to monetize vulnerabilities by selling them to official entities other than the vendor. It is difficult to tell whether gray hats are included or excluded from the scope of the argument in this Article, since that largely depends on their

---

[129] *See* Thompson, *supra* note 13, at 548.

[130] Susan Brenner, *Cybercrime Metric: Old Wine, New Bottles?* 9(13) VA. J. L. & TECH. 6–11 (2004).

[131] *See* Anonymous, *supra* note 15 (noting that "cybercrime can expose security flaws that, if fixed, can prevent more devastating").

[132] *See generally* SHON HARRIS, GRAY HAT HACKING THE ETHICAL HACKERS HANDBOOK (2008).

[133] *See* Kim Zetter, *Hacker Lexicon: What Are White Hat, Gray Hat, and Black Hat Hackers?* WIRED (Apr. 13, 2016), https://www.wired.com/2016/04/hacker-lexicon-white-hat-gray-hat-black-hat-hackers.

[134] *See* Zetter (Hacker Lexicon), *supra* note 133.

motivations and the precise nature of their activities. But assuming the gray-hat hacker in question follows the procedure of vulnerability disclosure and minimization of harm to third parties, they ought to be in the clear in terms of legal liability.

d. The Vulnerability Market

When considering a freedom to hack, it is also important to understand the incentives and realities of the "black-hat" vulnerability market.[135] In this market, hackers sell what are typically known as "zero-day exploits," meaning that vendors are unaware of these vulnerabilities in their systems, and therefore the chance of them getting patched is relatively low.[136] Governments, intelligence agencies, militaries, and cybercriminals find this black market for vulnerabilities very appealing, and hackers who end up selling vulnerabilities on that market believe that they are better off doing so rather than disclosing them to the respective vendor.[137]

In the digital era, knowing of a vulnerability can be either a weapon or a shield. Legalizing ethical hacking could be an incentive to use that knowledge as a shield while reducing the likelihood that researchers will sell vulnerabilities on the black market. In many respects, the legal challenges demonstrated in Section III of this Article create an incentive for researchers to sell vulnerabilities on the black market, rather than to disclose them to the relevant parties, for fear of legal jeopardy.[138] The result makes individual users less safe and creates a serious danger to the Internet as a whole, considering that critical infrastructure and other public services may be running software with exploitable vulnerabilities of which the vendor has no knowledge.

At the same time, there are white-hat vulnerability markets, which are often referred to as "bug bounty" programs, facilitated by the vendors themselves. These markets create incentives for security researchers by offering monetary rewards for reports of

[135] Bruce Schneier, *The Vulnerabilities Market and the Future of Security*, FORBES (May 30, 2012), https://www.forbes.com/sites/bruceschneier/2012/05/30/the-vulnerabilities-market-and-the-future-of-security/#696438d77536.

[136] Andy Greenberg, *New Dark-Web Market is Selling Zero-Day Exploits to Hackers*, WIRED (Apr. 17, 2015), https://www.wired.com/2015/04/therealdeal-zero-day-exploits.

[137] *See* Bambauer, *supra* note 34, at 1067.

[138] *See* Bambauer, *supra* note 34, at 1054.

vulnerabilities made directly to the vendors under predetermined conditions. Their purpose is to create a greater incentive for security researchers to cooperate with vendors in order to prevent vulnerabilities from being sold to potentially malicious actors – criminal hackers and hostile governments.[139]

e. Accountability in the IoT Industry

Allowing ethical hackers to freely snoop for vulnerabilities and flaws could facilitate a more accountable IoT industry: manufacturers will patch reported vulnerabilities and attempt to improve their products in a way that provides reasonable security, and therefore data privacy, in order to avoid negative publicity. The ethical hacking community is usually ahead of regulatory efforts to set standards for industries, which potentially allows for a more efficient and informed security atmosphere.

Regulatory agencies are slowly beginning to realize the immense potential of exposing IoT vulnerabilities with the help of the hacker community. This allows the industry to patch vulnerabilities before malicious actors can exploit them for criminal, political, or challenge-driven ends. The FTC has recently announced an IoT challenge to "combat security vulnerabilities in home devices,"[140] offering a monetary reward for a tool that would enhance IoT security in the form of a "physical device that the consumer can add to his or her home network that would check and install updates for other IoT devices on that home network, or it might be an app or cloud-based service, or a dashboard or other user interface."[141] However, this effort is still not actively encouraging ethical hacking; rather, it encourages innovation. At the same time, the FTC has also become an enforcer of cybersecurity and privacy,

---

[139] *See* Jay Kesan & Carol Hayes, *Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities*, 58 ARIZ. L. REV. 753, 759 (2016) (creating a distinction between white, black, and gray vulnerability markets).

[140] *See FTC Announces Internet of Things Challenge to Combat Security Vulnerabilities in Home Devices*, FEDERAL TRADE COMMISSION (Jan. 4, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-announces-internet-things-challenge-combat-security.

[141] *See* FTC Challenge to Combat Security Vulnerabilities in Home Devices, *supra* note 140.

under Section 5(a) of the FTC Act.[142] In the future, the FTC may play an active part in ensuring that vendors address vulnerabilities reported to them in a reasonable and timely manner.

III. THE FREEDOM TO HACK

Individuals tinker with their devices for many reasons, including for the challenge, to learn how the system works, or for diagnostic and repair purposes.[143] The freedom to tinker is important for innovation and creativity, and, as the next sub-sections will analyze, for the enhancement of security. Ensuring more ownership rights to consumers of otherwise copyrighted objects is not only a legalistic concept but an actual advocacy movement. For example, the Electronic Frontier Foundation (EFF), a nonprofit organization, is a strong proponent of a broad right to tinker, giving consumers more flexibility and autonomy and protecting civil liberties in the digital world. The ideology behind the movement is the belief that technology helps develop and protect civil rights and liberties like freedom of expression, privacy, and activism.[144]

Edward Felten notes that tinkering is not only a natural part of property rights, which the owner possesses, but an exercise in defining the relationship between the user and digital devices as "our experience is mediated through these devices."[145] Although tinkering is seemingly intuitively part of ownership, it has largely not been formally legally recognized.[146] When the law has addressed tinkering, it has mostly been framed under the "permission culture," which permits tinkering only under very limited and narrow

---

[142] 15 USC §45(a)(1). *See generally* Chris Jay Hoofnagle, *FTC Regulation of Cybersecurity and Surveillance*, *IN* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW (David Gray and Stephen Henderson, eds.) (Cambridge University Press 2017).

[143] *See* Samuelson, *supra* note 10, at 564.

[144] *See About EFF*, https://www.eff.org/about.

[145] Edward Felten, *The New Freedom to Tinker Movement*, FREEDOM TO TINKER (Mar. 21, 2013) https://freedom-to-tinker.com/2013/03/21/the-new-freedom-to-tinker-movement.

[146] *See* Andrew Torrance & Eric Von Hippel, *The Right to Innovate*, 2015 MICH. ST. L. REV. 793, 802. *See also* Samuelson, *supra* note 10, at 566.

circumstances.[147] Any deviation from this has generally been considered a prohibited criminal activity.[148]

Court cases on the freedom to tinker reach as far as the U.S. Supreme Court, which, in the recent *Impression Products v. Lexmark International*, allowed consumers to tinker with and reuse their printer cartridges without facing patent infringement charges, highlighting that this freedom is part of "the rights that come along with ownership"[149] and that "the buyer is free and clear of an infringement lawsuit" in such circumstances.[150]

Many have been advocating for a broad freedom to tinker with otherwise copyright-protected hardware and software. The EFF and other non-profit organizations have long pushed for a right to tinker with rightfully owned hardware and software, framing it as a broader "digital freedom."[151] In the past, consumers could reverse-engineer and research their devices, but nowadays, Section 1201 of the DMCA, which prohibits circumvention of Technical Protection Measures (TPMs), as well as the Computer Fraud and Abuse Act (CFAA) and wiretap laws have hampered that ability.[152]

The freedom to tinker encompasses many dimensions – it allows for the intellectual freedom to learn more about different objects in our lives.[153] In this Article, I wish to introduce a subset of the freedom to tinker – *the freedom to hack.*

By *freedom to hack*, I mean that the law, along with the institutions that interpret, apply, and enforce it, should recognize the benefits of security research (or ethical hacking). This mostly includes research into vulnerabilities in software, hardware, and networks with the intent of fixing these flaws and making the system

---

[147] *See* Felten (Movement of Freedom to Tinker), *supra* note 145.

[148] *See* Samuelson, *supra* note 10, at 566.

[149] *Impression Products* v. *Lexmark International*, 581 U.S. __ (2017).

[150] *Impression Products* v. *Lexmark International*, 581 U.S. __ (2017).

[151] Kit Walsh, *Digital Freedom Depends on the Right to Tinker*, ELECTRONIC FRONTIER FOUNDATION (Jan. 20, 2016), https://www.eff.org/deeplinks/2016/01/why-owning-your-stuff-means-owning-your-digital-freedom.

[152] *See* Walsh, *supra* note 151.

[153] *See* Samuelson, *supra* note 10, at 565.

less susceptible to malicious hacking and more secure overall. Therefore, to some extent, security researchers or hacking-savvy individuals should be able to hack and snoop for vulnerabilities and weaknesses in order to make computer systems and networks stronger by exposing these flaws. There is an ongoing debate over how to disclose vulnerabilities and software flaws, and I will discuss it further in Part IV of this Article.

The freedom to hack, only a small part of the freedom to tinker, focuses on one important dimension – the right to expose and disclose vulnerabilities to the vendor without being subjected to civil or criminal penalties. This does not entail an *unrestricted* right to hack. The law will still have to restrict hacking that causes serious harm to third parties (such as privacy violations), which should be treated under a criminal liability regime[154] or tort law.[155] Rather, there should be an intellectual freedom to use methods of hacking to fix and improve software and hardware, with a robust distinction between constructive and destructive (i.e., exploitative) hacking.[156]

Many tech companies, and even governmental authorities, actively encourage ethical hacking of their systems and provide what are referred to as "bug bounties," through which they invite hackers to test their systems for vulnerabilities and to report any possible flaws in exchange for monetary compensation.[157] However,

---

[154] *See* Samuelson, *supra* note 10, at 567.

[155] *See* Art. 652B of the 2nd Restatement of the Law on Torts (1977) ("One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."). *See generally* Art. 652D ("[O]ne who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."); Alexander Tran, *The Internet of Things and Potential Remedies in Privacy Tort Law*, 50 COLUM. J. L. SOC. PROB. 263, 265 (2017) (where author argues common law privacy torts, particularly "disclosure of private facts" and "intrusion upon seclusion," could provide some remedy to the privacy harms enabled by the IoT ecosystem).

[156] *See* Samuelson, *supra* note 10, at 566 ("a right to repair that which is broken and make other uses of artifact as long as one is not harming the interests of others) p. 568.

[157] *See, e.g.*, *Google Vulnerability Reward Program (VRP) Rules*, GOOGLE https://www.google.com/about/appsecurity/reward-program (providing the list of potential vulnerability types and their respective compensation, e.g., Google will pay $31,337 for a remote code execution type of vulnerability, if disclosed

there are still certain boundaries imposed by bug bounty programs in terms of what activities are allowed and prohibited.[158] Even when no compensation is guaranteed, or no official bug bounty program is in place,[159] many individual security researchers still engage in bug hunting for a variety of reasons.[160] This leads to some serious tensions. Not all tech companies encourage an active hunt for bugs in their software, and some would even be quite unwelcoming of any vulnerabilities reported, whether due to reputational or cost-associated reasons,[161] and might claim such vulnerability collection to be in violation of the law.[162]

With regard to possible circumvention liability, DMCA prohibits circumvention of TPMs in copyrighted software, thus possibly exposing security researchers to liability. At the same time, with regard to criminal liability, the CFAA contains a fair number of ambiguous concepts in relation to hacking that, if interpreted in a

---

according to the program's rules). *See also* Microsoft Security TechCenter, *Microsoft Bounty Programs*, https://technet.microsoft.com/en-us/library/dn425036.aspx (offering specific bug bounty programs to security researchers); G. Burningham, *The Rise of White Hat Hackers and the Bug Bounty Ecosystem*, NEWSWEEK (Jan. 31, 2016), http://www.newsweek.com/2016/02/12/white-hat-hackers-keep-bug-bounty-421357.html.

[158] *See* Kirsch, *supra* note 112, at 397 (quoting Google's vulnerability disclosure program, which requires that "testing must not violate any law, or disrupt or compromise any data that is not your own").

[159] Many companies do not have a vulnerability disclosure program. *See* Kirsch, *supra* note 112, at 398.

[160] *See* Bambauer, *supra* note 34, at 1066 (listing reasons for security researchers engaging in vulnerability hunting – "possible future remuneration, intellectual satisfaction, peer recognition, ideological commitment, animus toward a particular vendor, and expectations in a larger community of testers").

[161] *See* Bambauer, *supra* note 34, at 1065.

[162] *See* Jack Detsch, *Influencers: Antihacking Law Obstructs Security Research*, THE CHRISTIAN SCIENCE MONITOR (July 14, 2016), *available at* https://www.csmonitor.com/World/Passcode/Passcode-Influencers/2016/0714/Influencers-Antihacking-law-obstructs-security-research (comparing companies with established bug bounty programs to those who opted to use the CFAA as a weapon against security researchers, providing the example of Justin Shafer, who was arrested by the FBI for allegedly discovering a vulnerability in dental office management software, allowing access to the information of 22,000 patients, with the vendor arguing that Shafer's actions violated the CFAA).

certain light, could expose legitimate security researchers to legal jeopardy. Both the DMCA and CFAA challenges will be further discussed in the following two sub-sections.

a. The Digital Millennium Copyright Act (DMCA)

Computer software, just like any other creative work, is protected under copyright law.[163] In 1998, Congress enacted the DMCA, creating a legal barrier for tinkerers. The DMCA implemented the World Intellectual Property Organization (WIPO) treaties by creating a legal regime against circumvention of TPMs,[164] protecting copyrighted works through the criminalization of circumvention of these measures.[165]

Subsection 1201(a)(1)(A) of the U.S.C. reads, "No person shall circumvent a technological measure that effectively controls access to a work protected under this title."[166] In this way, Section 1201 restricts legitimate users from controlling their devices, since the IoT environment is ultimately a collection of devices running on copyrighted software. This would mean that smart vehicles, pacemakers, insulin pumps, thermostats, and any other IoT devices are covered by the Section on anti-circumvention, unless an explicit exemption is provided by the DMCA, as discussed below.

Realizing that an absolute exclusion of the right to tinker is unreasonable with respect to digital works, the DMCA also provides certain exemptions from infringement liability, which will be discussed in the following sections. Initially, however, the DMCA provided a very narrow exemption from copyright infringement for

[163] *See* Samuelson, *supra* note 10, at 581.

[164] *See* Executive Summary Digital Millennium Copyright Act (Section 104 Report), *available at* https://www.copyright.gov/reports/studies/dmca/dmca_executive.html. Also, for an elaborate analysis on the meaning of TPMs, see Ryan Iwahashi, *How to Circumvent Technological Protection Measures without Violating the DMCA: An Examination of Technological Protection Measures under Current Legal Standards*, 26 BERK. TECH. L. J. 491 (2011).

[165] *See* Samuelson, *supra* note 10, at 581.

[166] *See* 17 U.S. Code § 1201(a)(1)(A).

reverse-engineering of software for the purposes of interoperability,[167] encryption research,[168] and security testing.[169]

In addition to the DMCA, users often agree to certain "terms of service,"[170] which create a contractual obligation vis-à-vis the software or hardware vendor, creating another hurdle for users and, therefore, security researchers.[171] This private ordering restricts security researchers because it grants vendors legal tools to stifle security research, or any sort of tinkering with their products, purely for business reasons, trumping any security concerns.[172]

In 2002, for example, HP was allegedly the first company to use the DMCA as a weapon against security researchers.[173] HP threatened to file a lawsuit against software security company SnoSoft, which had identified a security flaw in HP's Tru64 operating system. HP threatened the researchers by noting that they "could be fined up to $500,000 and imprisoned for up to five

---

[167] *See* 17 U.S. Code § 1201(f)(1) ("Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.").

[168] *See* U.S.C. § 1201(g) ("[I]it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research.").

[169] *See* U.S.C. § 1201(j) ("[It] is not a violation of that subsection for a person to engage in an act of security testing." However, this exemption differs from the newly adopted security research exemption, since it required "authorization from the owner or operator" of the computer that was accessed.).

[170] The government has previously argued that violating Terms of Service ought to be considered a violation of the CFAA, since it is construed as "unauthorized access." *See* United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

[171] *See* U.C. Berkeley School of Information Report, *supra* note 33, at 8–9.

[172] *See* U.C. Berkeley School of Information Report, *supra* note 33, at 8–9.

[173] *See* Declan McCullagh, *Security Warning Draws DMCA Threat*, CNET (Aug. 1, 2012), https://www.cnet.com/news/security-warning-draws-dmca-threat.

years"[174] under the DMCA.[175] Eventually, HP had to back down from this threat, due to public scrutiny.[176] Since then, the DMCA has been used against *academic* researchers, such as when the Recording Industry Association of America (RIAA) threatened Professor Edward Felten. Felten's paper dealt with breaking the Secure Digital Music Initiative (SDMI) and incited the RIAA to demand that Felten withdraw his paper from a conference. Felten ultimately did so.[177] Felten is just one example of many researchers who, after disclosing vulnerabilities, receive cease-and-desist letters from companies with threats of legal action and explicit demands to discontinue any further security research due to the alleged illegality of the act.[178]

1. The DMCA Exemption for Security Research

Copyright (or the right to exclude tinkerers) is not an absolute legal concept, and certain interests, such as security and privacy, should prevail when balanced against the need to protect the rights of copyright owners.[179] Therefore, the Library of Congress (LoC) has a routine procedure – the triennial review – to assess whether certain exemptions from copyright (and criminal) liability are required in order to ensure that other important interests are fulfilled.[180] Before discussing the specific exemption within the DMCA relevant to IoT, it is essential to understand the triennial

[174] *Id.*

[175] John Leyden, *HP Withdraws DMCA Threat*, THE REGISTER (Aug. 2, 2002), https://www.theregister.co.uk/2002/08/02/hp_withdraws_dmca_threat.

[176] *Id.*

[177] *See* Freeman, *supra* note 289, at 129.

[178] *See* Zack Whittaker, *PwC Sends 'Cease and Desist' Letters to Researchers Who Found Critical Flaw*, ZDNET (Dec. 12, 2016), http://www.zdnet.com/article/pwc-sends-security-researchers-cease-and-desist-letter-instead-of-fixing-security-flaw/.

[179] *See* Helen Nissenbaum, *Where Computer Security Meets National Security*, 7 ETHICS OF INFORMATION TECHNOLOGY 61, 62 (2005) ("Security deserves a place alongside privacy, intellectual property, equity, and other values that have been vigorously debated in light of developments in and application of digital electronic information technologies.")

[180] *See* Arielle Singh, *Agency Regulation in Copyright Law: Rulemaking Under the DMCA and Its Broader Implications*, 26 BERK. TECH. L. J. 527, 529 (2011) ("When Congress drafted the DMCA, it recognized that it could not predict the future technology landscape, and therefore, included the rulemaking process in the statutory scheme to create flexibility").

process, as well as how the world of copyright slowly creeps into other territories, such as information security.

The DMCA created a procedure of triennial review so that potential exemptions to the DMCA could be proposed by the broader public.[181] Parties can claim that they are adversely affected by the DMCA's anti-circumvention rule, and, after public hearing and comment, the Registrar of Copyrights submits recommendations to the Librarian of Congress, who then determines whether to approve the proposed exemptions to the rule.[182] For example, the Librarian has to assess, among other things, "the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research"[183] and "such other factors as the Librarian considers appropriate."[184] In other words, the DMCA does not directly prescribe security as part of what the Librarian has to consider when recognizing new exemptions, but it gives the Librarian broad discretion.

---

[181] *See* 17 U.S.C. § 1201(a)(1)(C) ("[T]he Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation, shall make the determination in a rulemaking proceeding for purposes of subparagraph (B) of whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition under subparagraph (A) in their ability to make noninfringing uses under this title of a particular class of copyrighted works. In conducting such rulemaking, the Librarian shall examine—

(i) the availability for use of copyrighted works;

(ii) the availability for use of works for nonprofit archival, preservation, and educational purposes;

(iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;

(iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and

(v) such other factors as the Librarian considers appropriate.").

[182] *See* 17 U.S.C. § 1201(a)(1)(C).

[183] *See* 17 U.S.C. § 1201(a)(1)(C)(iii).

[184] *See* 17 U.S.C. § 1201(a)(1)(C)(v).

In 2015 the LoC authorized an exemption that was no less than a breakthrough for the computer security community.[185] The exemption reads as follows:

> (i) Computer programs, where the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates solely for the purpose of good-faith security research and does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986, as amended and codified in title 18, United States Code; and provided, however, that, except as to voting machines, such circumvention is initiated no earlier than 12 months after the effective date of this regulation, and the device or machine is one of the following:
>
> (A) A device or machine primarily designed for use by individual consumers (including voting machines);
>
> (B) A motorized land vehicle; or
>
> (C) A medical device designed for whole or partial implantation in patients or a corresponding personal monitoring system, that is not and will not be used by patients or for patient care.[186]

In addition to what could be considered an IoT device – a "device or machine designed to be used by individual consumers" – the exemption adds two standalone categories: motorized land vehicles and medical devices.

These two sub-categories are there for a reason. Any flaws and vulnerabilities in these two types of devices could potentially be deadly or at least pose a serious danger to the safety of their users.[187]

---

[185] *See* Jack Detsch, *The Legal Exemption Making Life Easier For Ethical Hackers*, THE CHRISTIAN SCIENCE MONITOR (Dec. 7, 2016), https://www.csmonitor.com/World/Passcode/Security-culture/2016/1207/The-legal-exemption-making-life-easier-for-ethical-hackers.

[186] 37 CFR § 201.40 - Exemptions to prohibition against circumvention, § 201.40 (b)(7).

[187] The FDA in its premarket cybersecurity guidelines for medical devices categorizes five types of risks – negligible (inconvenience or temporary discomfort); minor (results in temporary injury or impairment not requiring professional medical intervention); serious (results in injury or impairment requiring professional medical intervention); critical (results in permanent impairment or life-threatening injury), and; catastrophic (results in patient death).

Medical devices, including insulin pumps, pacemakers, implantable cardioverter defibrillators, and glucose monitors, are prone to software flaws, posing an actual and immediate danger to the patients using them.[188] Only recently the FDA reported that certain implantable cardiac devices are vulnerable to attacks, which could allow an unauthorized user to control the device and exfiltrate data from it.[189] Surprisingly, medical devices are ridden with vulnerabilities; as already reported, certain insulin pumps[190] and pacemakers[191] are vulnerable to hacking.

Motorized land vehicles are increasingly computerized and connected to the Internet, creating a whole host of vulnerabilities that may be fatal. The automobile industry has yet to realize the many risks associated with such development in the architecture of cars.[192] In fact, *Wired* reported that security researchers were able to hack into the entertainment-system computer of a Jeep, letting hackers command the vehicle – including steering and braking.[193] This led to Chrysler recalling its 1.4 million vulnerable vehicles in order to patch the bug.[194] The fact that smart vehicles often have

---

See Guidance for Industry and Food and Drug Administration Staff - Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, at 17 (Dec. 28, 2016), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf.

[188] Section 1201 Rulemaking: Sixth Triennial Proceeding October 2015 Recommendation of the Register of Copyrights, 378.

[189] FDA, *Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication*, (Jan. 9, 2017), https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm.

[190] Jim Finkle, *J&J Warns Diabetic Patients: Insulin Pumps Vulnerable to Hacking*, REUTERS (Oct. 4, 2016), http://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L.

[191] *See* Khandelwal, *supra* note 105.

[192] *See* U.C. Berkeley School of Information Report, *supra* note 33, at 3.

[193] Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – With Me in It*, WIRED (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway.

[194] Andy Greenberg, *After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix*, WIRED (July 24, 2015), https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix.

more than a hundred million lines of code strengthens the notion that security research is essential for vehicles.[195]

There are a few shortcomings to this DMCA exemption that could further stifle certain types of security research. While the exemption does give significant leeway to security researchers who circumvent the software of IoT devices designed for "use by individual consumers," it also overlooks an important subgroup of IoT devices – those that are not used by individual consumers, such as those used by the government or by organizations.[196] The DMCA exemption does not give guidance on what constitutes a device used by "individual consumers" except that it includes voting machines within that category. This could potentially stifle security research with regard to devices that were not necessarily designed for individual consumers' use.

i. Good Faith

The DMCA exemption is conditioned upon "good faith," which is tricky to define in the context of security research, particularly on behalf of unaffiliated hackers. The exemption provides that security testing

> . . . means accessing a computer program solely for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability, where such activity is carried out in a controlled environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained

[195] *See* David Zax, *Many Cars Have a Hundred Million Lines of Code*, M.I.T. TECH. REV. (Dec. 3, 2012), https://www.technologyreview.com/s/508231/many-cars-have-a-hundred-million-lines-of-code.

[196] *See* Erik Stallman, *A Qualified Win for Cybersecurity Researchers in DMCA Triennial Rulemaking*, CENTER FOR DEMOCRACY & TECHNOLOGY (Oct. 27, 2015), https://cdt.org/blog/a-qualified-win-for-cybersecurity-researchers-in-dmca-triennial-rulemaking/ (arguing that devices "primarily designed for the use by individual consumers" excludes a significant portion of devices not used by individual consumers).

> in a manner that facilitates copyright infringement.[197]

This requirement limits the security research exemption to circumvention efforts intended for *testing*, *investigation*, and *correction* of vulnerabilities and flaws. It also requires a controlled environment in order to prevent harm to third parties. The information obtained through the security research should be used *primarily* to promote security.

These requirements implicate security research in several ways. First, they exclude security researchers who happen to stumble upon a vulnerability or who identify a possible fix to a flaw without intending to do so. Recently, an "accidental hero" offered a kill-switch to the global ransomware "WannaCry," but according to him finding a solution to WannaCry had not been his intention initially.[198] This could stifle vulnerability reporting by researchers whose intentions at the outset are not to promote security. Second, a the DMCA does not define "controlled environment," therefore potentially excluding security researchers whose environments would not be considered "controlled" and possibly allowing vendors to abuse this requirement against unaffiliated security researchers. The introduction of cloud computing as a central part of the IoT ecosystem is another exacerbating factor to the notion of "controlled environment."[199] Third, the exemption provides that information gathered from exempted security research should be used "primarily" to enhance security and safety. However, this potentially opens the door to security research that crosses from a white- or gray-hat world into black hat-territory, where motivations are usually malicious.[200]

Lastly, these requirements provide a glimpse into the phenomenon of copyright bleeding over into cybersecurity,[201]

---

[197] 17 U.S.C. § 1201(j)(1).

[198] Nadia Khomami & Olivia Solon, *'Accidental Hero' Halts Ransomware Attack and Warns: This Is Not Over*, GUARDIAN (May 13, 2017), https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack.

[199] *See* Bambauer, *supra* note 34, at 1091.

[200] *See* Zetter (*Hacker Lexicon*), *supra* note 133.

[201] *See* Paul Ohm & Black Reid, *Regulating Software When Everything Has Software,* 84 GEO. WASH. L. REV. 1672, 1686 (2016) ("Suddenly, the Copyright

meaning that the requirement is not necessarily in line with the way ethical hackers actually operate in the vulnerability detection space. This is more of an institutional problem, in which the question is whether the organs involved in the DMCA triennial review process are actually well equipped to address the security issues within their purview.

ii. Opposition by U.S. Regulatory Agencies

Agencies who commented on the proposed exemption during the triennial review process had several reservations. While the National Telecommunication and Information Administration (NTIA) supported the aforementioned exemption to the prohibition on circumvention,[202] other agencies, such as the FDA, DOT, and EPA, strongly opposed and had significant reservations to exempting computer programs for good-faith security research.[203] The main thrust of these agencies' argument is that security research into computer programs could actually compromise security and privacy. As certain opponents noted, "'fixing' of medical devices without FDA or manufacturer permission would risk patient safety because it would 'enable others to bypass proper regulatory controls.'"[204]

The FDA, for example, opposed the exemption because every medical device has to undergo FDA pre-market approval,[205]

Office found itself at the center of a full[-]fledged, multiagency debate over the extent to which code regulation might be necessary not just for copyright policy reasons, but for environmental, traffic, health, and various other noncopyright policy reasons as well.").

[202] *See* Sixth Triennial Section 1201 Rulemaking – Recommendations of the National Telecommunications and Information Administration to the Register of Copyrights (Sept. 18, 2015), https://www.copyright.gov/1201/2015/2015_NTIA_Letter.pdf ("[T]o the extent that there is a copyright interest, NTIA believes that security research is noninfringing and constitutes fair use.").

[203] Section 1201 Rulemaking: Sixth Triennial Proceeding October 2015 Recommendation of the Register of Copyrights, p. 313.

[204] Section 1201 Rulemaking: Sixth Triennial Proceeding October 2015 Recommendation of the Register of Copyrights, p. 293.

[205] *See* Guidance for Industry and Food and Drug Administration Staff - Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (Dec. 28, 2016), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf.

and unrestricted meddling with or changes to software in medical devices would put patients "at increased risk from bad faith attempts to modify devices during the period required to develop and obtain [FDA] approval for the change."[206] As a result, the FDA, the agency responsible for the safety and privacy of medical devices, would not be able to support any exemption that would compromise that responsibility.

FDA guidance on Premarket Submissions for Management of Cybersecurity in Medical Devices contains certain suggestions for vendors of medical devices, such as limiting access to trusted users, ensuring trusted content, and planning for detection, response, and recovery from security compromises.[207] However, this guidance is only a recommendation for effective cybersecurity management. Though vendors submitting medical devices for FDA premarket review will want to implement these recommendations to ensure FDA approval, they are by no means legally binding.[208] This demonstrates that even the seemingly strictest agency in terms of IoT security provides only *recommended* guidelines to vendors, highlighting the need for external security research due to the increasing volume of vulnerabilities.[209]

b. The Computer Fraud and Abuse Act (CFAA)

Federal and state statutes have outlawed unauthorized access to computers.[210] While each state statute is slightly different, they all share some basic concepts.[211] The CFAA of 1984 criminalizes

---

[206] Section 1201 Rulemaking: Sixth Triennial Proceeding October 2015 Recommendation of the Register of Copyrights, p. 293.

[207] *See* Guidance for Industry and Food and Drug Administration Staff - Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, at 4 (Oct. 2, 2014), *available at* https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf.

[208] *See* FDA Premarket Content, *supra* note 207, at 2.

[209] *See* FDA, *Cybersecurity* (last updated Mar. 3, 2017), https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm ("This vulnerability increases as medical devices are increasingly connected to the Internet, hospital networks, and to other medical devices.").

[210] ORIN KERR, COMPUTER CRIME LAW 29–30 (3rd Ed., 2012).

[211] *See* Kerr, *supra* note 210, at 30.

certain potentially harmful computer-related activities. Since its enactment, the CFAA has been amended ten times, and each time its scope has been expanded.[212] The CFAA is often said to be one of the most "far-reaching criminal laws in the Unites States Code" due to its broad language and enforcement.[213] This vagueness raises constitutionality questions, particularly in the context of the void-for-vagueness doctrine,[214] exerting "pressure on courts to adopt narrow interpretations of access and authorization."[215] The statute was inspired by the common-law trespass doctrine, which does not always fit perfectly with the realities of the Internet.[216]

The central provision applicable to security research is located in 18 U.S.C. § 1030(a)(2), which deals with unauthorized access to protected computers and criminalizes the obtaining of "information from any protected computer"[217] through intentional access to "a computer without authorization" or exceeding "authorized access."[218] The concepts of "access" and "authorization" have been the subject of substantial debate.[219] This has led to confusion among computer users, security researchers, and even law enforcement.[220] Experts admit that this provision has the lowest thresholds and is therefore applicable to a broad subset of

---

[212] *See* Thompson, *supra* note 13, at 560.

[213] Orin Kerr, *Vagueness and Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1561 (2010).

[214] United States v. Williams, 128 S. Ct. 1830, 1845 (2008) ("Vagueness doctrine is an outgrowth not of the First Amendment, but of the Due Process Clause of the Fifth Amendment. A conviction fails to comport with due process if the statute under which it is obtained fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement.").

[215] *See* Kerr, *supra* note 213, at 1572.

[216] *See* Kirsch, *supra* note 112, at 393.

[217] 18 U.S.C. § 1030(a)(2)(C). The CFAA also prohibits obtaining "information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*)." (18 U.S. Code § 1030(a)(2)(A)] and "information from any department or agency of the United States" [18 U.S. Code § 1030(a)(2)(B)]).

[218] 18 U.S.C. § 1030(a)(2).

[219] *See* Orin Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes,* 78 N.Y.U. L. REV. 1596 (2003).

[220] *See* Kirsch, *supra* note 112, at 392–93.

online activities.[221] It would be outside the scope of this Article to reiterate the debate over the precise contours of authorization and access. The focus would be on how security research is stifled by the prohibition on unauthorized access.

The scope of unauthorized access largely criminalizes *any* instance of interstate hacking[222] and encompasses every Internet-connected device within the scope of "protected computer,"[223] including anything that has a "microchip or that permits digital storage."[224] The CFAA defines "computer" in a broad manner and excludes only a few devices, such as "an automated typewriter or typesetter, a portable hand held calculator, or other similar device."[225] Since some security research requires the use of hacking methods, this overbroad approach stifles research into vulnerabilities in such critical systems as voting machines,[226] resulting in adversaries learning about these vulnerabilities before the vendor can identify them.[227] Even at present, security researchers at the renowned DefCon hacking conference managed

[221] *See* Kerr, *supra* note 210, at 78.

[222] *See* Kerr, *supra* note 213, at 1567.

[223] *See* Kerr, *supra* note 213, at 1571.

[224] *See* Kerr, *supra* note 213, at 1571.

[225] 18 U.S.C. § 1030(e)(1) defines a "computer" as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."

[226] *See* Brian Barrett, *America's Electronic Voting Machines Are Scarily Easy Targets*, WIRED (Feb. 8, 2016), https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election (explaining that vulnerable voting machines are very much a reality, giving the example of WinVote, Virginia's voting machines that were vulnerable to remote hacking – "anyone within a half mile could have modified every vote undetected.").

[227] *See, e.g.*, Zapotosky, Demirijian, *Homeland Security Official: Russian Government Actors Tried To Hack Election Systems In 21 States*, WASHINGTON POST (Jun. 21, 2017), https://www.washingtonpost.com/world/national-security/homeland-security-official-russian-government-actors-potentially-tried-to-hack-election-systems-in-21-states/2017/06/21/33bf31d4-5686-11e7-ba90-f5875b7d1876_story.html.

to hack into several voting machines in less than ninety minutes.[228] This reveals the need to rebalance the goals of criminal law and cybersecurity.

The over-broadness of computer crime statutes is not a problem in only U.S. law; it has also been a matter of concern in security research communities overseas. For instance, in the UK, the Computer Misuse Act of 1990 was recently amended to criminalize the "creation, supply or application of 'hacker tools' for use in computer misuse offences."[229] This has significantly broadened the scope of application of the Act, making ethical hackers concerned about potential legal jeopardy.[230]

The threat posed to security researchers by the CFAA is far from theoretical. In 2002, Bret McDanel, an employee of Tornado Development, Inc., was convicted and sentenced to 16 months in federal prison for disclosing a serious vulnerability in the online-messaging product offered by his employer.[231] At first, McDanel reported the vulnerability to his employer, but the employer never patched it.[232] As a last resort, McDanel e-mailed as many as 5,600 Tornado customers to inform them of the unpatched vulnerability. As a result, the Department of Justice indicted McDanel, arguing that his actions knowingly caused "the transmission of a program, information, code, or command, and[,] as a result of such conduct, intentionally cause[d] damage without authorization[] to a protected computer."[233]

The DOJ has since admitted that prosecuting McDanel was a mistake; it filed a motion to reverse the conviction in the Ninth

---

[228] *See* Adam Lusher, *Hackers Breached Defences of US Voting Machines in Less Than 90 Minutes,* INDEPENDENT (July 31, 2017), http://www.independent.co.uk/news/world/americas/us-politics/us-election-hacking-russia-russian-hackers-cyberattack-donald-trump-voting-machines-def-con-a7868536.html.

[229] STEFAN FAFINSKI, COMPUTER MISUSE – RESPONSES, REGULATION AND THE LAW 76 (2009).

[230] A testimony by UK-based technician read, "That's the end of penetration testing. Why would I risk ending up in jail for doing my job? It's madness. It takes away the incentive for making systems secure and plays right into the hands of criminals." Fafinski, *supra* note 229, at 76.

[231] *See* Freeman, *supra* note 27, at 129.

[232] *See* Freeman, *supra* note 27, at 129.

[233] 18 U.S.C. §1030(a)(5)(A).

Circuit Court of Appeals, noting that his actions had not indicated an intent to harm his employer and could have potentially pressured his employer to fix the vulnerability, thus protecting the privacy of customers using the messaging product.[234] The relationship between *intent* and *harm* is a critical one, since it could exclude security researchers from the scope of the CFAA if unauthorized access can be shown to lack intent to cause harm.[235] Since the CFAA does not require a showing of scienter in relation to the harm, it "overcriminalizes hacking activity that involves mere access and inadvertent minor damage"[236] and "effectively establishes strict liability beyond the intentional access . . . regardless of moral culpability."[237]

However, it is not only hacking that is criminalized; access to portions of the Web that the owner did not design for public access is also generally deemed illegal. These were the facts in *United States v. Aurenheimer*, where the defendant, Andrew Aurenheimer, was charged under the CFAA for "unauthorized access" because he revealed an AT&T-owned URL that contained private account data belonging to as many as 100,000 iPad users.[238] Such an approach to the concept of unauthorized access puts security researchers at risk not only for using hacking techniques but also for pursuing benign activities online that the vendor or owner deems unfriendly. This leads to "authorization," a legal term of art within the CFAA, being de facto defined by tech companies rather

---

[234] *See United States* v. *Bret McDanel*, (Motion for Reversal of Conviction) C.A. No. 03-50135, *available at* http://www.steptoe.com/publications/273a.pdf ("[T]he government believes it was an error to argue that defendant intended an "impairment" to the integrity of Tornado's computer system… instead, the evidence established that defendant informed Tornado's customers --- the people whose data may have been vulnerable to unauthorized access --- about the vulnerability, an action that could have brought about repair of the problem."). Similarly, in *United States* v. *Morris*, Morris argued that he had no intent to cause damage when he created the *Morris* worm, although he did have intent to access a protected computer in an unauthorized manner (the double scienter question) which caused a considerable amount of damage to many computers affected by the Morris worm, *see* United States v. Morris, 928 F.2d 504, 507 (2d Cir. 1991).

[235] *See* Thompson, *supra* note 13, at 562.

[236] *See* Thompson, *supra* note 13, at 562.

[237] *See* Thompson, *supra* note 13, at 568.

[238] *See* United States v. Aurenheimer, No. 11-CR-470, 2012 WL 5389142, at *1 (D.N.J. Oct. 26, 2012).

than by Congress, courts, or law enforcement authorities.[239] This problematic breadth is paired with outdated notions of sentencing, discussed in the following subsection.

1. U.S. Sentencing Guidelines

The U.S. Federal Sentencing Guidelines can provide insight into how courts current approach punishment for computer crimes.[240] The Guidelines provide for harsher punishments for property crimes where the criminal act causes great economic loss.[241] In the context of computer crimes, such a loss includes, among other things, "the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost . . . ."[242] This punishment model does not take into account beneficial security research, and it ignores the far costlier alternative of malicious exploitation of vulnerabilities.[243] Losses also include the cost of patching a vulnerability, which would have taken place even in absence of the crime.[244]

The Guidelines impose still greater punishment if the target computer belonged to critical infrastructure.[245] The exploitation of vulnerabilities in critical infrastructure computers, such as those intended to manage power and gas, transportation, national security, and public health, could result in devastating disruption effects. At the same time, if critical infrastructure and other non-critical

---

[239] *See* Kirsch, *supra* note 112, at 399.

[240] U.S. Sentencing Guideline Manual (2016).

[241] U.S. Sentencing Guideline Manual § 2B1.1(b)(1) (2016).

[242] 2B1.1(3)(v)(III) U.S. Sentencing Guideline Manual § 2B1.1(3)(v)(III) (2016) ("reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service.").

[243] On the lack of instrumentality in the U.S. Sentencing Guidelines, see Anonymous, *Immunizing the Internet, Or: How I Learned to Stop Worrying and Love the Worm*, 119(8) HARV. L. REV. 2442, 2453 (2006) ("[C]urrent U.S. Sentencing Guidelines do not sufficiently take instrumental concerns into account.").

[244] *See* Anonymous, *supra* note 15, at 2454 (citing Creative Computing v. Getloaded.com LLC, 386 F.3d 930, 935–56 (where the court ruled that routine maintenance and updating would be assessed as part of the damages)).

[245] U.S. Sentencing Guidelines § 2B1.1(b)(18)(A).

computers operate on that same vulnerable software, it would be preferable to target the latter from a risk standpoint, however, that is not always possible when critical infrastructure computers operate on their own software and systems.[246] Therefore, the Guidelines should also consider the degree of benefit of the act in question, by comparing it to the full potential of exploiting the vulnerability, which could be far more devastating than the prosecuted crime.[247]

IV. CREATING A SECURE HYPERCONNECTED WORLD THROUGH LAW

If law, and the institutions creating, enforcing, and interpreting it, were to recognize the benefits of ethical hacking, this could help resolve many systematic shortcomings in what experts call the "security theater."[248]

First, incentivizing ethical hackers to report vulnerabilities to the vendor would decrease the overall number of unpatched vulnerabilities, narrowing down the opportunities for adversaries to attack the IoT ecosystem. This could also pressure the IoT industry to create secure devices, as companies will attempt to avoid public shaming based on flaws in their software detected by ethical hackers.[249] This will by no means prevent malicious hacking entirely; it may, however, decrease its likelihood, by increasing the costs associated with mounting a cyber-attack and enabling more targeted and efficient law enforcement efforts to deal with the most serious offenses. This could be achieved through clear distinctions between malicious and benevolent actors and through certain

---

[246] *See* Anonymous, *supra* note 15, at 2456.

[247] *See* Anonymous, *supra* note 15, at 2455 ("[P]unishments should encourage attacks that fall shortest of their full destructive potential, at the very least by taking into account the gap between potential and actual damage during sentencing.").

[248] Similarly, Bruce Schneier refers to a related phenomenon as "security theater," which is "security measures that make people feel more secure without doing anything to actually improve their security." Bruce Schneier, *Beyond Security Theater,* SCHNEIER ON SECURITY (Nov. 2009), https://www.schneier.com/essays/archives/2009/11/beyond_security_thea.html.

[249] Anonymous, *Immunizing the Internet, Or: How I Learned to Stop Worrying and Love the Worm,* 119(8) HARV. L. REV. 2442, 2450 (2006) ("media coverage, user complaints can prompt vendors to take action" otherwise, "vendors would be more complacent").

legislative and administrative adjustments, such as clarification of the boundaries of the CFAA and DMCA in relation to security research.

Second, there should be consensus on how to disclose vulnerabilities in an acceptable manner. At present, the philosophy on disclosure is highly fragmented and context-dependent. In *The Hacker's Aegis*, Derek Bambauer and Oliver Day recommend that security researchers adhere to five rules of thumb, in exchange for immunity from civil liability: report the vulnerability to the vendor first, do not sell it, test on the researcher's own system, do not weaponized it, and create a trail.[250] While these rules are certainly helpful, there is still a need to revisit the fundamental disagreement over disclosure practices.

Finally, allowing security researchers to snoop around for vulnerabilities is insufficient on its own; important modifications should support efforts to patch flaws in software. Such modifications might include requiring that vendors embed built-in *patchability* into IoT devices, using privacy tort law to address potential externalities associated with security research, tackling vendors who employ the "security by obscurity" practice, and empowering the FTC to enforce cybersecurity and vulnerability management practices against rogue vendors. These modifications are required in order to achieve a truly secure IoT ecosystem, one that encourages vendor accountability and cooperation.

a. Distinguishing Malicious from Benign Hackers

The main difficulty with the proposition that security research should not be impeded by legal hurdles is that it is somewhat burdensome to draw a clear line between benign and malicious activities in cyberspace.[251] This difficulty mainly arises because hackers use the same tools regardless of their motives.

---

[250] *See* Bambauer, *supra* note 34, at 1088.

[251] *See generally* Larisa Long, *Profiling Hackers*, SANS Institute InfoSec Reading Room (Jan. 26, 2012), https://www.sans.org/reading-room/whitepapers/hackers/profiling-hackers-33864 ("While the law is clear concerning hacking, the definition gets a bit fuzzy among the general population and even computer professionals. Added into this mix are the Gray Hats, or Ethical Hackers, who blur the line between White and Black.").

There are factors, however, that distinguish between malicious and benign hackers, though they are highly dependent on the specific case and facts in question. It is one thing to discover a vulnerability, and it is quite a different thing to exploit that vulnerability to its full disruptive and destructive potential.[252] The red line here should be focused on weaponization and exploitation – whether the hacker simply identified a flaw and reported it responsibly to the vendor (ethical hacking), or whether she or he exploited it to cause damage (malicious hacking). This is a case-by-case assessment that should focus on whether the hacker used tools and techniques that caused minimal harm given the specific circumstances.

The central part of this assessment is the nature of the vulnerability. Some vulnerabilities allow access to certain protected information; others grant full administrator privileges; and some could even result in malfunction or destruction of the hacked device. The dividing line is between reasonable tools and effects of vulnerability research versus unreasonable techniques that cause damage beyond what is required to identify the flaw.

Weaponization of a vulnerability can indicate that a hacker is motivated not by a desire to fix flaws but rather by a wish to monetize or exploit the vulnerability in a manner that causes damage to the unsecure computer systems and networks and thus violates the law. However, weaponizing a vulnerability (creating a mechanism to exploit the vulnerability) requires a tremendous amount of time and resources, and such a substantial activity would make it easier for law enforcement to determine whether the act in question is malicious or benign, since the effort of weaponizing is not trivial.[253]

Supplementing factors include whether hackers cooperate with law enforcement (if it comes to that), whether they disclose

---

[252] *See* Paul Stockton & Michele Golabek-Goldman, *Curbing the Market for Cyber Weapons,* 32 YALE L. & POL'Y REV. 239, 244 (2013) ("[A]s an alternative to engaging in 'responsible disclosure,' a researcher could instead 'exploit' or weaponize the 0-day vulnerability.").

[253] *See* Paul Stockton, Michele Golabek-Goldman, *Curbing the Market for Cyber Weapons,* 32 YALE L. & POL'Y REV. 239, 245 (2013) (noting that "transforming a vulnerability into a weaponized exploit may require significant investments of time, money, and resources").

their actions and findings to the vendor, and whether they provide as much information as possible to relevant agencies, if needed – for example, reporting a pacemaker vulnerability to the FDA, or using US-CERT as an intermediary in the process. At least one commentator argues that if a security researcher notifies the vendor within 24–48 hours of his or her activities, it should provide a "safe-harbor" in terms of CFAA liability.[254]

b. Legislative and Administrative Efforts to Date

Congress has realized the importance of ethical hacking on many occasions, primarily in proposed legislation initiatives. Recently, the Senate introduced a bipartisan "Internet of Things (IoT) Cybersecurity Improvement Act of 2017" bill, proposing, among other things, to amend the CFAA and DMCA to allow good-faith security research of "Internet-connected device(s)" used by a "department or agency of the United States."[255] The bill expands the notion of security research, which is already part of the DMCA exemption, to IoT devices used by the U.S. government and its agencies, removing the legal barriers if researchers follow a clear set of guidelines.[256] This addresses part of the critique this Article makes of the current DMCA exemption for security research, which excludes a whole subset of Internet-connected devices.

The Bill also requests that IoT contractors certify that their devices do not have any known vulnerabilities and that they are patchable and follow industry-standard protocols.[257] More importantly, the Bill empowers the National Protection and Programs Directorate (NPPD) to create guidelines, in consultation with security researchers, for vulnerability disclosure. At present, and as discussed below, there is no uniform federally mandated vulnerability disclosure procedure, and creating authoritative rules in this area is of the utmost importance.[258] However, this Bill creates

[254] *See* Kirsch, *supra* note 112, at 400.

[255] *See* Internet of Things Cybersecurity Improvement Act of 2017 (hereinafter "IoT Bill") (115th Cong.), https://www.documentcloud.org/documents/3911338-Internet-of-Things-Cybersecurity-Improvement-Act.html.

[256] *See id.* at § 3.

[257] *See id.* at § 3(a)(1)(A)(i).

[258] *See id.* at § 3(b)(1).

only minimal standards of cybersecurity and includes exceptions that still leave many potential gaps.

Additionally, in response to the Jeep hack, the Senate introduced a bill that deals specifically with vehicle security by requiring isolation of critical software systems from other internal networks as well as penetration testing by security analysts and onboard systems to detect malicious activity.[259] Considering that vehicle software may have as many as a hundred million lines of code, substantially more than other software, this vehicle-specific bill makes a lot of sense.[260] This demonstrates the magnitude of potential individuals (and vehicles) affected by unpatched bugs, the fact that it was not the vehicle manufacturer who identified the vulnerability, and that Congress realizes the looming threat of Internet-connected vehicles running flawed software. This has also led the vehicle industry to invest more in cybersecurity efforts. Volkswagen, for example, has established its very own cybersecurity firm with the goal of preventing hacking.[261]

Recently, Congress, realizing how integral ethical hacking is to overall cybersecurity, has attempted to come up with a resolution that proactively promotes ethical hacking,[262] including a bill creating a bug bounty program for vulnerabilities disclosed in a "Hack the Department of Homeland Security" program.[263] Other

---

[259] Security and Privacy in Your Car Act of 2015 (114th Cong.) https://www.congress.gov/bill/114th-congress/senate-bill/1806/all-info.

[260] *See* Gelles, Tabuchi, and Dolan, *Complex Car Software Becomes the Weak Spot Under the Hood,* N.Y. TIMES (Sep. 27, 2015) https://www.nytimes.com/2015/09/27/business/complex-car-software-becomes-the-weak-spot-under-the-hood.html.

[261] Michael Kan, *Volkswagen is Founding a New Cybersecurity Firm to Prevent Car Hacking*, PCWORLD (Sept. 14, 2016), http://www.pcworld.com/article/3120283/volkswagen-is-founding-a-new-cybersecurity-firm-to-prevent-car-hacking.html.

[262] *See* Morgan Chalfant, *Dem Pushes 'Ethical Hacking' Resolution,* THE HILL (July 19, 2017), http://thehill.com/policy/cybersecurity/342803-dem-pushes-ethical-hacking-resolution (Rep. Lou Correa (D-Calif.) introduced a resolution that would allow ethical hackers, who hack into computer networks and systems with the intent of identifying security vulnerabilities without malicious or criminal intent).

[263] *See* Maggie Hassan & Rob Portman, *Why We're Encouraging Ethical Hackers to Try and Hack the Department of Homeland Security*, TIME (Jun. 30, 2017), http://time.com/4837557/hackers-homeland-security-cyber-attacks (arguing that

departments announced similar challenges for private citizens, including the Department of Defense ("Hack the Pentagon"),[264] which also contacted the well-known vulnerability coordination platform HackerOne[265] in order to facilitate a vulnerability disclosure program for private security researchers.[266]

c. Clarifying CFAA and DMCA Boundaries

Clarifying the boundaries of CFAA and DMCA as pertaining to security researchers is immensely important.[267] The CFAA's strict liability for access "without authorization" is certainly a major threat to security researchers. At the same time, it discourages talented researchers from engaging responsibly with vendors. Although there have been many calls to reform the CFAA in recent years,[268] this Article advances a proposal focused on the DOJ, the prosecuting authority of the CFAA. The DOJ already acknowledged in the *McDanel* case that it had erred when it prosecuted an employee exposing a vulnerability in his employer's product.[269] This, however, is only one individual case and does not necessarily provide guidance for potential future prosecutions of security researchers engaged in vulnerability snooping.

"one of the best ways to protect places like DHS is actually to recruit hackers to attempt to hack into its own systems and networks") (citing Hack DHS Act, H.R.2774 (115th Cong.), *available at* https://www.congress.gov/bill/115th-congress/house-bill/2774/text?r=21).

[264] https://www.usds.gov/report-to-congress/2016/hack-the-pentagon/

[265] https://www.hackerone.com/about

[266] *See* HackerOne, *Hack the Pentagon*, https://www.hackerone.com/resources/hack-the-pentagon (noting that the first vulnerability was reported 13 minutes after the launch of the program).

[267] *See* McBoyle v. United States, 283 U.S. 25, 27 (1931), (noting that creation of new crimes requires giving "fair warning . . . in a language that the common world will understand").

[268] *See* Orin Kerr, *Proposed Amendments to 18 U.S.C. 1030*, VOLOKH CONSPIRACY BLOG (Jan. 20, 2013), http://volokh.com/2013/01/20/proposed-amendments-to-18-u-s-c-1030. *See also* Jennifer Granick, *Thoughts on Orin Kerr's CFAA Reform Proposals: A Great Second Step*, STANFORD CENTER FOR INTERNET AND SOCIETY BLOG (Jan. 23, 2013), http://cyberlaw.stanford.edu/blog/2013/01/thoughts-orin-kerrs-cfaa-reform-proposals-great-second-step.

[269] *See* Joseph Menn, *U.S. Admits Convicted Man Is No Hacker*, L.A. TIMES (Oct. 16, 2003), http://articles.latimes.com/2003/oct/16/business/fi-squirrel16.

The recommendation, therefore, is to facilitate publicly available CFAA enforcement guidelines in the context of security research. This would ensure that white- and gray hat-hackers engaging in vulnerability research are aware of the boundaries and limitations and of their rights and duties. For example, a simple port scan, a basic operation used to learn about services running on a computer and entryways into the system, could lead to prosecution under the CFAA.[270] While this is clearly absurd in the eyes of security researchers, law enforcement authorities may not have the same perspective. This is just one example of the many basic activities of security researchers on which the CFAA should elaborate, particularly in light of the Senate Judiciary Committee's statement during the passage of Section 1030(a)(2) clarifying that "mere observation of the data" is enough to qualify as "obtaining information," a constitutive element of the crime of unauthorized access.[271] This would place security researchers who do not copy, exfiltrate, or steal protected information under potential criminal liability.

Recently, the DOJ released to the public a Memorandum by the Attorney General setting guidelines for consistent law enforcement of "Computer Crime Matters."[272] While the Memorandum does acknowledge that federal criminal statutes "have not kept pace uniformly with developments in technology," it does not acknowledge the emerging unsecure IoT ecosystem and the role of ethical hackers. The Memorandum offers certain factors for consideration in CFAA prosecutions, such as the sensitivity of the

[270] Though, a U.S. District Court in Moulton v. VC3 ruled that port scan is not in violation of the CFAA, its decision does not have binding authority. *See* Moulton v. VC3, 2000 U.S. Dist. LEXIS 19916 (N.D. Ga.).

[271] Senate Judiciary Committee Report No. 99 432, 99th Cong., 2d Sess., at 6–7 (1986) ("Because the premise of this subsection is privacy protection, the Committee wishes to make clear that 'obtaining information' in this context includes mere observation of the data. Actual asportation, in the sense of physically removing the date from its original location or transcribing the data, need not be proved in order to establish a violation of this subsection.").

[272] *See* Office of the Attorney General, *Memorandum to the United States Attorneys and Assistant Attorney Generals for the Criminal and National Security Divisions – Intake and Charging Policy for Computer Crime Matters* (Sep. 11, 2014), *available at* https://www.justice.gov/criminal-ccips/file/904941/download.

computer system affected, national security concerns, and any nexus to a larger criminal endeavor.

The DMCA exemption for security research also raises questions in relation to scope and the meanings of key terms. Since exemptions expire after three years, requiring renewed submission of petitions for exemptions, that could be an opportunity to further clarify what a security research exemption means, especially when it comes to devices not for individual consumer use, and the meaning of "controlled environment" in the age of cloud computing.[273]

d. Requiring Built-In Patchability in IoT Devices

The important work of security researchers in the field of IoT security will not bear any fruit if IoT devices cannot be patched in the first place. While computer users generally have control over what they install, this is not necessarily the case in the IoT context, where users have limited control over security features and have to trust the vendor to ensure up-to-date and secure software. This means that regulators would have to require vendors to manufacture IoT devices that can be patched if security flaws are discovered. The reality is that the market does not incentivize vendors to do so; we must therefore consider a regulatory approach.[274]

Patchability has been an important topic of discussion in the IoT regulation context. Many agencies, including the FTC and NTIA, have been strong proponents of patchability as a requirement for responsible IoT manufacturing.[275] Patching is a substantial part

---

[273] *See* Erik Stallman, *The Current DMCA Exemption Process Is a Computer Security Vulnerability*, CENTER FOR DEMOCRACY & TECHNOLOGY (Jan. 21, 2015), https://cdt.org/blog/the-current-dmca-exemption-process-is-a-computer-security-vulnerability (also arguing that security research may take more than three years, in which the exemption is in force).

[274] *See* Mauricio Paez & Mike La Marca, *The Internet of Things: Emerging Legal Issues for Businesses*, 43 N. KY. L. REV. 29, 53 (2016) ("[M]anufacturers often lack an economic incentive to provide software updates and support: manufacturers of specialized computer chips, which are cheap and operate on a thin profit margin, are typically working on or shipping the next version of the chip, while the original device manufacturers-who often do not get their brand name on the finished product-are working to upgrade their product to support the new chip. In this mindset, where getting the product to the market is the overwhelming priority, security may not be a priority.").

[275] *See* National Telecommunications & Information Administration, *Multistakeholder Process; Internet of Things (IoT) Security Upgradability and*

of overall security, but it is by no means a magic solution. Many users do not patch their software (if given a choice); certain organizations, such as hospitals and power plants, cannot patch immediately due to concerns that the patch may create functionality problems; and patches often have flaws themselves.[276]

e. Privacy Tort Law Solutions

Allowing individual hackers to perform security research may put privacy at risk should researchers encounter sensitive private information.[277] Users whose private information is compromised or disseminated to the public should have legal recourse. In this context, privacy tort law may provide a partial remedy for informational harms caused by security research, even in cases where the private information is not otherwise protected by data protection laws.[278] Recent literature focuses on two torts – intrusion upon seclusion and publicity given to private life.[279]

So far, courts have largely dismissed data breach lawsuits by consumers against vendors, ruling that if consumers do not suffer quantifiable harm, there is no legal cause of action.[280] These, however, are lawsuits against vendors; courts may reach a different conclusion if the defendant is a security researcher who overstepped

Patching (July 18, 2017), https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

[276] *See* Kesan & Hayes, *supra* note 73, at 787.

[277] Some guidance could be provided by laws dealing with the protection of certain types of information. *See, e.g.*, 45 C.F.R. § 164.306 (Health Insurance Portability and Accessibility Act – HIPAA) (providing the security standards for electronic protected health information).

[278] See Alexander Tran, *The Internet of Things and Potential Remedies in Privacy Tort Law*, 50 COLUM. J. L. SOC. PROB. 263, 266 (2017).

[279] *See* Tran, *supra* note 155, at 280.

[280] *See The Liability of Technology Companies for Data Breaches*, ZURICH (ADVISEN) (2010), https://www.advisen.com/downloads/Emerging_Cyber_Tech.pdf ("Legal experts note that the majority of courts have rejected data breach claims brought by affected persons that did not suffer any appreciable injury. Simply having one's personal information lost or stolen may not be sufficient, as the plaintiff must actually have suffered a loss in order to claim damages.").

the boundaries of his or her specific research, though proving harm will still be a necessary component.[281]

f. Vulnerability Disclosure Procedure

The process by which vulnerabilities are disclosed has been a contentious topic in recent years.[282] Vulnerability disclosure[283] is essentially a double-edged sword; the benefits extracted from it are largely dependent on the methods of disclosure, including the parties who learn about it and what they decide to do with that information.[284] Intuition suggests that once security researchers identify a vulnerability, they should disclose it to the relevant party, who would in turn fix or patch the flaw, thereby enhancing the overall security of the software. In the words of then-Secretary of Defense Ash Carter this would be the equivalent of a "'see something, say something' policy for the digital domain."[285] Reality, however, has been slightly more complicated than that.

While disclosing vulnerabilities to the vendor was the norm for many years, security researchers became increasingly frustrated because they were often ignored by vendors, who were reluctant

---

[281] *See Strategic Principles for Securing the Internet of Things (IoT)*, Department of Homeland Security (Nov. 15, 2016), https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf (suggesting that "[w]hile there is not yet an established body of case law addressing IoT context, traditional tort principles of product liability can be expected to apply.").

[282] Susan Brenner, *Complicit Publication: When Should the Dissemination of Ideas and Data be Criminalized?*, 13 ALB. L. J. SCI. & TECH. 101, 237 (2003) (arguing that the controversy about vulnerability disclosure is over how the information is disseminated).

[283] *See* Williams, Pescatore, and Proctor, *Responsible Vulnerability Disclosure: Guidance for Researchers, Vendors, and End Users*, at 3, GARTNER (Oct. 17, 2016), http://attrition.org/misc/ee/gartner-responsible_disclosure-144061.pdf ("Publicity over vulnerabilities in software products is a double-edged sword. Making vulnerabilities public has, unfortunately, proved necessary to spur some software vendors to invest in better software development, patch production and patch distribution processes. However, it has also enabled attackers to more quickly produce exploits").

[284] *See* Williams et al., *supra* note 283.

[285] *See* U.S. Department of Defense, *DOD Announces Digital Vulnerability Disclosure Policy and "Hack the Army" Kick-Off* (Nov. 21, 2016), https://www.defense.gov/News/News-Releases/News-Release-View/Article/1009956/dod-announces-digital-vulnerability-disclosure-policy-and-hack-the-army-kick-off.

investigate reported vulnerabilities.[286] At that point, researchers published only very limited information about the existence of a vulnerability to the public, which resulted in some vendors claiming these vulnerabilities were "theoretical."[287] Only when security researchers finally published the information they had to the public in full did vendors start taking these matters seriously.[288] This has led to a fragmentation of the philosophy on vulnerability disclosure. While certain experts advocate for "responsible disclosure," which primarily focuses on disclosing vulnerabilities to the vendor, there is a strong group of experts who oppose that approach and argue for "full disclosure," encouraging security researchers to publish the flaws they have identified to the broader public and assuming the vendor will then be pressured to fix the flaw more promptly.[289] There is a substantial group of individuals and organizations who adopt the "nondisclosure" approach to vulnerabilities, mainly black hats and intelligence agencies such as the National Security Agency.[290]

i. Responsible Disclosure

Responsible disclosure typically refers to reporting a vulnerability to the relevant vendor and allowing the vendor a certain amount of time to fix the vulnerability, depending on its complexity and other circumstances.[291] This type of disclosure is the

---

[286] *See* Bruce Schneier, *Schneier: Full Disclosure of Security Vulnerabilities a 'Damned Good Idea'*, SCHNEIER ON SECURITY (Jan. 2007), https://www.schneier.com/essays/archives/2007/01/schneier_full_disclo.html.

[287] *See* Schneier, *supra* note 286.

[288] *See* Schneier, *supra* note 286.

[289] Edward Freeman, *Vulnerability Disclosure: The Strange Case of Bret McDanel*, 16 INFORMATION SYSTEMS SECURITY 127, 128 (2007).

[290] *See* Bruce Schneier, *The NSA Is Hoarding Vulnerabilities*, SCHNEIER ON SECURITY (Aug. 26, 2016), https://www.schneier.com/blog/archives/2016/08/the_nsa_is_hoar.html (explaining how the NSA is hoarding vulnerabilities of software used both by private and governmental entities, including companies like Cisco, Fortinet, TOPSEC, and more. A portion of these vulnerabilities was patched since, but some vulnerabilities were still unknown until a group named Shadow Brokers leaked 300 megabytes worth of NSA-hoarded vulnerabilities).

[291] *See* Marc Laliberte, *A Look Inside Responsible Vulnerability Disclosure*, DARK READING (Jan. 5, 2017), http://www.darkreading.com/threat-intelligence/a-look-inside-responsible-vulnerability-disclosure/a/d-id/1327800 ("First, the researcher identifies a security vulnerability and its potential impact . . . . Next, the researcher

most commonly used approach by vendors, who naturally prefer to learn about the vulnerability before other parties or the public.[292] Initially, the DMCA exemption for security research was expected to include a requirement of responsible disclosure as part of its good-faith term. However, the Librarian of Congress noted that the community was divided on what constituted responsible disclosure and that therefore the DMCA rulemaking did not require responsible, or any other, type of disclosure other than requiring that information gathered be used primarily "to promote the security or safety" of the device in question.[293]

This is not to say that the public will not learn about the vulnerability; rather, such information will be released to the public only once a patch is released and the risk of exploitation by third

---

creates a vulnerability advisory report including a detailed description of the vulnerability, supporting evidence, and a full disclosure timeline . . . . After submitting the advisory to the vendor, the researcher typically allows the vendor a reasonable amount of time to investigate and fix the exploit . . . . Finally, once a patch is available or the disclosure timeline (including any extensions) has elapsed, the researcher publishes a full disclosure analysis of the vulnerability.").

[292] *See, e.g.*, US CERT/CC Vulnerability Disclosure Policy, *available at* http://www.cert.org/vulnerability-analysis/vul-disclosure.cfm? (providing that "vulnerabilities reported . . . will be disclosed to the public 45 days after the initial report, regardless of the existence or available of patches"). *See also* Chris Evans & Drew Hintz, *Disclosure Timeline for Vulnerabilities Under Active Attack*, GOOGLE SECURITY BLOG (May 29, 2013), https://security.googleblog.com/2013/05/disclosure-timeline-for-vulnerabilities.html ("Our standing recommendation is that companies should fix critical vulnerabilities within 60 days—or, if a fix is not possible, they should notify the public about the risk and offer workarounds.").

[293] *See* U.S. Copyright Office, Library of Congress, *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, 80 FR 65944, 65956 (Oct. 28, 2015) ("As explained above, a significant issue with respect to the security exemptions involves the proper disclosure of security research findings, as the interests of the manufacturer and the public may both be affected by the nature and timing of disclosure of software flaws. Indeed, Congress included disclosure to the system developer as one of the factors to be considered in determining a person's eligibility for the security testing exemption in section 1201(j). Although the Register expressed support for responsible disclosure of security flaws, she acknowledged the difficulty of attempting to define disclosure standards in the context of this rulemaking, as opinions seem sharply divided on this point. Accordingly, rather than incorporating an express disclosure rule, the recommended exemption draws upon what the Register perceives to be the basic intent of section 1201(j) by specifying that the information derived from the research activity be used primarily to promote the security or safety of the devices containing the computer programs on which the research is conducted, or of those who use those devices.").

parties decreases.[294] Another variation of responsible disclosure is reporting all information regarding the vulnerability to the vendor while disclosing only limited information, excluding the proof of concept, to the public.[295] However, even that approach does not necessarily prevent malicious hackers from reverse-engineering the general vulnerability information that is provided to the public.[296] The general idea is to ensure that the public will not be able to directly use the information to exploit the vulnerability.

ii. Full Disclosure

Full disclosure, unlike responsible disclosure, is the practice of reporting a vulnerability to the public to the fullest extent possible and without informing the vendor of it beforehand.[297] The practice of full disclosure is evidence of some of the frustration of the security research community resulting from vendors sometimes ignoring vulnerabilities reported to them.[298] It is immensely controversial because it allows equal access to information about a vulnerability to vendors and to potential exploiters.[299] The idea behind full disclosure is to pressure the vendor to patch the vulnerability since public scrutiny is a strong motivation for vendors

---

[294] *See* Stephen Lynch, *Full Disclosure: Infosec Industry Still Fighting Over Vulnerability Reporting*, CISCO UMBRELLA (Oct. 16, 2015), https://umbrella.cisco.com/blog/blog/2015/10/16/full-disclosure-infosec-industry-still-fighting.

[295] *See* EFF, *Coders' Rights Project Vulnerability Reporting FAQ*, https://www.eff.org/issues/coders/vulnerability-reporting-faq.

[296] *See* Bambauer, *supra* note 34, at 1064 (explaining that "if they describe flaws with too much precision, hackers can probe the weaknesses, but if they are too general, customers will encounter difficulty taking precautions").

[297] *See* Taiwo Oriola, *Bugs for Sale: Legal and Ethical Properties of the Market in Software Vulnerabilities*, 28 J. COMP. & INF. L. 451, 483 (2011) ("[A] full disclosure occurs where independent security analysts promptly post vulnerabilities to a public listing.").

[298] *See* Bruce Schneier, *Debating Full Disclosure*, SCHNEIER ON SECURITY (Jan. 23, 2007), https://www.schneier.com/blog/archives/2007/01/debating_full_d.html.

[299] *See* Stephen Lynch, *Full Disclosure: Infosec Industry Still Fighting Over Vulnerability Reporting*, CISCO UMBRELLA (Oct. 16, 2015), https://umbrella.cisco.com/blog/blog/2015/10/16/full-disclosure-infosec-industry-still-fighting (arguing that full disclosure is controversial because it creates a race between vendors and potential exploiters, who both have equal access to the information pertaining to the vulnerability).

to take security seriously.[300] Bruce Schneier, a supporter of the full disclosure practice, called it a "damned good idea," [301] and many others agree.

However, full disclosure is not always a provocative step against vendors. It is often used to publish information about a vulnerability so that customers can protect themselves from exploitation, given that the vendor will either ignore or take too long to fix the flaw. Many assume that full disclosure allows malicious actors to exploit vulnerabilities published by security researchers, but there is an assumption that black-hat hackers are aware of certain vulnerabilities, if not sold them in the zero-day vulnerability market.[302]

iii. The Road Forward on Vulnerability Disclosure

This subsection has demonstrated that the debate over vulnerability disclosure stems from distrust between security researchers and vendors.[303] But security researchers could regain their trust in vendors, and vice versa, if a robust form of oversight is implemented. This can be achieved by relying on intermediaries and enforcers of norms in that context – for example, US-CERT and the FTC. Primarily, this will require official guidelines from an authoritative body (the FTC, for example) regarding how to responsibly disclose vulnerabilities in a way that properly balances vendors' interests and the need for cybersecurity.

g. Transnational Law Enforcement and Reducing National Security Threats

[300] *See* Schneier, *supra* note 298.

[301] Bruce Schneier, *Schneier: Full Disclosure of Security Vulnerabilities a 'Damned Good Idea'*, CSO ONLINE (Jan. 9, 2007), http://www.csoonline.com/article/216205/schneier-full-disclosure-ofsecurity-vulnerabilities-a-damned-good-idea-.

[302] *See* Schneier, *supra* note 286.

[303] *See Vulnerability Disclosure Attitudes and Actions,* Research Report from the NTIA Awareness and Adoption Group, https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf ("The assumptions and prejudices that impede collaboration between researchers and technology providers may be based on past experience.").

The DOJ recently indicted a group of Russian FSB officers who were involved in hacking Yahoo!, gaining access to as many as 500 million e-mail accounts.[304] Transnational law enforcement is expensive and resource-intensive. In an environment friendlier to ethical hacking, where tech companies do not threaten security researchers, such a massive data breach could have been prevented. In addition, the FBI has already admitted that it is losing the "war on hackers,"[305] which indicates that law enforcement may be increasingly inclined to consider "alternative architectures that are more secure" in the first place.[306]

Patching vulnerabilities before foreign governments learn about them could enhance overall national security. If we assume that national security includes dams, transportation, healthcare, and other sectors operating on information technology, we might also conclude that patching vulnerabilities in advance would keep foreign malicious actors largely at bay, since their options to attack the cyber infrastructure would be limited to only zero-day vulnerabilities, which would be far more limited than the number of vulnerabilities that could be identified by ethical hackers and patched by the manufacturer.

h. Tackling Security by Obscurity

The concept of security by obscurity provides that keeping the code for a particular piece of software, and therefore vulnerabilities in that code, hidden and unknown to hackers can make the software seemingly more secure.[307] In software engineering, this is

[304] Department of Justice, *U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts* (Mar. 15, 2017) https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.

[305] *See* Devlin Barrett, *U.S. Outgunned in Hacker War,* WALL ST. J. (Mar. 28, 2012), https://www.wsj.com/articles/SB10001424052702304177104577307773326180032.

[306] *See* Robert Mueller, *Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies,* 2012 RSA Cyber Security Conference (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

[307] *See* Yana Welinber, *Facing Real-Time Identification in Mobile Apps & Wearable Computers,* 30 SANTA CLARA COMPUTER & HIGH TECH. L.J. 89, 128 (2014).

sometimes called "obfuscation."[308] Vendors may make their code overly complex or ridden with gibberish code lines in order to confuse a potential attacker. But this has not worked in the past, and it will not work in the future. In today's cybersecurity world, it is almost impossible to hide vulnerabilities; the only way to prevent their exploitation is to patch them and get rid of them.[309] Security by obscurity also violates Kerckhoff's principle,[310] which posits that the public release of a system should not be to its detriment, since systems should be secure by design, not due to their confusing nature.[311]

This shows that the emphasis on securing IoT devices should be on revealing vulnerabilities, possibly providing an incentive for individuals to do so, as well as on patching those vulnerabilities, which is the responsibility of the vendor.

In this regard, the FTC can play an important role. The FTC has been recently actively enforcing consumer privacy based on Section

---

[308] *Innovation, Software, and Reverse Engineering*, 18 SANTA CLARA COMPUTER & HIGH TECH. L.J. 121, 131 (2001) ("[C]ode obfuscation consists of a process by which code contains sufficient decoys to obstruct reverse engineering.").

[309] Michael Gegick & Sean Barnum, *Never Assuming That Your Secrets Are Safe*, US-CERT (Sep. 14, 2015), https://www.us-cert.gov/bsi/articles/knowledge/principles/never-assuming-that-your-secrets-are-safe ("Always assume that an attacker knows everything that you know -- assume the attacker has access to all source code and all designs. Even if this is not true, it is trivially easy for an attacker to determine obscured information.") (citing Howard & LeBlanc, *Chapter 3, Security Principles to Live By*, *IN* NEVER DEPEND ON SECURITY THROUGH OBSCURITY ALONE 66–67).

[310] *See* Jesper Johansson & Roger Grimes, *The Great Debate: Security by Obscurity*, MICROSOFT TECHNET MAGAZINE (June 2008), https://technet.microsoft.com/en-us/library/2008.06.obscurity.aspx ("Security by obscurity is, in a nutshell, a violation of Kerckhoffs' Principle, which holds that a system should be secure because of its design, not because the design is unknown to an adversary. The basic premise of Kerckhoffs' Principle is that secrets don't remain secret for very long."). *But see* Corey Nachreiner, *How a Little Obscurity Can Bolster Security*, DARK READING (Apr. 17, 2014), http://www.darkreading.com/risk/how-a-little-obscurity-can-bolster-security/d/d-id/1204452.

[311] *See* Bruce Schneier, *Secrecy, Security, and Obscurity*, SCHNEIER ON SECURITY (May 15, 2002), https://www.schneier.com/crypto-gram/archives/2002/0515.html ("Today, there is considerable benefit in publication, and there is even more benefit from using already published, already analyzed, designs of others. Keeping these designs secret is needless obscurity. Kerckhoffs' Principle says that there should be no security determent from publication.").

5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[312] The FTC has become a "de facto data protection authority."[313] Given that the degree of privacy could be affected by the strength of security, the FTC ought to ensure that companies do not engage in practices that could compromise private information belonging to consumers, with security by obscurity being one of those practices.[314] Furthermore, the Third Circuit in *FTC v. Wyndham* held that the FTC has authority to sue for inadequate security practices.[315]

This common law of FTC privacy enforcement could lead to stronger enforcement against companies who do not act according to industry best practices of privacy and security.[316] Security by obscurity, a practice that certain vendors adopt in order to avoid vulnerability detection, should be treated as a deceptive or unfair practice in the same way the FTC deals with other security-violating practices.[317] The FTC has already pursued action against an IoT vendor, TRENDnet, in a claim that its smart webcams did not provide consumers with "reasonable security to prevent unauthorized access to sensitive information, namely the live feeds from the IP cameras."[318] It is anticipated that the FTC will pursue further enforcement against IoT vendors who engage in unfair or deceptive security or privacy practices, which should encompass

---

[312] *See* 15 U.S.C § 45(a)(1).

[313] *See* Steven Hetcher, *The De Facto Federal Privacy Commission*, 19 J. MARSHALL J. COMPUTER & INFO. L. 109, 131 (2000).

[314] *See* Daniel Solove & Woodrow Hartzog, *The FTC and The New Common Law of Privacy*, 114 COLUM. L. REV 583, (2014)

[315] FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 236 (3d Cir. 2015).

[316] *See* Solove & Hartzog, *supra* note 314, at 653 (providing examples of FTC common law of privacy enforcement against companies for "[f]ailure to implement cheap, easy-to-use, or common industry security practices").

[317] *See* Solove & Hartzog, *supra* note 314, at 637 ("In the early 2000s, the FTC initiated a flurry of activity around security—nearly overshadowing its privacy cases.").

[318] *See* Trendnet, Inc., No. 122-3090, 2013 WL 4858250, at *2 (F.T.C. Sept. 3, 2013) ("[A]s a result, hackers exploited the security vulnerabilities leading to 'compromised live feeds display[ing] private areas of users' homes and allow[ing] the unauthorized surveillance of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities.") (*cited in* Tran, *supra* note 155, at 276).

practices like security by obscurity and, perhaps, unwillingness to respond to vulnerability disclosures.

V. CONCLUSION

This Article argues that the DMCA and CFAA impede security research into software vulnerabilities, which are on the rise in the emerging IoT ecosystem due to an industry-specific market failure. These legal barriers discourage security researchers from discovering flaws and reporting them to the relevant vendors, which would enhance overall privacy and security. This could be partially resolved by mitigating the threat of legal jeopardy through clarification of the DMCA and CFAA boundaries as well as by enacting legal and regulatory adaptations such as requiring *patchability* in IoT, tackling security by obscurity, and enforcing the law against noncomplying vendors. This will create a friendly and fruitful environment for security research, leading to a more secure IoT ecosystem and, ultimately, a more secure Internet system.

The IoT ecosystem creates a host of opportunities but also a variety of risks and dangers, which should be addressed through legitimizing the activities of the community of dedicated vulnerability hunters. Security research is important where market forces fail and where vendors are unlikely to discover vulnerabilities on their own, which they currently lack the incentive to do. Broad interpretation of these "anti-hacking" laws is resulting in a less secure Internet, and the stakes are constantly increasing given the ubiquity of sensors and physicality of the IoT ecosystem.

The law should clearly distinguish between white- and gray-hat hackers, whose purpose is to fix flaws (to varying degrees), and black-hat hackers, who use vulnerabilities for criminal ends. This distinction has been overlooked for too long, and IoT ought to be a turning point in that regard, creating a space for benevolent actors to fully utilize their talent.