Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*

Sara Sun Beale# *and Peter Berris*+

Introduction

This is the age of the "Internet of Things," (IoT) where "everyday objects... connect to the Internet and... send and receive data."[1] The lines between computers and humans have blurred as "[t]he Internet now affects the world in a direct physical manner."[2] The Federal Trade Commission predicts that more than fifty billion devices will be part of the IoT by 2020,[3] including items ranging from kitchen appliances to Fitbits and heart monitors.[4] As Bruce Schneier explained to Congress, "everything is

---

* For a revised and extended version of this project, see Sara Sun Beale & Peter Berris, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, 16 Duke L. & Tech. Rev. 161 (2018) (examining reasons for vulnerability of IoT and how current legal system responds, discussing practical and legal barriers to investigation and prosecution of hacking, and evaluating the merits and pitfalls of hacking back against botnets from legal, practical, and ethical standpoints).

Charles L.B. Lowndes Professor, Duke Law School.

+ J.D., Duke Law School, 2017.

1 Federal Trade Commission, internet of things: Privacy & Security in a Connected World i (2015), available at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127IOTrpt.pdf.

2 *Understanding the Role of Connected Devices in Recent Cyber Attacks: Hearing Before H. Comm. on Energy and Commerce*, 114th Cong. 3 (2016) (statement of Bruce Schneier), [hereinafter "Schneier"].

3 Christina Scelsi, *Care and Feeding of Privacy Policies and Keeping the Big Data Monster at Bay: Legal Concerns in Healthcare in the Age of the Internet of Things*, 39 Nova L. Rev. 391, 396 (2015).

4 Andrew Meola, *What is the Internet of Things (IoT)?*, Business Insider, (Dec. 19, 2016), http://www.businessinsider.com/what-is-the-internet-of-things-definition-2016-8.

now a computer."[5] The reach of the IoT extends beyond consumer goods to major items and infrastructure components including cars, airplanes,[6] hospitals, telecommunications networks, and power grids.[7] As a result, "insecurity" in the IoT "puts human safety at risk."[8] Moreover, in the age of the IoT, the actions of "hackers" may carry physical consequences.[9]

This paper proceeds as follows. Section I describes episodes in which the IoT has already been hacked as well as the potential for other attacks, and Section II examines the reasons for the vulnerabilities that facilitate hacking. Section III explores how criminal law now responds to attacks on the IoT, and Section IV concludes with a discussion of legal reforms that might reduce the current vulnerabilities and prevent future attacks.

I. Threats and Vulnerabilities

A. How the IoT has been hacked

On October 21, 2016, major websites, including Netflix, Twitter, Reddit and the New York Times, were inaccessible for up to several hours.[10] The interruption was the result of a Distributed Denial of Service attack ("DDoS")[11] against the company Dyn, which "is one of many outfits that

---

5 *Understanding the Role of Connected Devices in Recent Cyber Attacks* (preliminary transcript): *Hearing Before H. Comm. on Energy and Commerce*, 114th Cong. 27 (2016) (testimony of Bruce Schneier), http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Transcript-20161116.pdf [hereinafter "Schneier Testimony"].

6 *Id.* at 29.

7 *Id.* at 57.

8 *Understanding the Role of Connected Devices in Recent Cyber Attacks: Hearing Before H. Comm. on Energy and Commerce*, 114th Cong. 3 (2016) (statement of Kevin Fu), http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Wstate-FuK-20161116.pdf [hereinafter "Fu"] (warning the HECC that "the Dyn attack is a sign of worse pains to come").

9 *See* section I, *infra*.

10 Nicole Perlroth, *Hackers Used New Weapons to Disrupt Major Websites Across U.S.*, N.Y. Times, Oct. 21, 2016, at https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?_r=0 [hereinafter "Perlroth"].

11 A DDoS is when "an attacker attempts to prevent legitimate users from accessing information or services. . . . [such as] when an attacker 'floods' a network with information. . . . The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process [legitimate re-

host the Domain Name System, or DNS, which functions as a switchboard for the internet."[12] The perpetrators of the Dyn attack exploited "a vulnerability in large numbers—possibly millions—of... devices like webcams and digital video recorders" and used them as a botnet[13] to flood Dyn with traffic.[14] This "attack traffic" combined with "legitimate traffic" to overwhelm Dyn,[15] taking down "dozens of websites" with it.[16]

Despite the large scale of the interruption, the Dyn attack has been characterized as "benign" since it did not result in physical injury or property damage.[17] Nevertheless, it underscored the risk that the next attack may be devastating.[18]

In response to the Dyn attack, the House Energy and Commerce Committee (HECC) held a hearing to address the threats posed by hacking in the IoT.[19] Expert testimony was grave. Bruce Schneier warned that "the internet is now dangerous...."[20] Dr. Kevin Fu told the HECC that he "fear[s] for the day where every hospital system is down, for instance, be-

---

quests]. This is a 'denial of service' because you can't access that site." Mindi McDowell, *Security Tip (ST04-015) Understanding Denial-of Service Attacks*, US-CERT, Feb. 6, 2013, https://www.us-cert.gov/ncas/tips/ST04-015.

12 Perlroth, *supra* note 100.

13 A botnet is a "collection of computers compromised by malicious code and controlled across a network." *Glossary*, US-CERT, Jan. 11, 2017, https://niccs.us-cert.gov/glossary#B. Although they can be used for collaboration, "botnet" is a pejorative term. Zach Lerner, *Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets*, 28 Harv. J.L. & Tech. 237, 237–38. (2014) [hereinafter "Lerner"].

14 Schneier, *supra* note 2, at 2.

15 Scott Hilton, *Dyn Analysis Summary of Friday October 21 Attack*, Dyn: Vantage Point, Oct 26, 2016, http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.

16 Schneier, *supra* note 14.

17 *Id.* at 3.

18 *See* Fu, *supra* note 8, at 2.

19 *Understanding the Role of Connected Devices in Recent Cyber Attacks* (preliminary transcript): *Hearing Before the H. Comm. on Energy and Commerce*, 114th Cong. 4–5 (2016) (statements of Greg P. Walden, Chairman, Subcomm. on Commc'n & Tech.), http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Transcript-20161116.pdf.

20 Schneier Testimony, *supra* note 5, at 59.

cause an [IoT] attack brings down the entire healthcare system."[21] Dale Drew cautioned that the culprits of the Dyn attack relied on "just a fraction of the total available compromised [IoT devices]... demonstrating the potential for significantly greater havoc...."[22]

Illustrations of the dangers abound. Many prominent examples of hacking in the IoT pertain to automobiles.[23] In 2015, Fiat Chrysler recalled 1.4 million cars in response to a widely publicized demonstration where hackers took control of a Jeep Cherokee through its infotainment system.[24] They were able to "turn the steering wheel, briefly disable the brakes and shut down the engine."[25] In 2010, the disgruntled former employee of a

---

21 *Understanding the Role of Connected Devices in Recent Cyber Attacks* (preliminary transcript): *Hearing Before the H. Comm. on Energy and Commerce*, 114th Cong. 43. (2016) (testimony of Kevin Fu), http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Transcript-20161116.pdf [hereinafter "Fu Testimony"].

22 *Understanding the Role of Connected Devices in Recent Cyber Attacks: Hearing Before the H. Comm. on Energy and Commerce*, 114th Cong. 3 (2016) (statements of Dale Drew), http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Wstate-DrewD-20161116.pdf [hereinafter "Drew"].

23 Automobiles are an obvious target for hackers because they can cause physical damage, *and* because they are vulnerable. *See* Cheryl Dancey Balough, Richard C. Balough, *Cyberterrorism on Wheels: Are Today's Cars Vulnerable to Attack?*, Bus. L. Today, November 2013, at 1 [hereinafter "Balough"] ("The potential exists that a car's computers, like any computer system, can be hacked, leaving the car vulnerable to infection by malware. These vulnerabilities pose serious safety hazards should they be exploited nefariously. Legal implications of this technological vulnerability have yet to be adequately addressed."). Cars contain dozens of Electronic Control Units (ECUs) "embedded in the body, doors, dash, roof, trunk, seats, wheels, navigation equipment, and entertainment systems," many of which connect to the internet and provide access points for hackers. *Id.* Disturbingly, "[t]he potential vulnerability of cars to hacking will increase as vehicle-to-vehicle (V2V) and self-driving cars become available" and "the average auto maker is about 20 years behind software companies in understanding how to prevent cyber attacks." *Id.* at 3.

24 Kelly Pleskot, *FCA Recalls 1.4 Million Vehicles Over Hacking Concern*, MotorTrend, Jul. 24, 2015, http://www.motortrend.com/news/fca-recalls-1-4-million-vehicles-over-hacking-concern/.

25 Craig Timberg, *Hacks on the Highway*, Washington Post, Jul. 22, 2015, at 3, http://www.washingtonpost.com/sf/business/2015/07/22/hacks-on-the-highway/ [hereinafter "Timberg"].

used-car dealership remotely accessed the company's computers and caused havoc by setting off car alarms and shutting down engines.[26]

The danger is not limited to cars. For example, in 2008, a fourteen-year-old boy hacked into the system controlling the trains of Lodz, Poland as a prank.[27] He made several trains change tracks, causing multiple derailments and injuries.[28] In 2013, the Federal Bureau of Investigation and the Department of Homeland Security "issued a warning" about "several... attacks against the 911 system."[29] The attacks were an attempt to extort money, and when the perpetrators received nothing they "launched [a] high volume of calls against the target network, tying up the system from receiving legitimate calls."[30] In 2016, Iranian hackers breached "the computer-guided controls" of the small Bowman Dam in suburban Rye Brook, New York.[31] The dam was offline for repair and immune to remote access, but the implications are disturbing because the hackers may have been trying to access an identically named dam in Oregon that is a formidable "245 feet tall and 800 feet long...."[32]

B. Other ways the IoT could be hacked

Security researchers have identified a range of other frightening vulnerabilities. Researchers have "demonstrated ransomware against home thermostats and exposed vulnerabilities in implanted medical devices.

---

26 *Id.* at 7; Matthew Shaer, *Disgruntled Hacker Remotely Disables 100 Cars*, Christian Science Monitor, Mar. 18, 2010, at 1, http://www.csmonitor.com/Technology/Horizons/2010/0318/Disgruntled-hacker-remotely-disables-100-cars.

27 Graeme Baker, *Schoolboy Hacks Into City's Tram System*, the Telegraph, Jan. 11, 2008 at http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html.

28 *Id.*

29 Kim Zetter, *How America's 911 Emergency Response System Can Be Hacked*, Washington Post: The Switch, Sep. 9, 2016 at 1, https://www.washingtonpost.com/news/the-switch/wp/2016/09/09/how-americas-911-emergency-response-system-can-be-hacked/?utm_term=.64b3faef0108.

30 *Id.* (internal citation omitted).

31 Joseph Berger, *A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case*, N.Y. Times, Mar. 25, 2016, https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html?_r=0.

32 *Id.*

They've hacked voting machines and power plants."[33] Indeed, many computer security experts fear that the USB port on an airline seat could potentially control the airplane's avionics.[34]

Clearly, the IoT offers a broad array of dangerous tools for hackers can exploit for a range of motives, including: terrorism,[35] "national aggression,"[36] pranking,[37] election tampering,[38] and monetary extortion.[39] Whatever the impetus for hacking in the IoT, the threats moving forward are considerable.

II. Why is the IoT so insecure and vulnerable to hacking?

Security researches have attributed the scale and ease of attack to "the quantity of insecure IoT devices operated by a highly distributed set of unwitting consumers,[40] and to a "fundamental market failure."[41] Because electronics consumers care most about affordability, "the market has prior-

---

33 Schneier, *supra* note 2, at 5. at 5. Although there is evidence of Russian hacking intended to affect the U.S. presidential election in 2016, these efforts seem to have been focused on the computers themselves and information contained on them (e.g., emails and donor databases), rather than on things connected to the computers, such as voting machines. *But see* David Smith & John Swain, *Russian Agents Hacked US Voting System Manufacturer Before U.S. Election*, The Guardian, June 5, 2017, at 1 (noting that although hacking and release of Democratic emails had been traced to Russia vote counting "was thought to be unaffected" before leaked report that Russian intelligence hacked into U.S. manufacturer of voting systems weeks before election).

34 Schneier Testimony, *supra* note 5, at 102.

35 *See generally* Balough *supra* note 23, at 1 (theorizing about the possibility that cars might be exploited for terrorism through the internet).

36 Schneier Testimony, *supra* note 5, at 57.

37 *See* Baker, *supra* notes 27 & 28, and accompanying text (chronicling a hacking attack executed as a prank).

38 *See generally* Bruce Schneier, *American Elections Will Be Hacked*, N.Y. Times, Nov. 9, 2016, at https://www.nytimes.com/2016/11/09/opinion/american-elections-will-be-hacked.html (summarizing the vulnerabilities of voting machines and infrastructure and the danger of election fraud).

39 *See* Drew, *supra* note 22, at 3 ("The primary motivation for [DDoS] attacks appears to be financial.").

40 *See* Fu, *supra* note 8, at 4 ("What's new is the scale and ease of attack because of the quantity of insecure [IoT] devices operated by a highly distributed set of unwitting consumers.").

41 Schneier, *supra* note 2, at 3.

itized features and cost over security."[42] Thus, the teams that make many IoT devices have less "security expertise" than major companies like Apple, because "the market won't stand for the additional costs that [similar training] would require."[43] Further complicating matters, many IoT devices are part of a complex global supply chain where they are "designed and built offshore, then rebranded and resold."[44] The resulting devices are the product of differing international standards of security.[45]

As a result, IoT devices in the U.S. exhibit a wide range of serious vulnerabilities. Many come with "default and easily-identifiable passwords that hackers can exploit."[46] Some of these passwords cannot be changed.[47] Similarly, many "devices also lack the capability of updating their firmware, forcing consumers to monitor for and install updates themselves."[48] Additionally, consumers "often have little way to know when [IoT] devices have been compromised."[49] The relationship between hardware and software further exacerbates the problem. When the underlying software has been corrupted, the object it is connected to often continues to function as intended, leaving little reason to replace it.[50] Even devices used as part of a botnet in an attack will "still work fine."[51] Additionally, the hardware of an object may last far longer than the software that powers it remains secure.[52]

---

42 *Id.*
43 *Id.*
44 *Id.*
45 Dale Drew Committee on Energy and Commerce, *Understanding the Role of Connected Devices in Recent Cyber Attacks* (preliminary transcript), Hearing, pp 37–38 Nov 16, 2016. Available at: http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Transcript-20161116.pdf; Accessed: 2/26/17 [hereinafter "Drew Testimony"] (explaining the need for international standards).
46 Drew, *supra* note 22, at 2.
47 *Id.*
48 *Id.*
49 *Id.*
50 See Fu Testimony, supra note 21, at 88 (using the example of an MRI machine to explain that consumers do not want to replace functioning hardware to fix a problem with vulnerable software, especially where the machine is expensive).
51 Schneier, *supra* note 2, at 4.
52 *Id.* at 3–4 (identifying the problem of longevity in internet enabled devices including cars, refrigerators, and thermostats).

III. The Internet of Things and the Current Legal Regime

This section explores the interaction between the IoT and the current legal regime. Subsection A discusses whether current laws prohibit hacking with an intent to control an object. Subsection B explores the problem of botnets. This section concludes that hacking in the IoT will often be illegal, though these laws punish conduct after the fact, but do not prevent it.

A. Scenario one: hacking with the intention of controlling an object

Consider the following hypothetical. Bill has a grudge against his neighbor Jeremy. He discovers that there is a security vulnerability in one of the many electronic control units (ECUs) of Jeremy's late model sedan,[53] and he hacks in through the internet and enters commands that take control of Jeremy's car.[54]

Bill's actions are increasingly plausible as cars become ever more connected and automakers struggle to update outmoded software.[55] The hypothetical identifies an intriguing problem in the IoT: the hackers' target is not the computer but rather the object it is connected to. This is true of many of the examples outlined above, although the motives varied: the fourteen-year-old hacked a train system for a prank; the Iranians hacked a dam possibly for terrorism; the extortionists attacked the 911 system for money; and the disgruntled employee hacked into cars sold by his former employer for revenge. All wanted to control an object, and the internet was just a means to that end.[56] In the IoT a key objective of remote access will be to control the "Things." Thus, a key question is whether the current

---

53 Such vulnerabilities are apparently not hard to track down. *See* Timberg, *supra* note 25.
("[S]ecurity researches" discovered "readily accessible Internet links to thousands of other privately owned Jeeps, Dodges and Chryslers....").

54 The exact form of hacking varies based on the specific ECU: "[s]ome entry points to a car's ECUs require a direct hard-wired connection, while others can be accessed wirelessly, including Wi-Fi or [Radio-frequency identification]." Balough *supra* note 23, at 1. Researchers demonstrated that once a vehicle has been started normally, key functions including the engine, brakes, and transmission can be controlled remotely by "typing on a MacBook Pro." Timberg, *supra* note 25.

55 Timberg, *supra* note 25.

56 *See supra* text accompanying notes 26–32.

legal regime covers this relatively new threat, and governs scenarios like the one with Bill and Jeremy. It does.

1. The Computer Fraud and Abuse Act

The most obvious law that could be employed to combat hacking with the intent to control is the Computer Fraud and Abuse Act ("CFAA"). The CFAA was "[o]riginally designed as a criminal statute aimed at deterring and punishing hackers, particularly those who attack computers used for compelling federal interests,"[57] but also includes "a trespass-like civil remedy under federal law" for various forms of hacking.[58] It is logical that the law would cover hacking with an intent to control an object, as it is believed that Congress passed the CFAA in response to the movie WarGames,[59] where the protagonist accidentally hacks into the computer controlling America's nuclear weaponry and nearly starts a third world war.[60]

Indeed, the provisions of the CFAA cover a range of conduct. The act prohibits:

> (1) unauthorized obtaining of national security information; (2) unauthorized obtaining of information from a financial institution, United States department or agency, or from any protected computer; (3) unauthorized access to government computers; (4) computer fraud; (5) computer damage; (6) passwords trafficking; and (7) computer extortion.[61]

---

57 COMPUTER FRAUD AND ABUSE ACT, SS032 ALI-ABA 993, 995.

58 5.06. Computer Fraud and Abuse Act, 1 E-Commerce and Internet Law 5.06 (2016 update).

59 *See* Fred Kaplan, *'War Games' and Cybersecurity's Debt to a Hollywood Hack*, N.Y. Times, Mar. 25, 2016, at https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html?_r=0 (chronicling the emergence of early federal cybersecurity laws in response to President Ronald Reagan's concern over the movie "WarGames"); Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 Harv. J.L. & Tech. 429, 492 (2012) [hereinafter "Kesan"].

60 For a synopsis of the movie Warm Games, see http://www.imdb.com/title/tt0086567/synopsis?ref_=tt_stry_pl (last visited August 31, 2017).

61 Ioana Vasiu & Lucian Vasiu, *Break on Through: An Analysis of Computer Damage Cases*, 14 U. Pitt. J. Tech. L. Pol'y 158, 163 (2014) [hereinafter "Vasiu"].

Section 1030(a)(5) is the subsection most likely to cover hacking with an intent to control an object. It criminalizes:

> knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer; intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage; or intentionally access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss.[62]

Whether § 1030(a)(5) prohibits hacking with an intent to control hinges on four key definitions: (1) "transmission," (2) "computer," (3) "protected computer," and (4) "damage."

"Transmission" encompasses a range of hacking activities, such as "[t]he transfer of operation or confidential information," "malicious software updates," "code injection attacks," DDoS, and the "embedding of malicious code" or malware.[63] Under the CFAA, transmission "can be accomplished either over the Internet or through a physical medium such as a compact disc."[64] This would cover many forms of hacking aimed at controlling an object. To return to the example of Bill and Jeremy, Bill's conduct qualifies, as he transmitted commands via the internet to take control of Jeremy's car.

Within the CFAA, "computer" is an expansive term. It defines a computer as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device...."[65] As Judge Easterbrook explained, the definition of "computer" in the CFAA is an example where the exclusions from the definition "show just *how* general" it is."[66] Indeed, CFAA subsection (e)(1) "carves out automatic typewriters, typesetters, and handheld calculators; this shows that other devices with embedded processors and software are covered."[67] Thus, most IoT devices are computers. The ECUs that Bill hacked in Jeremy's car cer-

62 18 U.S.C. § 1030(a)(5) (2012).
63 Vasiu, *supra* note 61, at 167–169.
64 174 A.L.R. Fed. 101 (Originally published in 2001).
65 18 U.S.C. § 1030 (e)(1) (2012).
66 *United States v. Mitra*, 405 F.3 d 492, 495 (7th Cir. 2005).
67 *Id.*

tainly would qualify, as they "are high speed data processing devices performing logical, arithmetic, or storage functions."[68]

Many IoT devices will also be *protected* computers. The CFAA defines protected computers to include not only those "exclusively for the use of a financial institution or the United States Government" but also computers "used in or affecting interstate or foreign commerce or communication...."[69] Courts have interpreted this definition broadly. Indeed, in *U.S. v. Mitra*, Judge Easterbrook explained that "the statute... protects computers (and computerized communication systems) used in such commerce, no matter how the harm is inflicted. Once the *computer* is used in interstate commerce, Congress has the power to protect it from a local hammer blow, or from a local data packet that sends it haywire."[70] This standard included the afflicted computer in *Mitra*—Madison, Wisconsin's "computer-based radio system for police, fire, ambulance, and other emergency communications"[71]—even though the hacker's "interference did not affect any radio system on the other side of a state line."[72] What mattered was that Madison's computerized radio system "operated on spectrum licensed by the FCC" and therefore implicated interstate commerce.[73]

Mitra is not an exception. Particularly relevant for devices that are part of the *IoT*, "[c]ourts generally hold that because the Internet and interstate commerce are inexorably intertwined, any computer connected to the Internet should be considered a computer affecting interstate commerce and therefore protected."[74] Thus, if Jeremy's ECU is internet-enabled, it is a protected computer under the CFAA. This seems a safe bet in an era where cars are increasingly connected and can "talk to the outside world through remote key systems, satellite radios, telematic control units, Bluetooth connections, dashboard Internet links and even wireless tire-pressure monitors."[75]

---

68 Balough *supra* note 23, at 3.
69 18 U.S.C. § 1030 (e)(2)(b)(2012).
70 *Mitra*, 405 F.3 d at 496.
71 *Id.* at 493.
72 *Id.* at 496.
73 *Id.*
74 Vasiu, *supra* note 61, at 164.
75 Timberg, *supra* note 25.

"Damage" is "defined as 'any impairment to the integrity or availability of data, a program, a system, or information,'"[76] and almost certainly encompasses hacking with the intent of controlling an object.[77] To begin with, a hacker damages a computer under the statute by forcing it to behave in a manner unintended by its owner.[78] Additionally, "[a]dverse actions.... that alter, encrypt, encipher, encode, transmit or delete data or exhaust system resources" all are damage under the CFAA because they impair the availability of the computer by making it unusable and inaccessible.[79] Transmission is damage under the CFAA because it "involves the deletion of computer data or files."[80] Clearly, Bill damaged Jeremy's car under the CFAA, since he caused it to behave contrary to the wishes of its owner.

Finally, CFAA penalties are structured in a manner that enhances punishment depending on the outcome of the hacking. The Act provides harsher penalties for those whose hacking causes "physical injury," "a threat to public health or safety," "damage affecting a computer used by or for an entity of the United States government in furtherance of justice, national defense, or national security," damage to at least ten computers within a year, or "modification or impairment... of the medical examination, diagnosis, treatment, or care of 1 or more individuals...."[81] Unsurprisingly, the stiffest retribution is reserved for those who "knowingly or recklessly caus[e] death from conduct in violation of" subsection (a)(5)(a).[82] Depending on the nature and results of Bill's hacking, he may be subject to some of these increased CFAA penalties. For example, if he took control of Jeremy's car while it was hurtling down a busy highway, it is easy

---

76 Jeffrey K. Gurney, *Driving into the Unknown: Examining the Crossroads of Criminal Law and Autonomous Vehicles*, 5 Wake Forest J.L. & Pol'y 393, 439 (2015) quoting 18 U.S.C. § 1030(e)(8) (2012)) [hereinafter "Gurney"].

77 As one commentator has summarized it, "nearly any instance of unauthorized hacking could be said to impair the integrity of a computer system." Ric Simmons, *The Failure of the Computer Fraud and Abuse Act: Time to Take an Administrative Approach to Regulating Computer Crime*, 84 Geo. Wash. L. Rev. 1703, 1712 (2016).

78 *See* Vasiu, *supra* note 61, at 160 ("Integrity generally refers to maintaining computer data in a protected state, unaltered by improper, unauthorized or subversive conduct or acts contrary to what the system owner or privilege grantor intended.").

79 *Id.*

80 *Id*. at 192.

81 18 U.S.C. § 1030(c)(4) (2012).

82 18 U.S.C. § 1030(c)(4)(F) (2012).

to imagine how Bill might have threatened public safety. If Jeremy's car crashed as a result of the hacking, Bill would face steeper sentencing under the CFAA if Jeremy was injured or killed.

2. Other laws

There are many other laws that could govern hacking with an intent to control an object. Although a full review is beyond the scope of this paper, this subsection summarizes a few obvious candidates.

One way to punish hacking with an intent to control an object is to look to state versions of the CFAA. All "fifty states... enact[ed] statutes specifically prohibiting computer misuse."[83] Like the CFAA, all of these laws employ the "common building block of unauthorized access to a computer," which is "usually supplemented by other elements to create additional criminal prohibitions, such as statutes preventing... computer damage."[84] Many of these laws could be construed as anti-hacking statutes.[85] Such laws could provide a useful tool in combatting hacking in the IoT. For example, Connecticut General Statute § 53-451(b) makes it "unlawful for any person to use a computer or computer network without authority and with the intent to... (2) Cause a computer to malfunction, regardless of how long the malfunction persists." Given the statute's broad definition of computer,[86] it would almost certainly govern hacking in an attempt to control an object. Other states have similar laws.[87] If the hypothetical involv-

---

83 Computer Crime Law, 29.

84 *Id*. at 29–30.

85 Gurney, *supra* note 76, at 434.

86 *See* Conn. Gen. Stat. § Sec. 53-451(a)(1) (2015) ("'Computer' means an electronic, magnetic or optical device or group of devices that, pursuant to a computer program, human instruction or permanent instructions contained in the device or group of devices, can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person. 'Computer' includes any connected or directly related device, equipment or facility that enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device.").

87 *See* Gurney, *supra* note 76, at 436 ("States also have vandalism hacking statutes. Unlike the trespassing statutes, the vandalism statutes "typically make it a more serious crime to purposely access a computer without authorization and alter, damage or disrupt the operation of the computer and/or the data it contains.").

ing Bill and Jeremy occurred in a state like Connecticut, than Bill would have violated state law by causing the ECU in Jeremy's car to behave in a manner other than its intended use.

Additionally, other state computer crime provisions may cover hacking in the IoT, depending on the outcome of the conduct. Indeed, several states "make it an offense to break into or tamper with a computer system and thereby cause the death of one or more persons or create a strong probability of causing death to one or more persons."[88] Relatedly, some state computer crime laws prohibit damaging the object for which control is sought, or other property.[89] Thus, if Bill damaged Jeremy's car, or Jeremy himself, he is likely culpable under additional state computer crime laws.

Of course, depending on the results of, and motivations behind, hacking, other non-computer crime laws might apply as well. For example, Bill might be culpable for kidnapping, joyriding, grand larceny, or even "[d]estruction of motor vehicles or motor vehicle facilities" under 18 U.S.C. § 33(a) (2012).[90] If Bill intends to kill Jeremy, and succeeds, he might be liable for murder.[91] In the IoT, hacking will often be a method for perpetrating another crime: as a result, other statutes will likely apply.

B. Scenario two: botnets

As discussed in Section I, botnets are a network of compromised computers, "often programmed to complete a set of repetitive tasks" without "the owner's knowledge or permission."[92] Botnets "are the instrumentality through which substantial amounts of cybercrime takes place."[93] Botnet based cybercrime includes spam, fraud, and—of particular relevance for the IoT—DDoS and the installation of malware.[94] Hackers used a botnet

88 Susan W. Brenner, *State Cybercrime Legislation in the United States of America: A Survey*, 7 Rich. J.L. & Tech. 28, 10 (2001).

89 See, e.g., Conn. Gen. Stat. § 53-451 (b)(5) (criminalizing "use [of] a computer or computer network without authority... with the intent to: Cause physical injury to the property of another....").

90 Gurney, supra note 76, at 433–442.

91 *Id*. at 438.

92 Lerner, *supra* note 13, at 237–38 (2014).

93 Zachary K. Goldman & Damon McCoy, *Deterring Financially Motivated Cybercrime*, 8 J. Nat'l Security L. & Pol'y 595, 608 (2016) [hereinafter "Goldman"].

94 Lerner, *supra* note 13, at 237–38.

in the Dyn attack, which prompted the HECC hearing discussed in Section I, about the dangers of hacking in the IoT.[95]

Unsurprisingly given the nature of their use, botnets are illegal under the CFAA.[96] For example, CFAA section 1030(a)(5) criminalizes "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer...."[97] Botnets are often created through malicious software that behaves in this manner.[98] Although there are practical problems to combating Botnets with laws like the CFAA,[99] there have been successful prosecutions.[100]

IV. Improving the Security of the IoT

Although the CFAA provides a tool to prosecute hacking in the IoT, the dangers in this new era are numerous and grave. As a result, better security in the IoT also requires a reduction of vulnerabilities and a mechanism for prevention.

As section II illustrates, the IoT is currently the victim of a market failure.[101] Consumers want IoT devices to be as cheap as possible.[102] Manufacturers and retailers oblige, prioritizing cost over security because they

---

95 *See* text accompanying notes 10–22 *supra*; Bruce Schneier, *Lessons From the Dyn DDoS Attack*, Schneier on Security (November 8, 2016, 6:25 AM), https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html.

96 *See* Kesan *supra* note 59 at 493 ("The CFAA's language is very broad and can be read to prohibit the creation of botnets.").

97 18 U.S.C. § 1030(a)(5) (2012).

98 *See* Kesan *supra* note 59 at 442–444 (explaining how botnets are created).

99 *See* Lerner, *supra* note 13, at 244 ("CFAA enforcement requires precise knowledge of the defendant's identity, which is often impossible to obtain in DDoS attacks... [In addition] CFAA prosecution of DDoS masters in foreign countries is impeded by a number of jurisdictional obstacles.").

100 *See*, e.g. Department of Justice Office of Public Affairs, *Arizona Man Sentenced to 30 Months in Prison for Selling Access to Botnets*, Justice News (September 15, 2014), https://www.justice.gov/opa/pr/arizona-man-sentenced-30-months-prison-selling-access-botnets (describing successful prosecution of a man who had sold "access to and use of thousands of malware-infected computers").

101 *See* text accompanying note 41, *supra*.

102 *See* text accompanying note 43, *supra*.

have no incentive not to.[103] International supply chains and the limited security expertise of many IoT design teams further complicate matters.[104] The widespread weaknesses in IoT devices offer an enticing tool and opportunity for nefarious activity. As a result, the IoT of today is a veritable wild west of the digital era, where a new frontier invites violence, theft, and mischief. To continue the metaphor, if existing laws are insufficient to remedy the dangers of the IoT, what *will* tame the west?

There are many possibilities,[105] and this section explores two options: a standards based approach, and a new or expanded regulatory agency. A third intriguing approach, sketched briefly below, is counter hacking.

A. The Standards Approach

Vulnerabilities like default passwords and static firmware threaten IoT security. Although devices with these vulnerabilities are suboptimal, they are not technically substandard. There is no uniform set of standards that IoT manufacturers or retailers must meet.[106] The standards approach would attempt to remedy this by imposing such a system on key players.

A standards system would combat the market failure by incentivizing better security practices in the proliferation of IoT devices.[107] According to one expert, adopting "defined standards" will "change buying and investment patterns" that are responsible for the current state of vulnerability in the IoT.[108] Imposing stronger security measures through standards for IoT developers is important because "[s]ecurity needs to be built into IoT devices, not bolted on. If cybersecurity is not part of the early design of an

---

103 *Id.*

104 *See* text accompanying note 44–45, *supra*.

105 *See, e.g.,* IoT Security Foundation, *IoT is Vast and Has Many Security Related Issues – how do we go about addressing them?*, IoT Security Foundation, https://iotsecurityfoundation.org/working-groups/(last visited Nov. 14, 2017) (listing and summarizing different practice groups, each focused on a different aspect of IoT security).

106 *See* Drew, *supra* note 22, at 4 ("The current lack of any security standards for [IoT] devices is certainly part of the problem that ought to be addressed.").

107 *See Id.* ("IoT manufacturers and vendors should embrace and abide by additional security practices to prevent harm to users and the internet.").

108 *See* Drew Testimony, *supra* note 45, at 97.

IoT device, it's too late for effective risk control."[109] Establishing standards that require better security measures from the start implicates "domestic and international" standards setting entities like the International Standards Organization or the National Institute of Standards and Technology (NIST),[110] and may require government intervention.[111]

Generally, organizations advocating for the use of a standards-based approach emphasize the importance of a consistent and uniform standard,[112] but the priorities of an IoT security standard might vary. For example, Dale Drew—a proponent of a standards approach—is preoccupied with remedying vulnerabilities like default passwords, "hard-coded credentials," and the "lack of capability of updating [IoT device] firmware."[113]

Assuming arguendo that agreement could be reached on the correct standards, this approach would still have a serious limitation: it would not affect the millions of existing devices.

B. Agency Regulation

Some experts have concluded that the pervasive threats to the IoT, and the related market failure, require increased government involvement.[114] They argue that "[c]ybersecurity ought to be a public good much like automo-

---

109 Fu, *supra* note 8, at 3.

110 *See* Drew Testimony, *supra* note 45, at 97–8. Indeed, the Institute of Electrical and Electronics Engineers is currently working on "P2413," a "standard for an architectural framework for the [IoT]" which will address security among other considerations. IEEE Standards Association, *Standard for an Architectural Framework for the Internet of Things (IoT)* IEEE (2017), http://grouper.ieee.org/groups/2413/.

111 *See* Drew, *supra* note 22, at 4 (Noting that in the context of standards setting, "there may be a role for the government to provide appropriate guidance").

112 *See Standard for an Architectural Framework for the Internet of Things*, IEEE Standards Association (2017), https://standards.ieee.org/develop/project/2413.html ("The adoption of a unified approach to the development of IoT systems will reduce industry fragmentation and create a critical mass of multi-stakeholder activities around the world.").

113 Drew, *supra* note 22, at 2.

114 *See* Schneier Testimony, *supra* note 5, at 43 ("The choice is not between government involvement and no government involvement, but between smart government involvement and stupid government involvement.").

bile safety."[115] One possible option to achieve that goal is to expand the capabilities of existing government agencies to test IoT security. To promote automobile safety, there are federally funded research and development centers, testing facilities run by the National Transportation Safety Board (post market), automotive crash safety testing (premarket), and the Nevada National Security Site (destruction and survivability testing). [116] But no analogous regulatory or research entities exist to provide a proving ground for the types of embedded cybersecurity defenses needed to guard the IoT.[117] Such a facility would remedy the government's lack of a means to "conduct thorough security testing and assessment on IoT devices" and would reduce the inefficiencies of having diffuse entities conducting independent research.[118] This expansion could potentially fall under the control of the National Science Foundation or the NIST.[119]

Another possibility is the creation of a new regulatory agency. Schneier advocates for this position and analogizes the IoT to the technologies of the past that gave rise to new agencies: "trains, cars, airplanes, radio, and nuclear power."[120] He argues that "[i]n the world of dangerous things, we constrain innovation,"[121] and that the IoT presents new dangers just as those technologies did during their development. As a result, even if regulation would stifle some creativity, Schneier suggests that this is a necessary sacrifice for security.[122] Furthermore, the IoT presents problems that the market cannot or will not solve on its own. The most prominent is the market failure and the lack of consumer and manufacturer incentives to resolve technological vulnerabilities in the IoT.[123] Schneier argues that as with environmental pollution, regulation is essential because the dangers and ill effects occur downstream.[124]

---

115 Fu, *supra* note 8, at 8.
116 *Id.* at 3.
117 *Id*.
118 *Id.* at 8–9.
119 See Fu Testimony, *supra* note 21, at 35 (advocating for increased support for these agencies).
120 *See* Schneier Testimony, *supra* note 5, at 31.
121 *Id.* at 59.
122 *See* Id. ("So, yes, this is going to constrain innovation... but this is what we do when innovation can cause catastrophic risk.").
123 *Id.* at 58.
124 *Id.*

In the current political environment, which favors smaller government and reducing regulation, it seems doubtful that this approach could get traction in Congress. And if it did so, recruiting the necessary expertise and resources could be a daunting task.

C. Legalizing Strikebacks

The far more difficult question is what measures can be taken legally to eliminate the threat posed by botnets. This is a pressing consideration because without curative solutions, botnets can be used in multiple crimes.[125] Once a device is recruited into a botnet, it becomes part of a "commodity" that can be rented out "by the hour" or purchased.[126] Relying on enforcement and litigation does little to prevent future attacks, and "is inherently *ex post facto*."[127]

Remedial actions, sometimes referred to as counterstrikes or hack backs,[128] could provide a solution to the botnet problem. These actions might "enable attacked parties to detect, trace, and then actively respond to a threat by, for example, interrupting an attack in progress to mitigate damage to the system."[129] Specific strategies could include implementing a "DoS attack at the botnet controller or hacking the botnet controller and thereby taking control of the botnet."[130] However, not all remedial efforts are so forceful: "Hacking back against a botnet can be as simple and nonaggressive as pushing security patches onto infected computers, just as patients with a deadly virus could be forcibly treated or quarantined to prevent a contagion's spread."[131] Either way, these methods have the potential to help combat botnets and prevent future attacks.

---

125 One illustration of the resilience of botnets can be found in Microsoft and Europol's attempt to dismantle the ZeroAccess botnet: though portions of the botnet were taken down, it was revived within months. Goldman, *supra* note 93, at 610.

126 Janine S. Hiller, *Civil Cyberconflict: Microsoft, Cybercrime, and Botnets*, 31 Santa Clara High Tech. L.J. 163, 168–69 (2015).

127 *See* Kesan, *supra* note 59, at 474.

128 *See* Kesan, *supra* note 59, at 434 (using the terms "hack back" and "counterstrike").

129 *Id.* at 475.

130 *Id.*

131 Patrick Lin, *Ethics of Hacking Back*, U.S. Nat'l Sci. Found. (Sept. 26, 2016), http://ethics.calpoly.edu/hackingback.pdf.

The problem is that such behaviors may be illegal.[132] Ironically, "[t]he same laws that make it illegal to hack in the first place—for instance, to access someone else's system without authorization—presumably make it illegal to hack back."[133] The CFAA both criminalizes botnets and limits recourse against them.[134] The Department of Justice, the FBI, and "White House officials" have all suggested that such remedial efforts may be illegal.[135]

As a result, the legal regime that is intended to protect the public from hacking also limits the extent to which such dangers may be fought. Could counter hacking be legalized? It would raise a host of issues. For example, what would be sufficient to trigger the authority to hack back? Would advance authorization be required? What safeguards would be necessary? Note that botnets may infect millions of computers. What mechanism or procedures could be devised to ensure that the parties who wished to hack back would not do more harm than good? Even if counter hacking is justified in a given instance, what about the danger of misattribution and the potential for injury to innocent parties? From an ethical standpoint, does counter hacking invite vigilantism? Questions abound, and the answers are not easy.

V. Conclusion

The extraordinary growth of the IoT and its extreme vulnerability threaten individuals, businesses, and the broader society. In the United States, federal and state law include offenses that criminalize a wide range of conduct involving the misuse of the IoT. But even the successful prosecution of those offenses—when the offenders can be identified and the U.S. has jurisdiction—does nothing to address two fundamental problems: the enormous number of insecure devices already in use, and the fundamental market failure that continues to bring insecure devices onto the market. The situation is urgent, and policymakers must find new approaches to address these structural problems.

---

132 *See* Kesan, *supra* note 59, at 475 ("Even though counterstrikes are currently of questionable legality....").
133 Lin, *supra* note 131 at 6.
134 *Id.* (Identifying CFAA as a law contributing to this paradox).
135 *Id.*