DEBUGGING THE REAL WORLD: ROBUST CRIMINAL PROSECUTION IN THE INTERNET OF THINGS

Matthew Ashton*

Internet-linked versions of ordinary objects now dominate the horizon of the technology industry. These devices, collectively referred to as the Internet of Things ("IoT"), span everything from toothbrushes to smart homes, from self-driving cars to refrigerators that know when the owner is out of eggs. Because IoT devices usually have minimal computing power, they are more vulnerable to security breaches than their more familiar cousins: laptops, tablets, and mobile phones. This creates the risk that hackers can gain control of real-world objects with minimal effort and a low probability of getting caught. To solve this problem, a three-pronged approach is necessary: existing criminal statutes must be refocused to impose the harshest sentences on the most damaging of cybercrimes; prosecutor's offices must incorporate specialized cybercrimes units to competently navigate the unique legal issues in IoT; and a civil enforcement regime must be brought to bear against companies that make products without adequate security protocols for the applicable task. By shoring up IoT security vulnerabilities through improved legislation, improved criminal enforcement, and improved technological barriers, the future of IoT can be kept safe for all to enjoy.

TABLE OF CONTENTS

---

* J.D. Candidate, University of Arizona James E. Rogers College of Law, Class of 2018. I thank Professor Derek Bambauer and my Note Editor, Hannah Willett, for their patient and expert guidance. I also thank the editorial team at *Arizona Law Review* for their tireless efforts. Any remaining errors are my own. Although I owe recognition to many more, I would finally like to thank my parents, Mark and Holly, for their love and support.

INTRODUCTION

In 2012, a web-security researcher named Barnaby Jack bragged that he could exploit a flaw in Internet-linked pacemakers to turn one of these life-saving devices into a completely anonymous assassination tool.[1] Fortunately for the hundreds of thousands of people in the United States who depend on pacemakers, Barnaby Jack was not a killer. Rather, he pointed out the existence of this flaw to raise awareness of the potential for malicious attacks on Internet-linked medical devices.[2] Still, his message rang loud and clear in the cybersecurity community: something needs to be done to ensure the security of devices in a world with an ever-increasing number of links to cyberspace. Otherwise, the next hacker capable of completing Jack's claimed feat could turn out to be more malicious, and proceed on an anonymous crime spree of anything from serial murder to leveraging people's own pacemakers against them for ransom.

Tragically, Jack died just a week before he was to present his research at the annual Black Hat hacker convention in Las Vegas in 2013.[3] His research and legacy, however, lived on.[4] His research on how to hack insulin pumps was already a major game-changer in cybersecurity, and at the very same convention he was to attend, other researchers demonstrated how modern cars could be similarly compromised.[5]

Shortly after Jack's death, regulators started to see the need to address this issue.[6] The Food and Drug Administration ("FDA") issued a public warning, which stated that malicious hackers could plant malware in pacemakers, implanted defibrillators, drug pumps, and ventilators to cripple these devices remotely.[7] The Federal Trade Commission ("FTC") hosted a workshop in November 2013 where industry leaders were invited to help identify and rectify the primary threats to Internet devices outside the prototypical examples of computers, tablets, and

---

1. Jeremy Kirk, *Pacemaker Hack Can Deliver Deadly 830-Volt Jolt*, COMPUTERWORLD (Oct. 17, 2012, 1:40 AM), http://www.computerworld.com/article/2492453/malware-vulnerabilities/pacemaker-hack-can-deliver-deadly-830-volt-jolt.html.

2. *Id.*

3. *Hacker Dies Days Before He Was to Reveal How to Remotely Kill Pacemaker Patients*, RUSS. TODAY (July 26, 2013, 3:07 PM), https://www.rt.com/usa/hacker-pacemaker-barnaby-jack-639/.

4. *See id.*

5. *See id.*

6. *US Warns of Cyberattacks Targeting Medical Devices*, RUSS. TODAY, (June 14, 2013, 6:39 PM), https://www.rt.com/usa/us-warns-medical-cyberattack-721/.

7. *Id.*

smartphones.[8] The Department of Commerce ("DOC"), on the other hand, purposefully took a slower route to rulemaking in this area, citing concerns that an international patchwork of different rules could stymie innovation in this ever-expanding field.[9] The DOC only recently announced a formal Request for Comments in preparation for rulemaking.[10]

Though Barnaby Jack's announcement of the fatal potential of Internet-linked devices came as a shock to some, IoT itself could hardly be said to have snuck onto the scene.[11] IoT, a term coined by journalist-turned-lipstick-tracker-turned-tech-wizard Kevin Ashton,[12] has seen explosive expansion since its birth in the late 90s.[13] But what is IoT? Though there is no universally-accepted definition, for purposes of this Note, the FTC's definition of IoT should suffice: it is the collection of all "devices or sensors—other than computers, smartphones, or tablets—that connect, store or transmit information with or between each other via the Internet."[14]

---

8. *FTC: Internet of Things: Privacy & Security in a Connected World*, 20 NO. 4 CYBERSPACE LAW. 5 (2015) [hereinafter *Privacy & Security*].

9. Paul Merrion, *Commerce Looks at Big Picture on Internet of Things*, CQ ROLL CALL WASH. DATA PRIVACY BRIEFING (Apr. 6, 2016), https://1.next.westlaw.com/Document/Iab0c43981b5011e698dc8b09b4f043e0/View/FullText.html.

10. *Id.*

11. For example, legal scholarship about IoT first popped up as early as 2004, when privacy concerns over radio-frequency identification ("RFID") tags pressured politicians to start drafting legislation to fix this issue before it began and scholars warned that premature legislation could hamper growth. *See, e.g.*, Jerry Brito, *Relax Don't Do It: Why RFID Privacy Concerns are Exaggerated and Legislation is Premature*, 2004 UCLA J.L. & TECH. 5. As for press, even IoT devices themselves could not resist the urge to step into the ever-brightening spotlight, with the famous Carnegie Mellon Internet-linked Coke machine "writing" a sort of autobiography more than two decades after its birth. *See The "Only" Coke Machine on the Internet*, CARNEGIE MELLON UNIV. (last visited Apr. 13, 2017), https://www.cs.cmu.edu/~coke/history_long.txt.

12. No relation to the Author. For a lengthier history on both Kevin Ashton and IoT, see Kevin Maney, *Meet Kevin Ashton, Father of the Internet of Things*, NEWSWEEK (Feb. 23, 2015, 12:10 PM), http://www.newsweek.com/2015/03/06/meet-kevin-ashton-father-internet-things-308763.html.

13. *See infra* notes 17–21 and accompanying text.

14. *Privacy & Security*, *supra* note 8. This definition of IoT is not the only one, though it may be the most convenient. "There is no hard and fast definition of IoT." Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security*, 31 BERKELEY TECH. L.J. 997, 1008 (2016). Swaroop Poudel lists a number of definitions given by various experts, most of which resemble the FTC definition. Others define IoT more vaguely as an all-encompassing, all-connecting network; Cisco chooses to define IoT instead as the point in time when the number of devices connected to the Internet exceeded the population of the world. *Id.* at 1008–09. In its request for comments, the Commerce Department defines IoT more abstractly as "the connection of physical objects, infrastructure, and environments to various identifiers, sensors, networks, and/or computing capability." Merrion, *supra* note 9. The Internet of Things Global Standards Initiative defined it instead as "[a] global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies." *Overview of the Internet of Things*, INT'L

Examples of IoT devices span from smart homes[15] to flip-flops[16] to toothbrushes.[17] The number of items that can possibly be linked to the Internet is limited only by the inventor's imagination.

This variation from product to product goes beyond the surface level of what the devices *look like* to how they *work*—particularly, how they connect to other devices. Different IoT devices use different types of connections: Bluetooth,[18] Wi-Fi,[19] and even good, old-fashioned wires. Most low-powered devices are connected by Bluetooth to another device (usually a phone, tablet, or computer), which in turn connects to the Internet through Wi-Fi or a mobile communications standard like 3G.[20] Some smart homes have Wi-Fi connections so that they can be controlled remotely by the homeowner, but also have Bluetooth, wired, or other connections within the home.[21] Some believe that IoT devices in the future will all connect to the Internet directly via low-frequency Wi-Fi, which maximizes the range and speed of the connection.[22]

Because of this extreme versatility and diversity, the size of IoT has grown at rates that never could have been expected back in its humble beginnings in the late 90s. Cisco, which has begun a mass shift in production towards IoT products, reported that the number of Internet-connected devices exceeded the world's population in 2012.[23] In 2015, ABI Research and Cisco both predicted that by 2020

TELECOMM. UNION 1 (2013), http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11559&lang=en.

15. Andrew Meola, *How IoT & Smart Home Automation Will Change the Way We Live*, BUS. INSIDER (Dec. 19, 2016, 4:44 PM), http://www.businessinsider.com/internet-of-things-smart-home-automation-2016-8.

16. Libby Watson, *15 Idiotic Internet of Things Devices Nobody Asked For*, GIZMODO (Apr. 14, 2017, 2:55 PM), http://gizmodo.com/15-idiotic-internet-of-things-devices-nobody-asked-for-1794330999.

17. Benny Evangelista, *Smart Toothbrushes the Latest Internet of Things Battleground*, SFGATE (June 9, 2016, 12:05 AM), http://www.sfgate.com/business/article/Smart-toothbrushes-the-latest-Internet-of-Things-7971669.php.

18. Bluetooth is basically a low-cost, short-range communication protocol most popularly used for cordless mobile phone accessories. GC, *Bluetooth Introduction*, TUTORIAL-REPORTS.COM (Feb. 18, 2013, 5:22), http://www.tutorial-reports.com/wireless/bluetooth/introduction.php.

19. Wi-Fi is the trademarked name for a wireless networking system that communicates with an Internet access point through radio waves. Vangie Beal, *Wi-Fi (Wireless Networking)*, WEBOPEDIA, http://www.webopedia.com/TERM/W/Wi_Fi.html (last visited Aug. 23, 2017).

20. Brian Barrett, *Next-Gen Wi-Fi Will Actually Connect the Internet of Things*, WIRED (Jan. 4, 2016, 4:36 PM), https://www.wired.com/2016/01/wifi-halow-internet-of-things/.

21. *See* Jacob Kastrenakes, *Wi-Fi and Bluetooth are Coming for the Smart Home*, THE VERGE (Jan. 8, 2016, 3:40 PM), https://www.theverge.com/2016/1/8/10737900/wifi-bluetooth-coming-for-zigbee-zwave-smart-home-iot-ces-2016.

22. Barrett, *supra* note 20.

23. DAVE EVANS, THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 (Cisco ed., 2011),

there would be as many as 50 billion items connected to the Internet.[24] Intel claimed they were both underestimating the figure, saying that over 200 billion devices would be connected by then.[25] The economic impact of all this is predicted to reach up to eleven trillion dollars by 2025.[26] The technology field has taken notice of this market explosion and its implications for the digital age, and several companies are shifting their considerable investment weight towards IoT in anticipation.[27]

There is good reason to curb this enthusiasm. As with any expansive and disruptive technology, IoT and its devices threaten to usher in a new wave of crime. This pattern of misusing otherwise-beneficial technology has repeated itself throughout history. Alfred Nobel watched as his dynamite moved from an industrial explosive to a weapon. The advent of the car brought with it careless driving and both accidental and intentional vehicular homicide. The digital age has brought new crimes in cyberspace with data breaches, viruses, and ransomware.[28] Because IoT acts both as a branch of cyberspace and as a portal between cyberspace and the real world, the technology makes the real world susceptible to all the weaknesses of cyberspace.[29] Clever hackers can use IoT devices to gain information from—or control over—objects in the real world.[30] Hackers gaining information they should not have is one problem; hackers infiltrating the security systems of a device they have no right to control is another. Most of the concerns with IoT-related crime center on these two issues: privacy and security.

The FTC and legal scholars have addressed privacy concerns relating to IoT at some length.[31] In 2013, the FTC recommended that IoT companies minimize

---

http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. Swaroop Poudel claims that this occurred even earlier, in 2010. Poudel, *supra* note 14, at 1008.

24. Daniel E. Harmon, *The IoT & Law Practice: How Will the Internet of Things Impact You This Year?*, 32 NO. 8 LAW. PC 1 (Jan. 15, 2015).

25. Leo Sun, *Internet of Things in 2016: 6 Stats Everyone Should Know*, THE MOTLEY FOOL (Jan. 18, 2016, 5:30 PM), http://www.fool.com/investing/general/2016/01/18/internet-of-things-in-2016-6-stats-everyone-should.aspx.

26. Peter M. Lefkowitz, *Making Sense of the Internet of Things*, 59 BOS. BAR J. 23, 23 (2015).

27. Cisco, in particular, has banked heavily on the growth of IoT in future years, shifting its business plan to focus almost entirely on what it calls the "next evolution of the Internet." *See* EVANS, *supra* note 23.

28. For a primer on the history of cybercrime's rise to significance, see generally M. E. KABAY, A BRIEF HISTORY OF COMPUTER CRIME: AN INTRODUCTION FOR STUDENTS (2008), http://www.mekabay.com/overviews/history.pdf.

29. *See, e.g.*, Harmon, *supra* note 24 ("It's possible for your 'smart' coffee maker to clue burglars as to your customary wake-up time."). Many similar hacks—whether to gain private information about the device owner or to gain control over the device itself—can be imagined.

30. *Id.*

31. *Id.*; *see also* Katherine Britton, *Handling Privacy and Security in the Internet of Things*, 19 No. 10 J. Internet L. 3 (2016); MARC GOODMAN, FUTURE CRIMES: INSIDE THE DIGITAL UNDERGROUND AND THE BATTLE FOR OUR CONNECTED WORLD (Anchor ed., 2016).

the amount of data their products collect and build in protocols to delete the data at regular intervals.[32] Scot Peppet, a privacy law scholar, has gone even further into this topic, pointing out how merely anonymizing or aggregating data does not solve the privacy issue completely.[33] This Note focuses instead on the under-addressed security issues in IoT.

This Note presupposes that the arms of the criminal justice system—particularly, the federal and state statutes that criminalize hacking—are already long enough to reach the types of crimes that can take place in IoT. Instead of taking issue with this scope, this Note argues that cybercrime-specific criminal statutes are lacking in focus: they fail to match the harshest sentences to the most damaging crimes, producing misdirected deterrent effects. This is partly a problem of just how few criminal statutes—or even civil laws or administrative rules—were designed to specifically address the threats posed by IoT.[34]

After summarizing the existing and proposed rules in this area, this Note turns to the primary cybercrime-specific, federal criminal statute that could apply to IoT, the Computer Fraud and Abuse Act ("CFAA"). The CFAA, far from lacking in scope, is generally considered overbroad.[35] This breadth is a result of a series of amendments through the years, each of which expanded the statute's scope in some way.[36] This Note does not attempt to fight against the litany of scholarly works that say the CFAA is overbroad,[37] nor does it advocate to overturn the cases that have continually found the statute constitutional and given its terms broad definitions.[38]

---

32. *Privacy and Security, supra* note 8.

33. Scot Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 129–30 (2014). Peppet's article also addresses the issues of discrimination, security breaches, and lack of consent that all may come up in an IoT-dominated digital world.

34. For an explanation as to why this is, see *supra* notes 7–10 and accompanying text. For a general discussion of the existing cybercrime-specific rules and regulations, see *infra* Part I.

35. In fact, Professor Kerr argued in 2010 that the statute was unconstitutionally vague absent caselaw limiting the definition of the phrase "without authorized access or exceeding authorized access" within the statute. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561–62 (2010). Regrettably, this work's influence and acceptance among the scholarly community were not paralleled by its reception from the bench, and several courts have interpreted the CFAA even more broadly since then. *See, e.g.*, United States v. Nosal, 844 F.3d 1024, 1033–38 (9th Cir. 2016).

36. Kerr, *supra* note 35, at 1561–64.

37. *See, e.g.*, *id.* at 1561–62; Samantha Jensen, Comment, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*, 36 HAMLINE L. REV. 81 (2013); Sarah Boyer, *Computer Fraud and Abuse Act: Abusing Federal Jurisdiction?*, 6 RUTGERS J.L. & PUB. POL'Y 661 (2009).

38. *See, e.g.*, Int'l Airport Ctr., LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (applying a broad agency-based interpretation of the term *without authorization*); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581–82 (1st Cir. 2001) (applying a slightly less broad contract-based interpretation of the term "without authorization"); *Nosal*, 844 F.3d at 1024 (holding that even under the Ninth Circuit's otherwise-narrow construction of the CFAA, sharing a password can constitute a violation).

Instead, this Note takes the CFAA "as is" in terms of scope and suggests a separate flaw: that the statute's sentencing structure fails to deter the types of conduct most harmful to consumers who use devices in IoT.

Next, this Note evaluates the readiness of law enforcement agencies to deal with cybercrime investigation and prosecution. Though some agencies have developed specialized units for dealing with cybercrime, others have left the issue for future generations. The result is an unspecialized law enforcement community that is unprepared to deal with the drastic increases in cybercrimes being ushered in by the digital age. This Note argues that more attention and more specialized efforts need to be put to work to effectively detect and deter cybercrime in IoT.

Finally, this Note argues that there is another fault in the overall criminal enforcement framework relating to IoT that cannot be fixed by any number of amendments to the CFAA or specialized law enforcement agents: cybercrimes in IoT are uniquely difficult—sometimes impossible—to detect and enforce.[39] To fix this flaw, this Note proposes a supporting structure of civil regulations designed to force companies to build security protocols into every IoT device they create; protocols that will make hacking difficult to accomplish and easy to detect. At the same time, this proposed regulation system must be loose enough to allow for the free innovation a young industry like IoT needs to reach its full potential.[40] To achieve such a system, this Note draws from the wisdom of emerging scholarship in Internet regulatory theory to bend Professor Lessig's Four Forces to the plow,[41] pushing developers to create products that will allow for effective detection and prosecution of crimes in IoT. The result of this three-pronged approach—refocusing the CFAA, specializing the law enforcement community, and deputizing IoT developers to assist law enforcement—is a robust criminal enforcement framework to protect the modern user from the modern criminal.

I. EXISTING CYBERCRIME-SPECIFIC CRIMINAL STATUTES

A. The Digital Millennium Copyright Act

The predominant federal cybercrime statutes are the CFAA and the Digital Millennium Copyright Act ("DMCA").[42] The former is incredibly useful for punishing hackers in IoT. The latter is not well-suited for that task. The DMCA is, as the name suggests, a piece of legislation adopted around the turn of the

---

39. *Infra* Part V.

40. This freedom to innovate has been a particular concern of Congress, the FTC, and other bodies that might otherwise naturally have introduced legislation in this area. *See supra* notes 7–10 and accompanying text. For an argument that at least loose regulation is necessary at this stage in IoT's development, see *infra* Part V.

41. *See* Lawrence Lessig, *The New Chicago School*, 27 J. LEG. STUD. 661, 661–63 (1998); *see generally* Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653 (2003).

42. Naturally, there are also child pornography statutes, but those are not the subject of this Note.

millennium as an extension of existing copyright protections.[43] In addition to its more famous "Safe Harbor" provision, the statute provides both civil and criminal law protections for copyrighted materials stored on digital media, so long as those materials are covered by a technological measure that "effectively controls access" to them.[44] For a host of reasons, the DMCA does not fit the need for a criminal statute that protects the security of devices in IoT. First, the data stored on IoT devices are often below even the minimal standard for creativity required for something to fall under copyright protections.[45] Much of this data is generated by computers observing nature—pure sensor input relating to temperatures, locations, and so on—without any humans in the middle. It would take real stretches of the imagination to think that these simple devices are capturing the sort of man-made artistry that can be captured through sound recordings or audiovisual equipment.[46] Second, IoT devices are often too small to have technological measures that "effectively control access."[47] As explored more fully below, certain simplistic devices are too small to even have their data files encrypted.[48] Third, the DMCA's criminal provisions require that the crime be committed both "willfully and for purposes of commercial advantage or private financial gain."[49] Many Internet crimes are committed for monetary gain, but a large percentage of the potential IoT crimes of the future could be spurred by violent, sexual, or even political motives.[50] Even if prosecutors started using the DMCA to prosecute cybercrimes affecting IoT devices, smart criminals would avoid prosecution by simply stealing data that could

---

43. To be very technical, it was intended to implement two World Intellectual Property Organization ("WIPO") treaties, but the function of those two treaties were to extend the rights of copyright holders. David Nimmer, *Appreciating Legislative History the Sweet and Sour Spots of the DMCA's Commentary*, 23 CARDOZO L. REV. 909, 961–62 (2002).

44. 17 U.S.C. §§ 1201–05 (1999).

45. The copyright test for creativity was articulated in *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 348 (1991). That case held that compilations of facts could be copyrighted, but only when some originality is involved in the way that the facts were selected, coordinated, and arranged. *Id.*

46. Though the *Feist* case articulated a low standard for originality, numerical compilations of data such as those acquired by Fitbits, smart homes, and Internet-linked cars still fall noticeably below this bar. Even assuming some enterprising attorney successfully argued that a Fitbit owner's gait was a copyrightable expression fixed in the form of the data recorded in the Fitbit, there would still be barriers presented by the merger doctrine. There are only so many different ways to walk. Also, the Constitution requires that the expression be the work of an *author*, as arguably opposed to a mere *walker*. *See* U.S. CONST. art. I, § 8, cl. 8. This sort of thorny constitutional question is precisely the type of thing that an ordinary prosecutor interested in gaining a conviction and preserving a strong record for appeal would be well-advised to avoid.

47. This size issue has led to the advancement of so-called Lightweight Cryptography methods that can be applied to small IoT devices in lieu of full encryption methods. *See, e.g.*, MASANOBU KATAGI & SHIHO MORIAI, LIGHTWEIGHT CRYPTOGRAPHY FOR THE INTERNET OF THINGS (2011), https://www.iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf.

48. *See id.*

49. 17 U.S.C. § 1204(a) (2012).

50. This assumes, of course, that the motives for ordinary "real-world" crimes will find outlets in cybercrime.

not be copyrighted, data that was stored on small and unprotected devices, or data that served noncommercial purposes. The DMCA was never intended to regulate security in IoT,[51] and it is simply not up to the task of protecting against a wide swath of potential hacks.

B. The Computer Fraud and Abuse Act

The CFAA, on the other hand, can be accurately thought of as a general anti-hacking statute. It began as a statute that merely prevented unauthorized access to government computers,[52] but over the years it has evolved into a behemoth of a federal felony statute.[53] Its broadest and most famous subsection punishes those who view information on a protected computer, either without authorization or in a way that exceeds authorized access.[54] If *protected computer* truly meant some special type of computer, or if it even meant that the device being hacked had to be a computer at all, this statute would be innocent enough—and would also be useless for the purposes of this Note. Indeed, the statute originally protected only computers owned by the government and computers that contained personal financial records.[55] But over the years, Congress has expanded the definition of *protected computer* to include essentially any device with some kind of microchip.[56] Phones, tablets, Fitbits, and even public transit cards with embedded computer chips are all included in the definition of a *protected computer*.[57] Theoretically, almost anything with at least a microchip and some relation to interstate commerce is a protected computer under the CFAA.[58]

The terms *without authorization* and *exceeds authorized access* offer cold comfort to those attempting to restrict the applicability of the CFAA. Though there is a significant split in the circuit courts as to the meaning of *exceeds authorized access*, all agree that bypassing any technological barrier—effective or not—to get

---

51. *See* Nimmer, *supra* note 43 (explaining the history of the DMCA in some depth without ever mentioning the Internet of Things).

52. Kerr, *supra* note 35, at 1563–64.

53. *Id.* at 1563–71.

54. 18 U.S.C. § 1030(a)(2) (2012).

55. Kerr, *supra* note 35, at 1563–64 ("Each offense then added requirements that collectively limited the statute to three specific scenarios: computer misuse to obtain national security secrets, computer misuse to obtain personal financial records, and hacking into U.S. government computers.").

56. 18 U.S.C. § 1030(e)(1), (e)(2)(B); Kerr, *supra* note 35, at 1570–71 ("[The CFAA] applies to all computers, period, so long as the federal government has the power to regulate them.").

57. 18 U.S.C. § 1030(e)(1), (e)(2)(B).

58. Kerr, *supra* note 35, at 1570–71, 1577–78 ("[Protected computers] can include coffeemakers, microwave ovens, watches, telephones, children's toys, MP3 players, refrigerators, heating and air-conditioning units, radios, alarm clocks, televisions, and DVD players, in addition to more traditional computers like laptops or desktop computers."). Curiously enough, one of the devices explicitly excluded from this definition is a handheld calculator, though that carries far more computing capacity than several of the other devices that are covered. 18 U.S.C. § 1030(e)(1).

at information will put a person on the bad side of this law.[59] Outside of the Ninth Circuit, *exceeds authorized access* is read to depend on a quasi-contractual definition of *authorized*, such that violations of a website's End User License Agreement ("EULA") make use unauthorized, even if the website itself is otherwise public.[60] The vast number of websites with EULAs and the carefree ease with which most users click through their acceptance of these contracts serves to demonstrate precisely what critics of the CFAA are afraid of: a nation in which every person is bound by contracts they have never read and guilty of a federal offense for breaking.[61] Like it or not, that is the current state of affairs in most of the United States.

The Ninth Circuit was, until recently, lauded in the literature for having a more sensible interpretation of *exceeds authorized access* than the other circuit courts.[62] Then there was *Nosal 2*.[63] This opinion seems to suggest that, even in the Ninth Circuit, a website's explicit retraction of authorized access is enough to make future use of the site a criminal violation.[64] While this is still a far cry from the expansive definition other circuit courts give to the phrase *exceeds authorized access*, this new interpretation of the CFAA was more than enough to draw public outcry.[65] News agencies had a field day with the decision, claiming that it made the relatively common practice of sharing a Netflix password a federal felony.[66] Whether that is a correct reading of the case remains to be seen, as no one has yet been prosecuted on that basis. One way or another, this opinion and the news frenzy that followed show that the flaws of the CFAA's breadth are only beginning to come to light.

By contrast, the flaws with the CFAA's sentencing structure could have been predicted as early as the eighteenth century. In Jeremy Bentham's *Introduction to the Principles of Morals and Legislation*, first published in 1789, Bentham outlines four aims of utilitarian punishment.[67] He states that legislators should aim to prevent as many offenses as possible, induce criminals to commit lesser crimes, induce criminals to commit fewer crimes, and do this all as cheaply as possible.[68] These aims have become staples in Anglo-American jurisprudence, such that the

---

59. *See supra* note 38.

60. *See supra* note 38.

61. *See, e.g.*, United States v. Drew, 259 F.R.D. 449, 466 (C.D. Cal. 2009) ("[Reading Terms of Service into the CFAA] would result in transforming § 1030(a)(2)(C) into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeanant criminals.").

62. Kerr, *supra* note 35, at 1583–85.

63. United States v. Nosal, 844 F.3d 1024 (9th Cir. 2016).

64. *Id.* at 1038.

65. *See, e.g.*, *Sharing Your Netflix Password is Now a Federal Crime*, WNEP (July 11, 2016, 3:27 PM), http://wnep.com/2016/07/11/sharing-your-netflix-password-is-now-a-federal-crime/.

66. *Id.*

67. JEREMY BENTHAM, AN INTRODUCTION TO THE PRINCIPLES OF MORALS AND LEGISLATION (1789).

68. *Id.* at 92–96.

vast majority of criminal laws follow at least the first three rules.[69] The CFAA as an enforcement system in IoT fails to follow the second of these centuries-old principles: laws should induce criminals to commit "lesser crimes" that cause less social harm than others.

As it currently stands, the CFAA theoretically doles out the same punishment for sharing one's Netflix password with a friend as it does for selling the password to an unclassified government computer on the black market.[70] Similarly, most of the circuit courts find the same maximum punishment applies for lying on a dating profile as for accessing another person's bank records.[71] Bentham would no doubt have a conniption, right after someone got through explaining to him what "Netflix," "dating profiles," and "computers" were.

Of course, it should not be assumed that the CFAA is wholly blind to the need for enhanced penalties for more harmful crimes. The very fact that the statute leaves punishments in terms of the maximum term of years to be imposed suggests that the drafters knew much would need to be left to the discretion of the courts.[72] There is also a natural tension for legislators trying to make criminal statutes both simple enough to be easily understood and yet complex enough to effectively differentiate between more and less severe crimes.[73] Furthermore, there are other parts of the CFAA that do a better job of differentiating between punishments. For example, subparagraphs (a)(7) and (c)(3) of the CFAA up the punishment from one to five years if the perpetrator uses the Internet as a tool for ransom.[74]

---

69. Kent Greenawalt, *Punishment*, *in* 3 ENCYCLOPEDIA OF CRIME & JUSTICE 1282, 1286–87 (Joshua Dressler ed., 2d ed. 2002).

70. *See* 18 U.S.C. § 1030(a)(6), (c)(2)(A) (2012). There is a maximum one-year prison sentence for both. *Id.*

71. *See* 18 U.S.C. § 1030(a)(2), (c)(2)(A). Orin Kerr reportedly told Congress that the CFAA is vague enough to be used to prosecute someone for "lying about [his] weight in [his] online dating profile," based on the same logic that was used by the prosecutors in *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009). Mark I. Schickman, *An Acting Up of Congress*, 21 NO. 18 CAL. EMP. L. LETTER 3 (2011).

72. The discretionary authority afforded to federal trial judges in the United States has been on somewhat of a rollercoaster, the ups and downs of which have been tracked by Susan Klein. Susan R. Klein, *The Return of Federal Judicial Discretion in Criminal Sentencing*, 39 VAL. U. L. REV. 693, 693–95 (2005). As Professor Klein notes, this discretion was on an upswing in 2005, which was also just before the most recent series of amendments to the CFAA. *Id.* at 731.

73. This tension—whether referred to as a tension between simplicity and complexity, between discretion and uniformity, or more philosophically between justice and mercy—pervades criminal law. Carol S. Steiker, *Justice vs. Mercy in the Law of Homicide: The Contest Between Rule-of-Law Values and Discretionary Leniency from Common Law to Codification to Constitution*, 47 TEX. TECH L. REV. 1 (2014); *see also* United States Attorneys' Manual § 9-10.030, https://www.justice.gov/usam/usam-9-10000-capital-crimes#9-10.030 (noting the importance of simultaneously deciding cases "within a framework of consistent and even-handed national application" and also "allow[ing] proper individualized consideration of the appropriate factors . . . .").

74. 18 U.S.C. § 1030(a)(7), (c)(3). Concerns about "ransomware" are already flooding American businesses and news outlets. *See, e.g.*, Kim Zetter, *4 Ways to Protect*

The CFAA's best attempt to differentiate punishments based on the harm suffered comes in subparagraph (c)(4)(A).[75] This subparagraph delineates six categories of harms; a conviction for causing any of these harms carries a sentence of up to five years in prison.[76] These categories are the following: (1) loss of more than $5,000; (2) modification of medical treatment; (3) physical injury; (4) threat to public health or safety; (5) damage to a government justice, defense, or security computer; and (6) damage to ten or more computers.[77] These categories do as good a job of differentiating punishments depending on the harm as anything in the CFAA. There are also parts of the CFAA that sharply increase the punishments if death or serious bodily injury results from someone's hacking activity.[78]

The biggest problem with this enhanced-penalty section is that it only applies to one of the seven paragraphs of the CFAA.[79] To be fair, that one paragraph is also one of the broadest of the seven. It applies to nearly anyone who damages a computer after intentionally accessing it.[80] Thus, the three sections of enhanced penalties outlined above address several of the major issues predicted in IoT-related crimes: using a pacemaker or an insulin pump to kill someone results in a potential lifetime sentence;[81] using the same technology to hold a person's body for ransom results in an enhanced sentence of up to five years;[82] and even crimes undergone for political purposes run serious risk of bumping into either the $5,000-in-loss provision of the statute or the ten-or-more-computers provision.[83] However, crimes

---

Against the Very Real Threat of Ransomware, WIRED (May 13, 2016, 1:00 PM), https://www.wired.com/2016/05/4-ways-protect-ransomware-youre-target/. IoT devices add another wrinkle onto this issue: if a device can be hacked and damaged, then the hacker can theoretically hold a physical object in IoT—or even, in the case of pacemakers or other medical devices, the victim's own life, hostage—until the victim pays a certain amount of money.

75. 18 U.S.C. § 1030(c)(4)(A).

76. *Id.*

77. *Id.*

78. *Id.* § 1030(c)(4)(E), (c)(4)(F).

79. *Id.* § 1030(c)(4)(A).

80. *Id.* § 1030(a)(5) (prohibiting intentional damage, reckless damage after intentional access, and damage and loss caused by intentional access).

81. *Id.* § 1030(c)(4)(F). Of course, as addressed more fully below, murders like these would be subject to whatever sentence the jurisdiction provides for that type of murder anyways. *See infra* Part III.

82. 18 U.S.C. § 1030(a)(7), (c)(3).

83. Prosecutors have noted just how easy it is to aggregate the total losses in such cases up to $5,000 or to find ten computers that were affected in one way or another by the hacker. *See* U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 42–43 (Feb. 2007), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (noting that *loss* includes costs to restore deleted data, check for damage, re-create lost work, reinstall system software, install security measures, and make up for lost advertising or sales, and exhorting prosecutors to "think creatively about what sorts of harms in a particular situation meet this definition"). Though this would appear to be a positive in terms of the deterrent effect provided by the statute, it also reduces the differentiation between criminals who legitimately cause substantial harm to several computers at once and criminals who cause harm that can be calculated as over $5,000 only through clever mathematical manipulation.

that do not harm computers or people are generally left out of the enhanced penalties provisions.[84]

One could logically ask the following: Who cares about cybercrimes that do not harm computers or humans? The sarcastic response to this rhetorical question is that many people care very much. The man whose Amazon account is hacked into, causing him to order millions of dollars in jewelry to be shipped to an address he does not recognize, cares very much about a crime that technically never injured his person or damaged his computer.[85] The woman whose profile picture on Facebook is continually changed to GIFs of "Nyan Cat"[86] cares very much that her friends think she is now obsessed with a feline that spews rainbows. A person's identity and interactions are increasingly controlled through an online persona, one which is neither linked to that person's physical body nor to any computer.[87] A person's bank account information, birthday, height, weight, mother's maiden name, and so on have obvious importance for online privacy, but the CFAA generally does not distinguish between different types of data. The need to protect an online persona's security from hacking is relatively unaddressed by the CFAA.[88] This is the problem. Each of the examples presented in this paragraph results in a fairly substantial social harm, but these types of social harms are ignored by the CFAA. Thus, there is no express enhancement to the sentence for any of these crimes. All the hypothetical hackers referenced in this paragraph would be left with the same one-year maximum sentence as people who share their Netflix passwords with their friends.[89] It does not take Bentham to recognize that there is something wrong with that.

Prosecutorial discretion and judicial discretion provide only a partial cure for this issue. Prosecutors have considerable discretion in terms of when they will

---

In Bentham's terms, then, there is minimal disincentive for criminals to cause as much *mischief* as possible.

84. 18 U.S.C. § 1030(c)(4)(A).

85. While this would be covered by the $5,000-in-loss provision mentioned earlier, this probably does not count as *damage* under the definitions used in the CFAA. *See* 18 U.S.C. § 1030(e)(8). For better or worse, the CFAA does not apply a torts-esque definition of *damage*. As such, this situation does not fall within any of the § 1030(a)(5) violations that provide for the enhanced penalties provisions. *See* 18 U.S.C. § 1030(a)(5). That said, this crime would probably constitute another crime, such as identity theft or even just theft. It is also likely that this amount would still have to be paid to the victim as restitution, even if the rote definitions under the CFAA are not expansive enough to include these types of harm.

86. *Nyan Cat* is a cat/Pop Tart hybrid that flies through space while a Japanese synth-pop song plays. It was viewed by 54 million people in 2011. Deborah Netburn, *Talking Twin Babies, Nyan Cat Among YouTube's Top Videos of 2011*, L.A. TIMES (Dec. 20, 2011, 4:29 PM), http://latimesblogs.latimes.com/technology/2011/12/talking-twin-babies-nyan-cat-and-friday-top-youtubes-most-watched-videos-of-2011.html.

87. *See* Daniel Nernet-Nejat, *Hey, That's My Persona!: Exploring the Right of Publicity for Blogs and Online Social Networks*, 33 COLUM. J.L. & ARTS 113, 118–24 (2009).

88. *See generally* 18 U.S.C. § 1030.

89. *Id.*

charge cases, what charges they will pursue, and what sentences they will seek;[90] and judges have considerable discretion—usually—in determining what sentences they will ultimately impose on the defendant.[91] Prosecutorial discretion is a staple of American criminal law,[92] and judicial discretion is built into sentencing legislation in most jurisdictions in the United States.[93] The reason given is simple: legislators cannot possibly anticipate every possible situation that could arise in the criminal law context, so room must be left for heightened or lessened sentences when the specific crime committed by the defendant is more or less severe than the general crime prohibited by the statute.[94]

When dealing with a statute as broad as the CFAA, judicial and prosecutorial discretion are even more important than usual. Though the circuit courts may rule that the CFAA is theoretically applicable to crimes as small as violating the EULA on a website, no self-respecting prosecutor would charge a defendant based on such a harmless act, without more.[95] Even if a judge were to allow such a case to move forward, the resulting negative press directed at that particular prosecuting agency would create political backlash, pressuring the prosecutor to move to dismiss the case.[96]

---

90. *See* Robert H. Jackson, Att'y Gen. of the U.S., The Federal Prosecutor, An Address at the Second Annual Conference of United States Attorneys (Apr. 1, 1940) ("The prosecutor has more control over life, liberty, and reputation than any other person in America. His discretion is tremendous . . . [t]he prosecutor can order arrests, present cases to the grand jury in secret session . . . [h]e may dismiss the case before trial . . . [o]r he may go on with a public trial. If he obtains a conviction, the prosecutor can still make recommendations as to sentence . . . .").

91. Klein, *supra* note 72, at 731. This discretion only expanded with the Supreme Court's ruling in *United States v. Booker*, striking down the mandatory provisions of the Federal Sentencing Guidelines. 543 U.S. 220 (2004).

92. Memorandum from Bo Cooper, General Counsel, U.S. Immigration and Naturalization Service, on INS Exercise of Prosecutorial Discretion, at 2 (available at INS and DOJ Legal Opinions § 99-5 MB 2006) ("The idea that prosecutor is vested with broad discretion in deciding when to prosecute and when not to prosecute is firmly entrenched in American law.").

93. Klein, *supra* note 72.

94. *See, e.g.*, 18 U.S.C. § 3553(a) (2012) (mandating that courts in sentencing consider such individualized factors as the nature and circumstances of the offense and the history and characteristics of the defendant).

95. There are always exceptions. The prosecutors in *United States v. Drew* raised precisely this charge, but the real reason was because a teenage girl had killed herself after the defendants conspired to use a fake MySpace profile to have a fabricated teenage boy tell her that "the world would be a better place without her in it." 259 F.R.D. 449, 452 (2009). This case illustrates how creative prosecutors can use the CFAA to charge misconduct that otherwise slips through the cracks of existing criminal statutes, and how such creativity can often be rejected on constitutional grounds.

96. Even in the case of *United States v. Drew*, the Electronic Frontier Foundation called the prosecutor's charging decision an "unprecedented, extraordinary, and dangerous extension of federal criminal law." Brief of Amici Curiae Electronic Frontier Foundation, in Support of Defendant's Motion to Dismiss Indictment for Failure to State an Offense and for

Still, it will be cold comfort to some to learn that the only thing standing between their violations of Facebook's EULA and a federal prison is the discretionary judgment of some federal prosecutor they have never met.[97] In terms of the sentencing discretion given to the judiciary under the CFAA, the fact that judges can give the maximum sentence to offenders whose crimes they deem more severe while reducing the sentence for offenders with less severe crimes certainly helps the CFAA align with the deterrent needs of cybercrimes prosecution in IoT.

But judicial and prosecutorial discretion fail to completely cure the issue. Obviously, the one-year maximum set on one of the broadest sections of the statute is just that—a hard cap on judicial discretion. Even in instances where the information or control obtained through unauthorized access to the protected computer is incredibly valuable or potentially harmful, the one-year cap still applies unless the prosecutor can prove one of the other six subsections of the CFAA, triggering the enhanced-penalty provisions.[98] The risk of detection and prosecution is so small for many cybercrimes today[99] that it only makes that one-year maximum even smaller in terms of its deterrent effects.

In the context of IoT, this problem of insufficient detection is even worse than in most cybercrime contexts. The relative simplicity of most devices in IoT renders them both more susceptible to hacking and less capable of identifying the hacker than more traditional Internet-linked devices.[100] Less detection means less prosecution and less deterrence. When a potential criminal weighs the benefits to be gleaned from hacking an IoT device against the minimal risk of being caught and jailed for a maximum of two years for hacking a device that cannot encrypt its data or even register the breach in most cases, the choice is obvious: hacking is worth the risk.

Though the primary fix for this issue must come in the form of better detection, as addressed more fully in Part III, modifications to the CFAA could also help. Most importantly, the sentence-enhancement provision for causing damage to a computer should be adapted to the section about accessing information online without authorization. To do this, the value of the information itself and the value of the control gained by accessing that information would have to be given some type of differentiation.

Vagueness, United States v. Drew, 259 F.R.D. 449 (2009) (No. CR-08-05282-GW), https://www.eff.org/files/filenode/US_v_Drew/drew_amicus.pdf.

97. This is really not that rare of a situation, unfortunately. There are several criminal statutes, other than just the CFAA, that are written quite broadly. One writer has even suggested that the average American commits roughly three felonies a day. HARVEY SILVERGATE, THREE FELONIES A DAY: HOW THE FEDS TARGET THE INNOCENT (2009).

98. 18 U.S.C. § 1030(c)(4)(A), (c)(4)(G) (2012).

99. *See infra* Part III.

100. *See infra* Part III.

One rough method of accomplishing this would be to differentiate between ordinary "protected computers"[101] and computers that need even more protection than the average.[102] In fact, a simple structure for doing this is already built into the wording of the CFAA.[103] Subsection (a)(2) draws a distinction between information obtained from the U.S. government, financial institutions, or just any other protected computer.[104] It would be easy to increase the maximum sentence for violators who illegally access government computers and decrease the maximum sentence for violators who access ordinary protected computers. Making this simple dichotomy would significantly improve the structure of the CFAA to reflect different data security needs. With a bit more effort, this same improvement could be extended from two categories of information to five or six, each receiving stronger or weaker levels of protection based on the importance of the data.

Devices in IoT could certainly benefit from this more discerning punishment structure. The information stored on an Amazon Echo, for instance, is likely much more important than the data stored on a Fitbit.[105] One might logically expect that the more important data would receive more protection through a harsher punishment for unlawfully accessing it. The CFAA fails to successfully make this distinction, in part because the statute's own provisions undo any sentencing variation they appear to create. For example, data that is worth more than $5,000 is already protected by a five-year sentence rather than the typical one-year sentence.[106] But this attempt at sentencing variation is functionally undone by a previous section, which makes any CFAA violation that furthers any crime or tort punishable by a maximum of five years in prison.[107] As scholars have pointed out, it is difficult to imagine any example of taking someone else's data over the Internet without authorization that is not in furtherance of at least some crime or tort in some jurisdiction.[108] The statute's broad-strokes approach to regulation of the Internet comes back to haunt it. The ultimate result is that, as things currently stand, the

---

101. As addressed above, this definition is very inclusive. 18 U.S.C. § 1030(e)(1)–(2) (defining a protected computer as any processing device performing at least storage functions and affecting interstate commerce).

102. The history of the CFAA shows that certain computers were protected before others. Presumably, these were the computers in most urgent need of protection. *See* Kerr, *supra* note 35, at 1563–64 (showing that the first CFAA protections were for government and financial computers).

103. *Compare* 18 U.S.C. § 1030(a)(2)(A) (financial computers), *and* 18 U.S.C. § 1030(a)(2)(B) (government computers), *with* 18 U.S.C. § 1030(a)(2)(C) (any computer affecting interstate commerce).

104. *See supra* note 103.

105. The Amazon Echo line of products can record the user's voice and can be used to make purchases from the Amazon website. AMAZON, https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/dp /B00X4WHP5E (last visited Sept. 3, 2017). By contrast, a Fitbit generally records only biometric data for health purposes. *See Our Technology*, FITBIT, https://www.fitbit.com/technology (last visited Sept. 3, 2017).

106. 18 U.S.C. § 1030(c)(4)(A)(i)(I).

107. 18 U.S.C. § 1030(c)(2)(B)(ii).

108. *See, e.g.*, Timothy P. O'Toole, *Digital Defense: Meeting the Challenges that the Computer Fraud and Abuse Act Poses*, 37-OCT Champion 44, 48 (2013).

maximum punishment of five years stands for a whole swath of both cybercrimes in IoT and more conventional cybercrimes.[109]

II. ORDINARY CRIMINAL LAW AS APPLIED TO IOT

Fortunately, criminal statutes outside the context of the Internet are generally written in method-neutral terms, making them just as applicable to IoT crimes as to other real-world crimes.[110] In other words, murder is murder whether it is carried out by means of a sword, a gun, or a laptop.[111] The logic for this is simple: Anglo-American criminal law is built on principles of retribution and utilitarian deterrence, and thus criminal statutes depend primarily on the type of social harm caused and the mental state of the criminal.[112] By writing criminal statutes in broad terms with respect to method, legislatures avoid having to revise the law every time a well-versed criminal finds a new method to commit an old crime, and prosecutors can get guilty verdicts if the defendant's guilt is proven, even if the method of carrying out the crime is unknown.[113]

Naturally, there are exceptions to this general rule that the method of carrying out a crime does not affect its punishment.[114] A number of criminal statutes provide for aggravated, enhanced, or otherwise lengthened sentences for crimes carried out in a certain manner.[115] Other statutes provide completely different elements for crimes carried out in misuse of various pieces of infrastructure.[116]

---

109. *See supra* notes 75, 77, 83, 106–08.

110. *See, e.g.*, COLO. REV. STAT. ANN. § 18-3-102 (2000) (method-neutral murder statute in Colorado); ARIZ. REV. STAT § 13-1105 (2009) (same in Arizona); 18 PA. CONS. STAT. § 2502 (1978) (same in Pennsylvania); *but see* NEB. REV. STAT. § 28-303 (2015) (making homicide automatically first-degree murder when committed by poison).

111. *See supra,* note 110.

112. *See* Hopt v. Utah, 110 U.S. 574, 579 (1884) (utilitarian); Gregg v. Georgia, 428 U.S. 153, 183–84 (1976) (retributivism); CAL. PENAL CODE § 1170(a)(1) (West 2017) (listing punishment, rehabilitation, and restorative justice as viable theories of sentencing, with the ultimately utilitarian goal of preserving the safety of the community); MODEL PENAL CODE: SENTENCING § 1.02(2)(a) (AM. LAW INST. Tentative Draft No. 1, 2007) (listing rehabilitation, general deterrence, incapacitation, restoration, and reintegration as legitimate goals of sentencing). Deterrence theories in particular necessarily implicate the mens rea or mental state of the defendant, since awareness of the offense soon to be committed is a prerequisite to recognition of potential punishments that may result.

113. For an entertaining list of interesting murder weapons throughout history, see Petr H., *25 of the Most Bizarre Murder Weapons Ever*, LIST 25 (Jan. 6, 2015), http://list25.com/25-of-the-most-bizarre-murder-weapons-ever/..

114. *See, e.g.*, ARIZ. REV. STAT. ANN. § 13-1204(A) (2017) (turning an assault charge into an aggravated assault charge if committed by a "deadly weapon or dangerous instrument," or even "a simulated deadly weapon," in addition to other method-neutral provisions relating to the intent or extent of the injury).

115. *See, e.g., id.*

116. There are a litany of federal fraud statutes, several of which are dependent on the method used to perpetrate the fraud. *See, e.g.*, 18 U.S.C. §§ 1005 (2012) (bank fraud), 1030 (2012) (computer fraud), 1037 (2012) (email fraud), 1341 (2012) (mail fraud). Some of this distinction is a reflection of the different constitutional provisions that enable each statute,

Generally speaking, though, ordinary criminal laws can be applied to crimes carried out by means of IoT devices.[117]

Thus, murder committed by an 830-volt shock from a pacemaker is still murder,[118] and criminally damaging a car by remotely applying its brakes is still criminal damage.[119] The means do not decriminalize the ends, so to speak. Fortunately, the security concerns about IoT products tend to arise in areas where the social harm is already criminalized.[120] All of this means that the scope of existing criminal statutes will typically cover the IoT counterparts of more traditional and familiar crimes.[121]

That the scope of these statutes is sufficient to cover IoT crimes does not mean that the enforcement systems used for ordinary criminal laws will be adequately adapted to IoT crimes. Specialized police and prosecutors are necessary to effectively identify, charge, and try defendants for cybercrimes generally.[122] Cybercrimes raise unique issues not commonly seen in other areas of the law: identifying the defendant beyond a reasonable doubt based primarily on an IP address, questioning a computer-forensic expert to explain the significance of a defendant's search history or use of hard-drive cleaning software, and navigating the jurisdictional and legal eccentricities of law applied to the Internet.[123] IoT will raise even more eccentricities on top of these, especially in that the victim device—the device hacked into or otherwise improperly used—will generally be far less sophisticated than computers and servers hacked as part of a more traditional

---

but the fact remains that there are different statutes and different penalties for frauds carried out by different means.

117. *See supra* note 110 and accompanying text. Anecdotally, the otherwise method-neutral criminal statutes the Author has interacted with do not include a section stating "this statute does not apply if the crime is carried out using an Internet of Things device," for obvious reasons.

118. *See, e.g.*, ARIZ. REV. STAT. ANN. § 13-1105 (2009) (including this act in the definition of first degree murder).

119. *See, e.g.*, ARIZ. REV. STAT. ANN. § 13-1602(A)(2) (2015) (including this act in the definition of criminal damage).

120. In addition to the security concerns cited in notes 118–19, the other examples addressed in this Note could, for the most part, also be charged under traditional criminal statutes. The coffee-maker burglary example addressed in note 29 and Part IV, for example, could be charged as burglary and conspiracy. The ransomware concerns in note 69 could theoretically be charged as theft or criminal damage. The Amazon account hacking in note 81 is identity theft and theft. Even the *Nyan Cat* profile picture hacker in note 82 could—though this would be quite a stretch—be charged with criminal copyright infringement.

121. *See supra* notes 117–20.

122. Even as early as 2001, then-incoming president of the National District Attorneys Association Kevin P. Meenan noted the need to help the nation's prosecutors meet the challenge of cybercrime. *New NDAA President Vows to Respond to Cybercrime and Attacks on Prosecutors*, 35-OCT Prosecutor 8 (2001) (noting the need to assist prosecutors in using technology to fight crime and quickly respond to challenges).

123. *See* U.S. DEP'T OF JUSTICE, *supra* note 83, at 113–19, 173–84.

cybercrime.[124] As the Internet—and particularly, IoT—makes up a wider and wider slice of American life, the number of crimes perpetrated using the Internet will naturally increase as well. Even if the old laws still apply, those laws will do little to protect cyberspace and IoT if law enforcement agencies and prosecutors are not ready to enforce the laws in a new arena.

III. LAW ENFORCEMENT'S UNPREPAREDNESS FOR DETECTING CRIMES IN IOT

As a general rule, modern local prosecutors' offices only have dedicated cybercrimes divisions if the corresponding county's population is large enough to justify it—and it rarely is.[125] This raises concerns that the special resources and training necessary to prosecute these kinds of crimes may not be available at the local level.[126] Of course, it should not be assumed that the absence of an official cybercrimes unit on an organizational chart implies a complete lack of specialized cybercrimes prosecutors. As is common practice in large offices in all areas of law, it is likely that many large counties have go-to cybercrimes prosecutors who understand the special issues that arise in this area of law. However, the lack of a formally defined cybercrimes unit may suggest that most district attorneys do not yet see cybercrime as a major priority.

The possible reasons for this are many, but the two most obvious are that prominent cybercrimes are still rare[127] and that they almost automatically fall within

---

124. *See* Brian Buntz, *11 IoT Predictions for 2017*, INTERNET OF THINGS INST. (Nov. 10, 2016), http://www.ioti.com/iot-trends-and-analysis/11-iot-predictions-2017 ("At present, the industry uses machines that are frankly fairly dumb.").

125. *See, e.g.*, *Organization Chart*, OFFICE OF THE DIST. ATTORNEY FOR THE CTY. OF SONOMA (Nov. 17, 2016), http://www.sonoma-county.org/district_attorney/documents/DA_orgchart.pdf (no dedicated cybercrimes unit in a county of roughly 500,000 people); *Organization Chart*, OFFICE OF THE DIST. ATTORNEY FOR THE CTY. OF SAN DIEGO (2015), http://sandiegodaannualreport.com/wp-content/uploads/2016/03/org_chart15.pdf (no dedicated cybercrimes unit in a county of roughly three million people); *but see Organization Chart*, OFFICE OF THE DIST. ATTORNEY FOR THE CTY. OF L.A. (June 1, 2016), http://da.lacounty.gov/sites/default/files/June%202016%20Org%20Chart.pdf (dedicated High-Tech Crime unit in a county of 10 million people, the largest in the U.S.).

126. The Los Angeles District Attorney's Office—one of the few that has a dedicated cybercrime unit—points out the special training necessary to handle computer-related crimes, as well as the forensic equipment, business partnerships, and rapid-response teams necessary to investigate this specialized area of crime. *Cyber-Crime*, L.A. CTY. DIST. ATTORNEY'S OFFICE, http://da.co.la.ca.us/operations/cyber-crime (last visited Apr. 26, 2017).

127. Security group Kaspersky Lab notes that amateur and copycat cybercriminals have recently come onto the ransomware scene en masse, mainly by wholesale replication of existing Trojan horses. Kaspersky Lab, *Story of the Year: The Ransomware Revolution*, KASPERSKY SECURITY BULLETIN 11 (2016), http://media.kaspersky.com/en/business-security/kaspersky-story-of-the-year-ransomware-revolution.pdf. A related issue is the fact that cybercriminals are very rarely caught. *Id.*; *see also* Roger A. Grimes, *Why Internet Crime Goes Unpunished*, CSO ONLINE (Jan. 10, 2012), http://www.infoworld.com/article/2618598/cyber-crime/why-internet-crime-goes-unpunished.html.

the jurisdiction of state and federal prosecutors when they do occur.[128] Only a small fraction of the population even knows how to commit a cybercrime worth prosecuting.[129] Those who can pull off sophisticated exploits, however, can do immeasurably more damage through a single cybercrime than most traditional criminals ever cause.[130] The FBI recognizes this threat, calling it "incredibly serious—and growing."[131] This severity, coupled with the inherent federal interest in protecting the Internet—itself a spawn of the Department of Defense[132]—suggests why so many cybercrimes are left to be investigated by the FBI and prosecuted by the applicable U.S. Attorney's Office.

Federal authority over cybercrimes enforcement has its upsides—it means that Assistant U.S. Attorneys can pursue charges under the CFAA along with ordinary criminal charges, and it avoids jurisdictional headaches that might arise if a local agency were to prosecute an out-of-state defendant for harm suffered inside the county.[133] It also means that only established prosecutors and extensively trained

---

128. The Internet clearly affects both multiple counties within a state and multiple states, and as such it fits the typical jurisdictional limits for both state and federal prosecutor's offices. *See, e.g.*, United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) (finding that proof of an Internet connection generally satisfies the interstate commerce jurisdiction requirement); United States v. Jones, 580 F.2d 219, 222–24 (6th Cir. 1978) (affirming judgment of acquittal where federal prosecutor failed to prove the interstate commerce nexus); *About the Office of Attorney General*, ARIZ. ATTORNEY GEN., https://www.azag.gov/about (last visited Apr. 27, 2017) (noting that the Attorney General's jurisdiction is limited to enumerated crimes and crimes committed in more than one county).

129. This is not to say that most people do not commit cybercrimes. Quite the contrary, millions of people unknowingly or carelessly violate either copyright law or the CFAA through everyday activities like redistributing videos, sharing Netflix passwords, and lying on dating profiles. These activities generally harm only the copyright holder or the Tinder user who suddenly wonders why her date is five-foot-six when his profile clearly stated six-foot-two. These types of crimes are typically best resolved by either sending a DMCA takedown notice or forcing him to pick up the check rather than bringing the weight of a criminal prosecution to bear. By contrast, cybercrimes that substantially affect the function of one or more devices, or that steal data or money, are generally best left to law enforcement.

130. The reason for this is the breadth of the Internet and the replicability of crimes carried out by code. Simply put, if a code can be run once to steal data from one device, it can be run several times to steal data from other devices. *See* Grimes, *supra* note 127. A related issue is the fact that, if an experienced hacker can create a certain hacking tool or method, novice hackers—termed *script kiddies*—can replicate the same hack with minimal effort.

131. *Cyber Crime*, FBI, https://www.fbi.gov/investigate/cyber (last visited Apr. 28, 2017).

132. For a brief history of the Internet, see *ACLU v. Reno*, 929 F. Supp. 824, 830–32 (E.D. Pa. 1996).

133. Though cybercrime jurisdiction is generally considered to exist so long as the harm is felt in the prosecuting jurisdiction, the cases on the fringe of this jurisdictional bound always raise at least some litigation risk. Depending on the policy of the local prosecutor, this risk may cause the prosecuting office to either drop the case or offer more generous plea deals than they might otherwise consider. Extradition is a related issue, and the main cybercrime hubs of the world—Russia, China, and the United States—do not always cooperate with each other. Roger A. Grimes, *5 Reasons Internet Crime is Worse than Ever*, CSO ONLINE (Aug. 5,

FBI agents have their hands in what can be a thorny area of practice.[134] That said, federal enforcement is generally disfavored in criminal law as a matter of tradition and policy.[135] If criminal prosecution is rightly understood in some retributivist's terms as a sort of communal expression of wrath for wrongdoing,[136] then it only makes sense to limit that community to a small-enough region to ensure that communal mores are as consistent as possible. This and other theories have led criminal law to join family law and education law as bastions of state power upon which the federal government may not tread.[137] On a more practical note, the sheer volume of cybercrimes committed may soon overcome any federal efforts to curb its growth as the population becomes more technology literate and the number of hackable devices continues to skyrocket.[138]

This suggests that existing law enforcement agencies and prosecutors' offices will need to make drastic changes to keep up with the impending uptick in cybercrime.[139] Ordinary line prosecutors will need more training on issues particular to IoT devices, law enforcement will need to be trained to investigate such devices and preserve them from an evidence standpoint,[140] and officially designated

---

2014), http://www.infoworld.com/article/2608631/security/5-reasons-internet-crime-is-worse-than-ever.html#tk.drr_mlt.

134. One of the particular tricks here is not tipping off the defendant to the investigation until sufficient evidence has been built up to obtain not only an indictment but a verdict. CCleaner and other data-purging software is too readily available and too effective a clean sweep for a prosecutor to be able to indict before gathering all the evidence that will be necessary before proceeding to trial. CCleaner for Mac, for example, can be downloaded for free. *CCleaner for Mac*, CNET (May 31, 2014), http://download.cnet.com/CCleaner/3000-2144_4-75453127.html. For an example of such data-wiping in a civil discovery context, see *S. New England Tele. Co v. Global NAPs, Inc.*, 251 F.R.D. 82, 88–89 (D. Conn. 2008) (finding that defendant had used "Window Washer" software to wipe important hard drives that would have been subject to discovery and granting plaintiff's motion for default judgment for willful violation of the court order). Though spoliation-of-evidence jury instructions would seem to solve this issue, the fact of the matter is that it takes expensive expert analysis to analyze metadata and find out if such software was used. Run-of-the-mill criminal cases just do not justify that kind of expense. *See id.*

135. Assistant U.S. Attorneys are not supposed to prosecute cases if the defendant "is subject to effective prosecution in another jurisdiction" or if there is "an adequate non-criminal alternative to prosecution." U.S. ATTORNEYS' MANUAL 9-27.000 § 9-27.220, https://www.justice.gov/usam/usam-9-27000-principles-federal-prosecution#9-27.220.

136. One early example of this theory comes from James Fitzgerald Stephen, who called it "highly desirable that criminals should be hated" and said that criminal punishment is an "expression [of] that hatred." JAMES FITZGERALD STEPHEN, A HISTORY OF THE CRIMINAL LAW OF ENGLAND 80–82 (1883).

137. *See* United States v. Lopez, 514 U.S. 549, 564 (1995) (noting the historical sovereignty of states in areas of family law, criminal law, and education in overturning a national ban on firearm possession near schools).

138. *See supra* note 23 and accompanying text.

139. Cybercrime as a whole just keeps growing. In the ransomware context in particular, the attacks on small businesses tripled just between January and September of 2016, and the attacks on individuals doubled. Kaspersky Lab, *supra* note 127, at 3.

140. One particularly fascinating department policy issues every police officer a roll of ordinary aluminum foil along with the badge and belt. Officers who seize cell phones

cybercrimes units will have to become more commonplace to afford the necessary training and resources to an ever-expanding new group of "cyber-prosecutors."[141] The same will likely happen on the defense side of the criminal bar, as public defenders will see the need for special training in cybercrime and private defense attorneys will find more market opportunity to specialize in this field.

IV. REFOCUSING AND REPURPOSING EXISTING CRIMINAL LAWS FOR IOT

Neither the CFAA nor ordinary criminal statutes were designed to operate in IoT.[142] Because of the rapid growth of IoT technologies, prosecution agencies have begun to teach their line attorneys how to apply these older statutes to the new crimes made possible by IoT.[143] Creativity in charging decisions, not often considered a virtue, is essential in cybercrimes prosecution.[144] The simple reason is that the cybercriminal of today is a moving target.[145] Cybercrimes are committed in new ways, to achieve new ends, and against new victims every day.[146] Each time a new exploit or hacking tool is developed, internet-security researchers must

---

are instructed to wrap the phone in three layers of the foil to prevent the device from being remotely wiped while it is in evidence. Bob Sorokanich, *Warrant or No, Cops Can Use Aluminum Foil to Block Smartphone Wiping*, GIZMODO (Aug. 28, 2013, 12:10 PM), http://gizmodo.com/warrant-or-no-cops-can-use-aluminum-foil-to-block-smar-1214921221.

141. For just a sampling of the new cybercrime units that have popped up in the United States in the past few years, see Doug Chartier, *Federal Prosecutors Launch New Cyber Crime Unit in Colorado*, LAW WEEK COLO. (Feb. 1, 2017), http://lawweekcolorado.com/2017/02/federal-prosecutors-launch-new-cyber-crime-unit-colorado/; *Federal Prosecutor's Office in Atlanta Adds Cybercrime Unit*, FOX 5 ATLANTA (Nov. 22, 2016, 11:32 PM), http://www.fox5atlanta.com/news/219316949-story.

142. For the legislative history of the CFAA, see U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 1–3 (Scott Eltringham ed., Feb. 2007), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf; Kerr, *supra* note 35, at 1563–71. Pertinent criminal law statutes, such as the murder, assault, and theft statutes, have been on the books since they were adapted from their common-law counterparts in the late-nineteenth century. For the legal theory debates that led to this adaption, see Gerald Leonard, *Towards a Legal History of American Criminal Theory: Culture and Doctrine from Blackstone to the Model Penal Code*, 6 BUFF. CRIM. L. REV. 691, 756–74 (2003).

143. U.S. DEP'T OF JUSTICE, *supra* note 83, at 149–55.

144. *Id.* at 43 ("Prosecutors should think creatively about what sorts of harms in a particular situation meet [the CFAA's definition of loss]."). The same can be said of artful pleading in the civil context. *See* CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1023 (S.D. Ohio 1997) (finding that unsolicited emails avoiding plaintiff's technological blocking measures were actionable under the centuries-old tort theory of trespass of chattels).

145. New hacking techniques and exploits are developing at an alarming rate. For example, hackers are now able to use the physics of computers to break through some encryption protocols in a process called *Rowhammer*. Andy Greenberg, *Forget Software—Now Hackers are Exploiting Physics*, WIRED (Aug. 31, 2016, 7:00 AM), https://www.wired.com/2016/08/new-form-hacking-breaks-ideas-computers-work/.

146. *See, e.g.*, *id.*

scramble to address it.[147] Legislators and law enforcement cannot afford to be behind on this issue.

Even with the statutes currently available, prosecutors and police can probably handle many of the cybercrimes that can happen in IoT—for now, at least.[148] Because so much of modern criminal law is based on the social harm suffered rather than the methods used, law enforcement can easily apply familiar statutes, albeit in unfamiliar areas of work. The main limit is on the ingenuity of the investigators to determine the purpose of the hack.

For example, suppose a hacker accesses the Internet-linked coffee-makers of a dozen of the richest people in the area.[149] The hacker never uses this control over the coffee-makers to make a pot of joe, or worse, to prevent these social elites from getting the caffeine they need in the morning, so many people are left to wonder why the hacker bothered with the hack in the first place. If law enforcement officers just leave it at that, without investigating into what information was obtained, the crime will likely go unsolved for some time. Suppose further that, as time goes on, mysterious reports of burglaries begin to pop up. Each of the homes of these wealthy people is burglarized while the homeowner is away on vacation. It is only after the crimes have been perpetrated that police pick up on how the crimes were connected: the hacker accessed the coffee-makers and monitored them to see when they had been turned off for a week or more. Based on that information, the hacker had a solid guess that the homeowner was out of town for a while. The hacker then had the choice to either do the dirty work personally and burglarize the houses for pure profit, or sell the information to teams of burglars who would be happy to share in the risk of getting caught if it meant an equal share in the proceeds.

If, instead, the police could understand ahead of time what motives a person could have for hacking an IoT coffee-maker, then they could ask for the homeowners' permission to set up video surveillance around the houses affected. When the hacker or the hired burglars broke into the house, the police would arrive shortly thereafter—or, better yet, be surveilling the house and waiting for them—and arrest the lot of them on both burglary and hacking charges. Even if the hacker chose not to participate in the burglary directly, and if the police were unable to track this perpetrator through an IP address, the prosecutors would likely still be able to leverage one or two of the burglars into revealing the source of their information.

Other examples of how IoT devices could be used for crime abound. Smart cars could be hacked to take the passengers to places they never meant to go, smart houses could be hacked to just generally ruin someone's day, and even things as

147. *See, e.g.*, Elizabeth Weise, *Security Experts Scramble to Plug "Bash Bug" Hole*, USA TODAY (Sept. 25, 2014, 11:43 AM), https://www.usatoday.com/story/tech/2014/09/25/bash-bug-computer-security-shellshocked/16203647/.

148. *See supra* Parts I and II.

149. This idea is drawn from Harmon, *supra* note 24 ("It's possible for your 'smart' coffee maker to clue burglars as to your customary wake-up time.").

simple as a Fitbit could potentially provide a hacker with personal information about the victim's height, weight, sex, step count, and sleeping habits.[150]

Hackers are, almost by definition, smart; and to keep up with their methods, law enforcement officers will have to be smarter.

V. INTRODUCING A SUPPORTING CIVIL STRUCTURE TO IMPROVE ENFORCEMENT

Changing the criminal statutory framework and the structure of law enforcement agencies solves only part of the problem. Greater issues that will plague prosecutors and law enforcement officers in dealing with crimes committed in IoT include detecting that a crime has occurred,[151] identifying the device or devices used in an exploit,[152] and determining who was using the device when a crime occurred. Furthermore, if the suspect resides outside the United States, the prosecutor must go through more hoops to extradite the defendant and make use of Mutual Legal Assistance Treaties ("MLATs") in place of garden-variety warrants and subpoenas.[153] Crimes in IoT, other than run-of-the-mill data breaches, may be easier to detect than most cybercrimes because of their real-world implications. At the same time, IoT crimes may be even more difficult to trace back to a suspect than most cybercrimes because the victim's IoT device is unlikely to have an interface

150. This type of data seems innocent enough, but when coupled with information from other sources, it has the potential to provide a hacker with the identity of the person whose Fitbit he has hacked into. From there, the hacker could figure out when the victim is out for a run, and use the victim's name to identify the victim's address. Once again, we have the same sort of situation as with the coffee-maker, and a simple Fitbit has just made the victim a target for burglary or worse. For an explanation of the issues of de-anonymizing data like this, see Peppet, *supra* note 33, at 129–33.

151. Unlike ordinary crimes confined to the physical world, clever hackers who breach security protocols to access personal data relating to an IoT device may have the ability to erase any hint of their presence from the "crime scene." *How to Cover Your Tracks & Leave No Trace Behind on the Target System*, NULL-BYTE (Aug. 9, 2013, 12:38 PM) ("In this guide, I'll show you a few ways that we can cover our tracks, making it VERY difficult for a system admin, forensic investigator, or law enforcement agent to track our malicious activities.").

152. Through use of botnets and IP spoofing, hackers are able to make use of intermediary computers to carry out the legwork of their exploits. *See Bots and Botnets—A Growing Threat*, NORTON, https://us.norton.com/botnet/ (last visited Apr. 29, 2017). This effectively frames the owner of the intermediary computer, who may not even know that her computer was part of a botnet.

153. Depending on the country and the company holding the needed data, these two processes can range anywhere in difficulty from simple to impossible. Roger A. Grimes, *Why It's So Hard to Prosecute Cyber Criminals*, CSO ONLINE (Dec. 6, 2016, 3:00 AM), http://www.infoworld.com/article/3147398/security/why-its-so-hard-to-prosecute-cyber-criminals.html ("We have established cross-boundary, reciprocal legal rules with many cyber allies, but many more countries don't and won't participate. China and Russia will never honor our warrants of arrest any more than we would honor theirs.").

sophisticated enough to provide law enforcement much useful information without using data-extraction software.[154]

Because of these various practical difficulties, cybercrimes prosecutors have been stymied despite the broad scope of the CFAA and other statutes like it.[155] Such difficulties in enforcement reduce the deterrent effect of these statutes.[156] Without a fix for the enforcement difficulties, refocusing the sentencing structure of the CFAA as proposed in this Note will have little to no effect on deterring wrongful conduct.

A number of possible solutions to these enforcement issues immediately come to mind. One would simply be to throw money at the problem, theoretically increasing the quality and quantity of prosecutors and law enforcement officers working in cybercrimes. This method shows little promise, in part because no reasonable amount of funding could put cybercrime prosecutors on par with even junior associates at Big Law firms in terms of salaries.[157] Another solution would be to keep the same personnel and provide them with better equipment and resources. For offices with outdated equipment, this technique may be helpful, even necessary. However, even the best investigators working with the best equipment will never be able to track a crime unless there is some trace to follow. The inherently limited interface of most IoT devices gives hackers more limitations in the types of data

---

154. Some examples illustrate this point. Many Fitbits have screens no larger than half an inch. *Fitbit Flex*, CNET (last visited Aug. 14, 2017), https://www.cnet.com/products/fitbit-flex/specs/. The Amazon Echo has no screen, and the user has to communicate with the device mainly through speech. Ry Crist & David Carnoy, *Amazon Echo Review: The Smart Speaker that Can Control Your Whole House*, CNET (July 18, 2017), https://www.cnet.com/products/amazon-echo-review/. Even these fairly sophisticated products are unwieldy for law enforcement purposes. Data extraction, or at least a smartphone app interface, is necessary before police can analyze data from these devices.

155. One security researcher claims that "[f]or every [cybercriminal] that gets caught, 10,000 go free." Grimes, *supra* note 153.

156. This concern should be familiar to practitioners and scholars in the field of Internet copyright. A potential criminal worried about jail time theoretically weighs the benefit to be obtained by committing the crime against the perceived risk of being caught, convicted, and sentenced to prison. *See* Peter S. Menell, *This American Copyright Life: Reflections on Re-Equilibrating Copyright for the Internet Age*, 61 J. COPYRIGHT SOC'Y U.S. 235, 359 (2014). Draconic sentences that are rarely enforced amount to a minimal risk. In some cases, consistent slaps on the wrist would give—by sheer irritation, if nothing else—more deterrent effect than rare but harsh sentences.

157. Presumably, those who pursue prosecution rather than other fields of law do so more for psychic benefits than financial ones. At last count, junior associates at the top few firms can make up to $180,000 a year. Elizabeth Olson, *Law Firm Salaries Jump for the First Time in Nearly a Decade*, N.Y. TIMES (June 6, 2016), http://www.nytimes.com/2016/06/07/business/dealbook/law-firm-salaries-jump-for-the-first-time-in-nearly-a-decade.html. By contrast, even Assistant U.S. Attorneys with a few years of experience under their belts are unlikely to make six figures. *Administratively Determined Pay Plan Charts*, U.S. DEP'T OF JUSTICE: OFFICES OF THE U.S. ATTORNEYS, https://www.justice.gov/usao/career-center/salary-information/administratively-determined-pay-plan-charts (last visited Apr. 29, 2017).

they can transmit to and from these devices, but it also leaves these devices without means to store information about how they were accessed, and by whom.

To solve this detection problem, either the design of the IoT device must make unauthorized access a complete impossibility or at least an economic infeasibility, or the device must store some type of identifying information about each other device used to access it, sufficient to provide law enforcement with the first bread crumb to find the perpetrator. These proposed solutions to the traceability problem were not drawn randomly from a hat. Each proposal corresponds, at least roughly, to one of Lawrence Lessig's Four Forces.[158] Complete impossibility of unauthorized access is only attainable through clever and elegant design of the code-based "architecture" of the device.[159] Economic infeasibility will be assessed by whether market forces make each method of breaching the device a pointless venture.[160] The storage of identifying information is only effective if there are laws in place with sufficient scope and severity to punish and deter harmful conduct.[161] Inherently, all three solutions rely on code, with the first being a purely code-based solution, while the others are hybrids of code and other forces.[162]

The viability of each of these three methods depends on the application of the device. For simple IoT devices mainly used for low-importance data recording,[163] it may be enough to ensure that there is no economic benefit to be obtained by hacking into such devices and stealing their data. The deterrence lies in the difficulty of hacking a device. For example, Fitbits and similar products

158. *See* LAWRENCE LESSIG, CODE: VERSION 2.0, at 123–24 (2006) (introducing the idea that four regulatory forces control interactions in cyberspace: law, code as the "architecture" or "nature" of the web, economic market forces, and social norms).

159. *Id.* at 124–25.

160. *Id.* at 124.

161. The careful reader will note that only three of Lessig's Four Forces have been addressed here. Social norms are conspicuously absent from this analysis for a number of reasons, chief among them the fact that social norms have minimal effect on actors who cannot be identified, and the purpose of this analysis has been to make hackers identifiable. Though law is another force requiring identification of the actor, law has a supreme advantage over social norms in that teams of government employees—law enforcement officers—seek to identify individuals who break the law, whereas no comparably strong body exists for identifying social pariahs.

162. Lessig must also be credited with the proposal of hybrid interactions such as these. *See* LESSIG, *supra* note 158, at 125–27.

163. Good candidates for this type of unregulated protection include the Internet-linked refrigerator and the smart toothbrush. If a hacker decides to go to all the effort of cracking into some poor law student's mini-fridge, the hacker's two options will be to either check whether that student's milk has gone sour or to buy the student eggs. Either way, the student is unlikely to complain. This example is illustrative of an overarching consideration applicable to all devices in this unregulated category: these devices must not store complete payment information on the device. Otherwise, the mini-fridge intended for convenience in food purchases will turn into a convenient way for criminals to steal thousands of dollars. However, there is an even bigger issue lurking here. Hackers can leverage their access to one device to gain access to a linked device. Thus, the security needs of a device depend not only on the value of the information stored on that device, but on the value of the data stored on all linked devices.

generally communicate through Bluetooth[164] or another short-range communication system, so there is no way to efficiently gather the data from several of the devices at once.[165] If this security norm were to become a security regulation, all devices with low-value data would be protected from hacking by this pragmatic barrier.[166] Thus, any economic incentive to hack into low-value devices to retrieve their data would be greatly diminished.

For IoT devices that require long-range communication with a number of different devices, or IoT devices that control functioning mechanics in the real world, economic forces may never be sufficient to remove the incentives for hacking IoT devices. For one thing, many crimes are motivated not by traditional economic forces, but by rage, vengeance, aberrant sexual pleasure, desire for power, or even no cognizable motive at all.[167] These types of crimes have been reasonably well-regulated in their real-world applications,[168] which suggests that effective

---

164. *See supra* note 18.Bluetooth is basically a low-cost, short-range communication protocol most popularly used for cordless mobile phone accessories. GC, *Bluetooth Introduction*, TUTORIAL-REPORTS.COM (Feb. 18, 2013, 5:22), http://www.tutorial-reports.com/wireless/bluetooth/introduction.php.

165. Bluetooth transmissions for low-energy devices can have a working range up to about 300 feet. Jon Gunnar Sponas, *Things You Should Know About Bluetooth Range*, NORDIC SEMICONDUCTOR (June 2, 2016), http://blog.nordicsemi.com/getconnected/things-you-should-know-about-bluetooth-range. Thus, a criminal attempting to hack multiple Bluetooth devices at once must find a place where several of the same type of Bluetooth devices are within 600 feet of each other—the hacker being in the middle. Unless these devices have extreme importance, it is unlikely that any criminal would find it worth the time to find so many devices so close together. There is also an added risk of detection when hacking through short-range communications: if the hacker has to get close to pull off his exploit, an astute victim aware of the hack may be able to catch the criminal in the act.

166. The counter-argument to this is that the norm of using Bluetooth in low-value devices makes it unnecessary to enforce short-range communications in these devices. However, IoT security is notoriously under-appreciated by consumers. *See infra* note 179 and accompanying text. Thus, the most competitive product on the market will generally be the one that sacrifices security for profits. In some devices, those higher profits can be obtained by expanding the communication range of the IoT device, leaving the consumer to bear the hidden cost of lost security.

167. It should not be assumed that these types of noneconomic crimes and motives will be wholly absent from cyberspace. Murder and assault, crimes commonly motivated by rage and vengeance, are both achievable through an Internet-linked pacemaker or insulin pump. *See Hacker Dies Days Before He Was to Reveal How to Remotely Kill Pacemaker Patients*, *supra* note 3. Surreptitious recordings could be obtained through hacked cameras. *See* OccupytheWeb, *How to Secretly Hack Into, Switch On, & Watch Anyone's Webcam Remotely*, NULL-BYTE (June 15, 2016, 6:14PM), https://null-byte.wonderhowto.com/how-to/hack-like-pro-secretly-hack-into-switch-on-watch-anyones-webcam-remotely-0142514/. Ransomware, typically used for financial gain, could just as easily be turned to gain social or political control over someone. Hacking—even more often than traditional crimes—can also be carried out just for the fun of it or to gain notoriety in certain circles. *Why do People Hack Computers?*, COMPUTER HOPE (Apr. 26, 2017), http://www.computerhope.com/issues/ch001530.htm.

168. This phrase may have already raised some eyebrows, as the efficacy and equity of the American criminal justice system has come under fire from numerous sources in recent

enforcement and well-designed punitive statutes should be sufficient to keep their IoT counterparts in check.

This brings back the question of effective enforcement, though: how can law enforcement officers detect the existence, much less the perpetrator, of a crime if the victim's device contains no data to indicate that a breach has occurred? The simple answer is that these officers probably cannot. The more complex answer is to ensure that any device important enough to need this type of legal protection has the equivalent of a passenger jet's black box; a piece of code that latches onto any would-be user's IP address and stores basic information about when the user accessed the device and when the user stopped access.[169] From this information, even a moderately savvy user would be able to trace the rough location of the unauthorized user, and a trained law enforcement agent with a warrant could get a precise location.[170]

Finding this IP address does not end the inquiry, though, because there is no one-to-one relation between people and IP addresses.[171] IP addresses can be used by multiple people, and people can use multiple IP addresses.[172] The former occurs in everyday homes, where multiple roommates or family members might use the same router or even the same device to access the Internet. The latter can occur by many means. Two of the most common examples of how one person can use multiple IP addresses are dynamic IP addresses and multiple static IP addresses.[173] Sophisticated hackers can even take advantage of something called a proxy server to hide their activity among hundreds and even thousands of legal users all employing the same IP address.[174]

---

years. *See, e.g.*, Alex Kozinski, *Criminal Law 2.0*, 44 GEO. L.J. ANN. REV. CRIM. PROC. iii–xiv (2015). By *reasonably well-regulated*, all that is meant is that complete anarchy does not yet reign. Hopefully, that premise can still be sustained without citation.

169. The most basic version of this is called an event logger, which tracks things like when the device is connected to the Internet, when it is not, and what devices it is communicating with and when. Simple logging protocols can easily be applied to even low-power IoT devices. Jeffrey Bausch, *Why Log Management is a Key Underpinning of the Internet of Things*, LOGGLY (Jan. 13, 2015), https://www.loggly.com/blog/log-management-key-underpinning-internet-things/.

170. For a shortlist of software that can be used to trace IP addresses, see Philip Bates, *How to Trace an IP Address to a PC & How to Find Your Own*, MAKE USE OF (Feb. 8, 2017), http://www.makeuseof.com/tag/how-to-trace-an-ip-address-how-to-find-your-own-nb/.

171. An IP address is a unique series of digits separated by decimal points, identifying any given device accessing the Internet. *Id.*

172. *See id.*

173. *See id.* A person could have multiple static IP addresses by simply having multiple Internet-linked devices.

174. These powerful tools for hiding one's identity online are shockingly simple to find. A simple Google search for the words *proxy server* brings up as the second result a website called "Hide Me" which purports to allow users anonymous web surfing free of charge through a VPN. *Free Anonymous Proxy Browser*, HIDE ME, https://hide.me/en/proxy (last visited Apr. 30, 2017).

Thus, this approach of having dedicated storage for the information of all who access the device is far from a perfect solution. It merely means that law enforcement is not flying completely blind when attempting to catch a hacker who abuses an IoT device. Clever techniques and advanced technologies must be developed to reliably take IP information from this "black box" and use it to identify a criminal.[175]

The final method of prevention is both the most exciting and the most terrifying. If an IoT device can be completely immunized from access by any unauthorized device,[176] it can safely be used in even the most sensitive of circumstances. How this can be accomplished, however, is another matter. Some methods of encryption offer near-perfect results.[177] For any device to communicate with an encrypted IoT device, the user would probably have to know a passcode. That "probably" may be good enough to ensure that the total number of flops it takes to break an encryption algorithm by brute force is impractically excessive.[178] Where the stakes get higher, though, is precisely where very bad things can happen. If IoT devices are used in increasingly important applications—a trend that seems to be beginning even now[179]—then the techniques used to secure a user's control over IoT devices need to be flawless. For applications of this caliber, structural preventive methods are preferable. Some simple examples include ensuring that only one computing device can communicate with the IoT device, requiring an input on the IoT end of the communication simultaneous with the input from the interface device to verify identity, and the temporal but incredibly effective technique of disconnecting the device from the network while not in use.

All three of these methods for solving the security risks to IoT devices come at a cost. Encryption is fairly cheap,[180] but there is always an additional second or two required to put in a username and password when accessing the device lawfully, and some devices in IoT are actually too small to run more heavy-duty encryption protocols.[181] Installing a "black box" storage system for all of the information necessary to identify past hackers requires building in a separate storage

---

175. The intricacies of these technologies and techniques are, admittedly, beyond the expertise of this Author. It may well be that additional information beyond the mere IP and time of access is necessary to identify the offending device. If so, this additional data should be collected.

176. It is doubtful whether this exists at all. Encryption technologies have gotten very good, but hackers get more creative by the day.

177. Contel Bradford, *5 Common Encryption Algorithms and the Unbreakables of the Future*, STORAGECRAFT (July 31, 2017), http://www.storagecraft.com/blog/5-common-encryption-algorithms/.

178. Brute forcing is a term used to describe the most basic and obvious method of hacking into an encrypted device. The hacker simply tries all possible combinations of characters to eventually arrive at the password. *See id.* Because the amount of time required to guess a password increases exponentially with the number of characters in the password, brute forcing becomes impractical as the length of the password increases. *See id.*

179. Internet-linked medical devices are one example of this trend. *See supra* notes 1–7 and accompanying text.

180. *See* Bradford, *supra* note 177.

181. KATAGI & MORIAI, *supra* note 47.

unit—or, more likely, cloud storage space—that has nothing to do with the function of the device itself.[182] In an era when the trend is to minimize the size of everything but the battery and the screen, these "black boxes" will take up computing power and space that could otherwise be put to a more marketable purpose. Limiting the functionality of an IoT device by having it only link up to certain computers or requiring an input from the user on the IoT device end in order to access the device every time severely hinders the usefulness of having the device linked up to the Internet in the first place.

Because of these costs of security, and because the average consumer tends to undervalue the security of Internet-based products,[183] entrepreneurs and companies in IoT have little incentive to ensure that their products are up to snuff on best practices in security. This is where the elephant in the room rears its gray head: how can policymakers ensure that these types of security measures are implemented in the devices themselves to make sure that criminal law still functions as it applies to IoT? By using civil law and administrative regulations to make companies and consumers internalize the costs of the security risks their products pose. As addressed in Part I, regulatory bodies have been incredibly hesitant to push for binding regulations over IoT devices.[184] The argument against regulating IoT is that IoT is an industry that, despite its massive size, is still in the infancy of its potential.[185] The economic benefits to be gleaned from IoT products are endless.[186] Furthermore, this technology and its ramifications are still only fuzzily-understood by most policymakers, even those who make concerted efforts to understand the technology.[187] Thus, these regulatory bodies argue, IoT producers should be left to roam relatively unhindered by substantial regulatory burdens.[188]

These arguments would be more persuasive if they were less dangerous. As carried to the extreme, at least, the idea that IoT products should be left unhindered by regulation opens up a strong likelihood of security breaches and privacy problems. Economic forces acting on producers could lead inexperienced or unscrupulous sellers to put out products with little to no effective security. Even if there is a security system of some sort in each device, the likelihood of inconsistencies between different security measures could pose problems for

---

182. Bausch, *supra* note 169.

183. For a behavioral law and economics explanation of how consumers leave privacy—and similarly, security—out of their cost-benefit analysis when deciding to buy IoT products, see Melissa W. Bailey, Note, *Seduction by Technology: Why Consumers Opt Out of Privacy by Buying Into the Internet of Things*, 94 TEX. L. REV. 1023, 1034–41 (2016).

184. *See supra* Part I.

185. The FTC made a statement to this effect in its IoT security and privacy workshop four years ago. The "great potential for innovation in this area" led the agency to the conclusion that "IoT-specific legislation at this stage would be premature." FTC, *Internet of Things: Privacy and Security in a Connected World*, at vii–viii (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

186. *Id.* at 7–9.

187. *Id.* at 48–49.

188. *Id.*

whatever devices are seen by hackers as the stragglers in the pack in terms of security. Consumer demand is unlikely to see these security concerns as a major issue until it is too late.[189]

Thus, minimum standards of security are necessary to rebalance the market forces governing IoT to ensure that security and safety remain a priority. These standards should be kept loose to allow for the fullest growth of this emerging industry, but at the same time they must be severe enough to ensure that consumer faith in IoT is not destroyed by cataclysmic breaches of data or control. The point of control for these regulations must be the producers, as they are the ones best equipped and most easily incentivized to ensure that their products meet regulatory guidelines. If producers fail to meet these regulations, there must be civil punishments in place to deter future failures. Leaving this regulation up to common-law theories of product liability and breach of implied warranty would place the future of cybersecurity on shaky ground. Legislatively structured civil deterrence is necessary to keep the future of IoT secure.

CONCLUSION

The Internet of Things is an exciting new field of technology. Its acceleration from humble beginnings as microchips installed on lipstick bottles[190] to a multi-billion dollar industry[191] has been exponential, to put it mildly. With that rapid a change, however, comes inherent danger. Laws and law enforcement must be ahead of the curve on adapting to the changes that this new technology will bring to everyday life. Otherwise, criminals will find ways to abuse this technology to harm its users. With the implementation of structural changes to the major cybercrime statutes, the addition of dedicated cybercrimes divisions in both prosecutors' offices and police departments, and the insistence on market standards for the security of any device that will ultimately be linked up to the Internet, a substantial amount of crime can be prevented before it even happens. As cyberspace becomes a larger part of the average American's everyday life, cyberspace must be kept safe from the real world, and the real world must be kept safe from cyberspace.

189. Bailey, *supra* note 183.
190. Maney, *supra* note 12.
191. *See supra* notes 15–17, 23–27 and accompanying text.