AN INTERNET OF TORTS

Rebecca Crootof[*]

This is a freewheeling first draft – please do not cite or quote.

[*] Executive Director, Information Society Project; Research Scholar and Lecturer in Law, Yale Law School. I am extraordinarily grateful to BJ Ard and Jack Balkin for years of ongoing conversations about the interactions between law and technology, which inform this entire piece. For productive conversations and useful insights, thanks also to Douglas Bernstein, Oona Hathaway, Woody Hartzog, and the participants in the ISP Fellows' Writing Workshop. And finally, kudos to Ido Kilovaty the working title!

CONTENTS

INTRODUCTION

Once, missing a payment on a leased car would be the first of a multi-step negotiation between a company and a customer, bounded by consumer protection and contract law, mediated and ultimately enforced by the government. Today, as permitted by their lease agreements, car companies are using starter interrupt devices to remotely "boot" cars just days after a payment is missed, effectively side-stepping consumer protection laws and state enforcement procedures.[1] Meanwhile, an individual relying on that car for transport to work, to get to a hospital, or to escape a dangerous situation has an increased risk of injury when his otherwise operational car doesn't start.[2]

Internet of Things (IoT) companies are creating and enforcing their own contractual and architectural governance regimes, enabling currently-lawful but troubling—and sometimes even abusive—practices that increase the risk of property damage and physical harm. This Article explores the social, technological, and legal causes of this changed relationship between companies and consumers; considers how tort law has historically addressed new technologies that altered relationships between industries and individuals; and proposes modifications to existing tort categories to hold companies accountable for their IoT-enabled harms.

IoT devices offer previously-unimaginable convenience, safety, savings, and health and environmental benefits.[3] Pill bottles can remind forgetful individuals to take their medicine, refrigerators can order fresh milk when a family runs out, and tires can send alerts when they become deflated.[4] Chore automation might "cut 100 hours of labor per year for the typical household."[5] Cities can use IoT devices to minimize traffic congestion, tweak public transport schedules, and improve public health through air and water quality monitoring.[6] IoT-enhanced factories are expected to improve

---

[1] Michael Corkery & Jessica Silver-Greenberg, *Miss a Payment? Good Luck Moving That Car*, N.Y. TIMES, Sep. 24, 2014, at A1.

[2] *Id.* (reporting cases where borrowers with disabled cars were unable to take children to the emergency room, were "stranded in dangerous neighborhoods," or had their cars "shut down while idling at stoplights").

[3] While there is no common definition for the Internet of Things, it can be generally understood as the network of implantables, devices, vehicles, buildings, and other physical items that have sensors, software, and network connectivity that enables data collection and sharing. *See infra* Part I.A.

[4] Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 812 (2016) (observing that "objects will collect and share data in an effort to be more efficient or user-friendly").

[5] McKinsey Report, *supra* note 39, at 8.

[6] *Id.* at 3, 9; Meg Leta Jones, *Privacy Without Screens & The Internet of Other People's Things*, 51 IDAHO L. REV. 639, 644 ("Smart street lights that dim automatically

labor efficiency, equipment maintenance, inventory optimization, and worker health and safety.[7] Medical wearables and embedded devices allow for better drug management and the early identification of a need for intervention.[8] The wearable healthcare device market alone is expected to save 1.3 million lives by 2021.[9]

Given these benefits, the IoT device market is growing exponentially. The central finding of a recent McKinsey report was that, if anything, "the hype may actually understate the full potential of the Internet of Things."[10] It estimated that the potential value of the IoT market is now approximately $3.9 trillion, and that its value will increase up to $11.1 trillion by 2025 (which at that time would represent approximately 11% of the world economy).[11] The healthcare IoT market alone is currently worth over $60.4 billion dollars and estimated to reach $136.8 billion by 2020.[12]

But, as with any beneficial new technology, there are accompanying drawbacks and negative externalities. Recent scholarship has highlighted a host of issues raised by the proliferation of IoT devices, including their extensive cybersecurity problems,[13] privacy harms,[14] issues associated with

---

when no one is around save electricity; water mains can inform city managers when to replace or repair them; and parking spaces signal to nearby cameras that they are empty and available to drivers.").

[7] McKinsey Report, *supra* note 39, at 8-9.

[8] Syagnik Banerjee, Thomas A. Hemphill & Phil Longstreet, *Is IOT a Threat to Consumer Consent? The Perils of Wearable Devices' Health Data Exposure* (manuscript), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038872.

[9] Brian Dolan, *Prediction: Health Wearable to Save 1.3 Million Lives by 2020*, MOBIHEALTHNEWS, Dec. 16, 2014, http://www.mobihealthnews.com/39062/prediction-health-wearables-to-save-1-3-million-lives-by-2020.

[10] *Unlocking the Potential of the Internet of Things*, McKinsey Global Institute, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world (last visited Oct. 20, 2017).

[11] McKinsey Global Institute, The Internet of Things: Mapping the Value Beyond the Hype 2 (2015) [hereinafter McKinsey Report], *available at* file:///C:/Users/rlc2/Desktop/The-Internet-of-things-Mapping-the-value-beyond-the-hype.pdf.

[12] Adnan Malik Mohd, *Internet of Things (IoT) Healthcare Market by Component, Application – Global Opportunity Analysis and Industry Forecast, 2014-2021*, ALLIED MARKET RESEARCH (2014), *available at* https://www.alliedmarketresearch.com/iot-healthcare-market.

[13] *See, e.g.*, Ido Kilovaty, *Freedom to Hack*, XX OHIO STATE L.J. (forthcoming 2018).

[14] *See, e.g.*, Laura DeNardis & Mark Raymond, *The Internet of Things as a Global Policy Frontier*, 51 U.C. DAVIS L. REV. 475 (2017); Margot E. Kaminski, Matthew Rueben, William D. Smart & Cindy M. Grimm, *Averting Robot Eyes*, 76 MARYLAND L. REV. 983, 984 (2017).

expanded law enforcement and industry surveillance capabilities,[15] and increased opportunities for surreptitious consumer manipulation.[16]

While this paper will touch on many of these issues, it will not fully address them. Instead, this Article considers how IoT devices empower companies in ways that increase the risk of consumer harm, and how tort law might evolve to hold companies accountable for such actions.

First, IoT companies impose a contractual governance regime on consumers through their terms of service,[17] allowing companies to supplant the "law of the state" with the "law of the firm."[18] Furthermore, IoT companies employ both ex ante architectural regulation and ex post technological self-help to enforce these contracts, thereby sidestepping the state's checks on unfair contractual provisions.[19] Updates necessary for the continued functioning of a device can be conditioned on your consenting to a less restrictive data privacy policy.[20] Your garage door can be left open because you left a bad review on Amazon.[21] Your car can be remotely booted days after a missed payment.[22]

These practices are concerning enough in the digital world, where terms of service and digital rights management (DRM) technologies may keep consumers from copying a DVD or sharing an e-book with friends, but they have far more sinister and dangerous implications in the IoT context. IoT companies can harness devices' surveillance capabilities to impose and monitor compliance with increasingly invasive terms[23]; they can condition

---

[15] *See, e.g.*, Ferguson, *supra* note 4; Steven I. Friedland, *Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things is Changing the Face of Privacy*, 119 W. VIR. L. REV. 891 (2017).

[16] *See, e.g.*, Ryan Calo, *Tiny Salespeople: Mediated Transactions and the Internet of Things*, 2013 IEEE SECURITY AND PRIVACY 70; *see also* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014) (detailing how collected information can be used to manipulate consumer choice).

[17] The issue of inadequate consent has been explored extensively in the privacy harms literature. *See, e.g.*, Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1889-93 (2013).

[18] Radin, *supra* note 31, at 143.

[19] *Id.* at 151 ("The advent of Digital rights Management Systems (DRMS's) has the potential to read out the regulatory contouring of contract . . . .").

[20] Zack Whittaker, *Sonos Says Users Must Accept New Privacy Policy or Devices May "Cease to Function"*, ZERO DAY, Aug. 21, 2017, http://www.zdnet.com/article/sonos-accept-new-privacy-policy-speakers-cease-to-function/.

[21] Sean Gallagher, *IoT Garage Door Opener Maker Bricks Customer's Product After Bad Review*, ARS TECHNICA, Apr. 4, 2017, https://arstechnica.com/information-technology/2017/04/iot-garage-door-opener-maker-bricks-customers-product-after-bad-review/.

[22] Corkery & Silver-Greenberg, *supra* note 1.

[23] *See infra* Part II.A.2 (discussing how GPS trackers are being used to determine in rental and leased cars are driven outside of proscribed areas).

needed security and software updates on consumers agreeing to contractual modifications[24]; and they can they can also disable paid features remotely.[25] Furthermore, because IoT devices often interact with or control the physical environment, should a company "digitally repossess" a device or discontinue the service that renders it useful—either capriciously or per a contractual agreement—there is an increased risk that the consumer will suffer property damage and physical harm.[26] In short, IoT devices enable companies to increase the risk of harm to consumers in new but entirely foreseeable ways.

The history of tort law is a study in how new technologies alter relationships between entities, demanding the creation of expanded duties to address new, technologically-enabled conduct and harms. The Industrial Revolution, whose deadly machines fostered "stranger cases"—situations where one entity unintentionally harmed an unknown other—caused courts to expand negligence from a duty owed a specific, known other to a duty owed to all the world.[27] The rise of mass manufacturing and shipping resulted in the products liability revolution, as courts recognized that industries should owe a duty of due care both towards individuals with whom they shared privity of contract and to anyone who might be foreseeably harmed by their products.[28]

Today, we are at the inflection point of another such revolution. As a product that is both an object and an ongoing service, IoT devices create a new relationship between companies and consumers that is difficult to shoehorn into traditional categories[29]—and this new relationship empowers companies in ways that increase consumers' risks of property damage and physical harms. As with prior, technological-enabled relational shifts, the proliferation of IoT devices will necessitate a reconsideration of what duties industries owe to individuals who will be foreseeably harmed by their actions.

---

[24] *See infra* Part II.A.3 (discussing how Sonos conditioned the ongoing utility of its smart speakers on consumers agreeing to a less restrictive privacy policy).

[25] *See infra* Part II.B.2.b (discussing how Nokia forced a software update that disabled a headlining feature of its smart scales).

[26] *See infra* Part I.B.3 (providing examples).

[27] *See, e.g.*, G. EDWARD WHITE, TORT LAW IN AMERICA: AN INTELLECTUAL HISTORY 13, 16 (1980).

[28] *See, e.g.*, MacPherson v. Buick Motor Co., 111 N.E. 1050, 1053 (N.Y. 1916); Escola v. Coca Cola Bottling Co. of Fresno, 150 P.2d 436, 443 (Cal. 1944) (Traynor, J., concurring).

[29] Granted, contracts that bundle the sale of goods with the provision of services have long existed. As discussed below, however, this is a situation where a difference in degree—in the amount of consumer data collected and in the number of interactions—becomes a difference in kind, as it significantly empowers companies at the expense of consumers. *See infra* Part I.C.

While this Article is the first to explore these issues, it builds upon and contributes to several ongoing conversations. First, as noted above, there is a burgeoning IoT literature. To the extent this literature considers liability issues, however, it tends to do so in the context of addressing cybersecurity problems, privacy harms, and software-related defects.[30] This piece is the first to discuss how the IoT enables companies to create and enforce their own governance regimes and the implications for consumer safety.

Second, Margaret Radin and other intellectual property and cyberlaw scholars have mapped out the issues regarding companies using contract law and technological self-help enforcement mechanisms to sidestep consumer protections and state involvement.[31] I develop these arguments in the IoT context, where increased surveillance capabilities allow companies to create and enforce far more expansive contractual terms, and the physicality of IoT devices permits a different level of architectural enforcement.

Third, technology law scholars are considering how new technologies have rendered fundamental precepts of classic legal subjects nearly unrecognizable. Contract law relies on informed consent and a meeting of the minds—but "shinkwrap" and "click-wrap" contracts make a mockery of

---

[30] While some have acknowledged the increased risk of physical harm associated with IoT devices, invariably this discussion is focused on harms caused when a third party hacks a vulnerable device or there is a software error. *See, e.g.*, FEDERAL TRADE COMMISSION, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 12 (2015) [hereinafter FTC REPORT]; U.S. Chamber Institute for Legal Reform, Torts of the Future: Addressing the Liability and Regulatory Implications of Emerging Technologies 42-43 (2017); Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, 50 U. MICH. J. LAW REFORM 913 (2017); Stacy-Ann Elvy, *The Hybrid Transactions and the INTERNET of Things: Goods, Services, or Software?*, 74 WASH. & LEE L. REV. 77, 118 (2017); Scott J. Shackelford et al., *Securing the Internet of Healthcare*, XX MINN. J.L. SCI. & TECH. (forthcoming 2018). Hackable or malfunctioning cars, pacemakers, and other IoT devices certainly raise a problem worth addressing, but it is fundamentally distinct from the increased risk of physical harm that arises when a company digitally alters or repossesses a device.

[31] MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2012); Julie Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH L.J. 1089, 1103 (1998); Margaret Jane Radin, *Regulation by Contract, Regulation by Machine*, 160 J. INST. THEO. ECON. 142 (2004).

Similarly, scholars from multiple disciplines are exploring how, with the help of new technologies, companies are increasingly appropriating roles once reserved to states. Kate Klonick has highlighted how the content moderation policies of online platforms are shaping what speech is allowed in the public sphere, Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. (forthcoming 2017); Rory Van Loo has discussed how companies internal dispute processes are replacing arbitration and trials, Rory Van Loo, *The Corporation as Courthouse*, 33 YALE J. REG. 547 (2016).

the concept. First year law students learn that property is about a bundle of ownership rights—but in today's world of Kindle books, Uber rides, and Spotify music, there has been a seismic shift from ownership to licensed use.[32] Consumer protection law,[33] copyright law,[34] criminal law,[35] First Amendment law[36]—new technologies are challenging paradigms across the board, rendering any attempt to list the uncertainties they generate necessarily incomplete. This piece's discussion of the interactions between new technology and tort law contributes to this growing TechLaw canon.

Part I discusses how three distinct characteristics of IoT devices—namely, their ability to collect individualized data, their capacity for ongoing communication with a cloud-based service provider, and their physicality—combine to form a product that is simultaneously an object and an ongoing service, which in turn alters the nature of the relationship between companies and consumers. Part II explores why this combination of traits enables new kinds of industry overreach and technologically-enabled industry self-help, with the ultimate effect of increasing the likelihood of consumer property damage and physical harm. Part III considers how this new power imbalance continues a long tradition of technological developments that shifted relations between industry and individuals and discusses how it might be addressed through expansions of products liability law and fiduciary duties.

I. THE INTERNET OF THINGS

Three characteristics of IoT devices—namely, their ability to collect individualized data, their capacity for communication with a cloud-based service provider, and their physicality—combine to form a product that is

---

[32] *See, e.g.*, JOSHUA A.T. FAIRFIELD, OWNED: PROPERTY, PRIVACY AND THE NEW DIGITAL SERFDOM (2017) (warning that we must protect our traditional ownership rights or risk losing them entirely); AARON PERZANOWSKI & JASON SCHULTZ, THE END OF OWNERSHIP: PERSONAL PROPERTY IN THE DIGITAL ECONOMY (2016).

[33] Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 MARYLAND L. REV. 785, 787-88 (2015) (discussing how robots are raising both "common consumer protection issues, such as fraud, privacy, data security, failure to exercise reasonable care and the exploitation of the vulnerable" as well as entirely "new consumer protection issues").

[34] *See, e.g.*, Margot E. Kaminski, *Authorship, Disrupted: AI Authors in Copyright and First Amendment Law*, 51 U.C. DAVIS L. REV. 589 (2017).

[35] *See, e.g.*, Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y. U. ANN. SURV. AM. L. 533 (2017).

[36] *See, e.g.*, Stuart Minor Benjamin, *Algorithms and Speech*, 161 U. PA. L. REV. 1445 (2013); Kaminski, *supra* note 34; Toni M. Massaro, Helen Norton, & Margot E. Kaminski, *SIRI-OUSLY 2.0: What Artificial Intelligence Reveals About the First Amendment*, 101 MINN. L. REV. 2481 (2017).

simultaneously an object and an ongoing service.[37] This distinctive product fundamentally alters the nature of the relationship between companies and consumers.

A. Definition and Scope

There are various definitions for the IoT. A Federal Trade Commission report describes it as encompassing "'things' such as devices or sensors—other than computers, smartphones or tablets—that connect, communicate or transmit information with or between each other through the Internet."[38] A McKinsey report defined it as "sensors and actuators connected by networks to computing systems," "exclude[ing] systems in which all of the sensors' primary purpose is to receive intentional human input."[39] Delightfully, some have described IoT devices as "enchanted objects": "ordinary things made extraordinary."[40]

For the purposes of this paper, I define the IoT as the network of implantables, devices, vehicles, building systems, and other physical items that have sensors, software, and network connectivity that enables data collection and sharing.[41] As this paper is primarily concerned with the relationship between an IoT service provider and consumer, however, it focuses primarily on IoT devices marketed for individual use, rather than industrial IoT systems.

IoT devices might include relatively independent gadgets (like a "smart" front door lock) and integration systems (like a "smart" home hub that networks your front door lock, lights, entertainment, and environmental controls). The universe of IoT devices expands or contracts according with one's definition—but all commentators tend to agree that there is already a mind-boggling number of IoT devices, and that number is set to skyrocket as companies incorporate sensors and wireless capabilities into more and

---

[37] Jack Balkin has cautioned against hyperfocusing on the "essential traits" of a new technology; rather, any analysis of technological-fostered legal disruption must instead be grounded on "what features of social life the technology makes newly *salient*," with an awareness that "[w]hat we call the effects of technology are not so much features of *things* as they are features of *social relations* that employ those things." Jack Balkin, *The Path of Robotics Law*, 6 CALIF. L. REV. CIRCUIT 45, 46, 49 (2015).

[38] FTC REPORT, *supra* note 30, at 5-18, 5.

[39] McKinsey Global Institute, The Internet of Things: Mapping the Value Beyond the Hype 2 (2015) [hereinafter McKinsey Report], *available at* file:///C:/Users/rlc2/Desktop/The-Internet-of-things-Mapping-the-value-beyond-the-hype.pdf.

[40] DAVID ROSE, ENCHANTED OBJECTS: DESIGN, HUMAN DESIRE, AND THE INTERNET OF THINGS 7 (2014).

[41] One of the major definitional debates is whether desktop computers, laptops, or tablets should be included in the definition.

more items.[42] A 2015 McKinsey Report estimated that "there are more than nine billion connected devices around the world, including smartphones and computers," and that by 2025 there may be somewhere between 25 to 50 billion such devices.[43] Others predict that there will be more than one trillion IoT devices by 2025.[44]

B. Relevant Traits

1. Sensors and Identifiers

The ability to collect, share, and process individualized data is a critical IoT trait. Indeed, the term "Internet of Things" was coined in a discussion of this new capability, when Kevin Ashton noted, "Adding radio-frequency identification and sensors to everyday objects will create an Internet of Things, and lay the foundations of a new age of machine perception."[45] Sensors may collect information on anything from the ambient temperature to how many mantras you have recited on your prayer beads.[46]

While general, anonymized data provides a wealth of information on its own, IoT sensors often link information to a unique identifier. A patient telemonitoring system, for example, would be of little use if the gathered data was not associated with a particular individual. Here, the possibility of particularized data raises the possibility of particularized data disclosures, as early Fitbit users awkwardly learned.[47]

---

[42] Thanks to recent technological, economic, and regulatory advancements, it is increasingly easy to transform a once "dumb" item into an IoT device. This bent has sparked Twitter feeds like @internetofshit, which catalogs completely unnecessary IoT products, including doghouses, coffee mugs, sex toys, jean jackets, condoms, and fidget spinners.

[43] McKinsey Report, *supra* note 39, at 17.

[44] Bill Wasik, *In the Programmable World, All Our Objects Will Act as One*, WIRED (May 14, 2013), http://www.wired.com/2013/05/internet-ofthings-2/all.

[45] Kevin Ashton, *That 'Internet of Things' Thing*, RFID J. (June 22, 2009), http://www.rfidjournal.com/articles/view?4986.

[46] Ko Tin-yao, *Buddhists Go High-Tech: Acer to Launch Smart Prayer Beads*, EJINSIGHT, Jan. 30, 2018, http://www.ejinsight.com/20180130-buddhists-go-high-tech-acer-to-launch-smart-prayer-beads/.

[47] Fitbit originally made its users' profiles and activity public by default, with the intention of advertising the service. Unfortunately, this resulted in many users unintentionally publishing records of their sexual activity. Jack Loftus, *Dear Fitbit Users, Kudos On the 30 Minutes of "Vigorous Sexual Activity" Last Night*, GIZMODO, Jul. 3, 2011, https://gizmodo.com/5817784/dear-fitbit-users-kudos-on-the-30-minutes-of-vigorous-sexual-activity-last-night.

Much of the data currently collected by purchased IoT devices is explicitly or implicitly volunteered[48]: Individuals choose to wear fitness trackers and to install smart home hubs. Increasingly, however, data about or lives is being collected without our knowledge—by our own IoT devices,[49] by others' devices,[50] and by public devices[51]—and additional data is generated through aggregation and extrapolation.[52] In 2012, for example, London installed smart garbage bins, which collected data from smart phones to provide targeted advertisements.[53] Thus the growing IoT ecosystem is creating an environment of ongoing state and industry surveillance.[54]

2. Communication with a Cloud-Based Service Provider

IoT devices have one or multiple transmitters that permit information sharing with other devices and with cloud-based service providers, either on a sporadic or constant basis.[55] Device-to-device systems are useful when there is no need to share data widely, as is the case with a heart monitor paired with a smartwatch or a key fob paired with a vehicle.[56] Most IoT

---

[48] Friedland, *supra* note 15, at 898. However, consumers often have nearly no ability to accurately judge the consequences of sharing information.. *See, e.g.*, Solove, *supra* note 17, at 1889-93.

[49] Ferguson, *supra* note 4, at 822 (noting that "many consumers may not even know they possess objects that are revealing information about their personal lives"); *see also* Hudson Hongo, *Smart Sex Toy Maker Sued for Sneakily Collecting 'Intimate' Data*, GIZMODO, Sep. 12, 2016, https://gizmodo.com/smart-sex-toy-maker-sued-for-sneakily-collecting-intima-1786559792 ("In August, hackers at the Def Con security conference revealed that Standard Innovation's We-Vibe smart vibrators transmitted user data—including heat level and vibration intensity—to the company in real time.").

[50] Ferguson, *supra* note 4, at 811 ("[W]hat we ordinarily think of as static objects will become communication tools, revealing our paths, interests, habits, and lives to companies and law enforcers.").

[51] Jones, *supra* note 6, at 647 ("There is no opportunity for notice and choice in smart publics or any smart shared space.").

[52] As IoT devices collect information on the "micro-patterns" of an individual's habits, it will be increasingly possible to predict "future macro-patterns." Ferguson, *supra* note 4, at 822.

[53] Siraj Datoo, *The Recycling Bin is Following You*, QUARTZ, Aug. 8, 2013, https://qz.com/112873/this-recycling-bin-is-following-you/.

[54] *See infra* Part II.A.1 (discussing pervasive IoT-enabled surveillance).

[55] IoT connectivity structures can take a variety of forms: IoT devices can connect with and transmit data to other devices, to a cloud-based service provider, or to a hub or gateway which then connects to a cloud-based service provider. David Hamilton, *The Four Internet of Things Connectivity Models Explained*, WEB HOST INDUSTRY REVIEW, Apr. 29, 2016, http://www.thewhir.com/web-hosting-news/the-four-internet-of-things-connectivity-models-explained.

[56] *Id.*

devices, however, are able to communicate with a cloud-based service provider.[57] As this paper is primarily concerned with issues arising from the ability of IoT devices to communicate with both their owners and with outside entities, it focuses on IoT devices that directly or indirectly connect with cloud-based service providers.

IoT devices' connectivity is vital to their continued utility, both because connectivity is necessary to many of the tasks for which the devices are purchased and because it allows companies to send security updates that address newly-discovered zero-day vulnerabilities and malware. However, connectivity also introduces a host of cybersecurity issues, largely because a communications stream introduces attack vectors. As IoT devices proliferate, so do stories of hacked IoT devices causing harms, ranging from hackers terrorizing individual children through baby monitors[58] and remotely controling vehicles[59] to wide scale privacy violations[60] to worldwide botnet attacks that can take down large swaths of the internet.[61]

---

[57] *Id.* Sometimes this is accomplished directly; other times, devices will connect to a hub that acts as a gateway to the cloud-based service provider. *Id.* Fitbits, for example, upload information to a smartphone app, which then transmits that data to the cloud; smart home IoT devices are often networked through some kind of hub. Sometimes the service-provider is the same company that sold the device; sometimes it is a third party, providing a separate servive. Various health-related apps, for example, will collect and aggregate data from wearable trackers, smart scales, and other IoT devices to create a more holistic assessment of an individual's overall health profile.

[58] *Man Hacks Monitor, Screams at Baby Girl*, NBC NEWS, Apr. 28, 2014, https://www.nbcnews.com/tech/security/man-hacks-monitor-screams-baby-girl-n91546.

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

[60] In 2012, hackers posted live feeds to the Webs from nearly 700 cameras made by Trednet for everything from baby monitoring to home security. Richard Adhikari, *Webcam Maker Takes FTC's Heat for Internet-of-Things Security Failure*, TECHNEWSWORLD, Sep. 5, 2013, https://www.technewsworld.com/story/78891.html.

[61] In October 2016, the Mirai malware compromised IoT devices—including printers, security cameras, and baby monitors—were used to launch the largest distributed denial-of-service (DDoS) attack to date. Lily Hay Newman, *What We Know About Friday's Massive East Coast Internet Outage*, WIRED, Oct. 21, 2016, https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/. The target, Dyn, plays a critical role in the internet infrastructure; when it was overwhelmed, most of the U.S. Eastern seaboard had limited or no access to popular sites like AirBnB, Amazon, BBC, CNN, Comcast, Etsy, 538, Fox News, HBO, Imgur, Netflix, the *New York Times*, Overstock, Paypal, Pinterest, Reddit, Spotify, Starbucks, Tumblr, Twitter, Verizon Comm'n, Visa, Walgreens, the *Wall Street Journal*, Wikia, Wired, Xbox Live, and Yelp. *Id.*; Ethan Chiel, *Here Are the Sites You Can't Access Because Someone Took the Internet Down*, SPLINTER, Oct. 21, 2016, https://splinternews.com/here-are-the-sites-you-cant-access-because-someone-took-1793863079. A newly discovered malware, known as IoT Troop and Reaper, may be even more pernicious than Mirai. Andy Greenberg, *The Reaper*

While the (lack of) cybersecurity for IoT devices is a growing problem, this paper focuses instead on two other implications of IoT devices' ongoing connectivity. First, ongoing connectivity enables more extensive company surveillance, as devices are constantly "reporting back" on their owners.[62] Second, it allows companies to alter how already-purchased devices operate.[63]

3. Physicality

IoT devices have physicality: a presence in and ability to interact with the physical world. To some, this is the most important feature. According to Laura DeNardis and Mark Raymond, "The 'Internet of Things' is a tepid conceptual phrase designed to characterize [a] major transformation in the evolution of the Internet: its expansion beyond communication between people, or between people and information content, and into billions of everyday objects."[64]

With physicality comes the possibility of physical harm.[65] Consider the relatively innocuous Roomba, an autonomous vacuum cleaning robot. The ability to interact with the physical world has allowed Roombas to clean untold numbers of floors, but one Roomba caused the Pooptastrophe[66]; another "attacked" its sleeping owner[67]; and a third destroyed itself on a hot plate and, due to the resulting smoke damage, left its owner homeless.[68]

Similarly, IoT devices have the potential to cause or increase the risk of physical damage, ranging from inconvenient property destruction to life-threatening harms. A car that doesn't start is more than an inconvenience—

IoT Botnet Has Already Infected a Million Networks, WIRED, Oct. 20, 2017, https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/.

[62] *See infra* Part II.A.1.

[63] *See infra* Part II.B.2.

[64] DeNardis & Raymond, *supra* note 14, at 477.

[65] Balkin, *The Path of Robotics Law*, *supra* note 37, at 49; Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513, 534 (2015).

[66] Jessie Newton, Facebook, Aug. 9, 2016 ("Do not, under any circumstances, let your Roomba run over dog poop. . . . Because if that happens, it will spread the dog poop over every conceivable surface within its reach, resulting in a home that closely resembles a Jackson Pollock poop painting.").

[67] Justin McCurry, *South Korean Woman's Hair 'Eaten' By Robot Vaccum Cleaner as She Slept*, THE GUARDIAN, Feb. 8, 2015, https://www.theguardian.com/world/2015/feb/09/south-korean-womans-hair-eaten-by-robot-vacuum-cleaner-as-she-slept (noting that the vacuum may not have been appropriately programmed for cultures where it is common to sit or nap on the floor).

[68] *Robot Suicide? Rogue Roomba Switches Self On, Climbs Onto Hotplate, Burns Up*, THE HUFFINGTON POST, Nov. 13, 2013, https://www.huffingtonpost.com/2013/11/13/robot-suicide-roomba-hotplate-burns-up_n_4268064.html.

in certain situations, it can be the difference between safety and danger.[69] A disabled smart thermostat could allow a house to become so hot or cold that materials, plumbing, pets, and potentially even people could be harmed. Should an IoT door opener be deactivated, the home might be burgled and the occupant assaulted.

IoT medical devices (the "Internet of Us" or "Internet of Things Inside Our Body") makes these risks all the more obvious. For example, in 2016, a man who passed out while driving due to low blood sugar filed a suit against Dexcom, alleging that their smart glucose monitoring device's alarm didn't go off when his blood sugar levels dropped.[70] He crashed his car, suffering injuries and totaling the vehicle.[71]

Some of these harms will merely be the latest manifestation of familiar product liability problems. As with any other product, "smart" devices, vehicles, or buildings can be poorly designed, improperly manufactured, or inadequately labeled with appropriate instructions for use. In *In re Toyota Motor Corp*., for example, plaintiffs alleged first that their Toyotas had a software defect that caused the cars to accelerate even while the driver was applying the brakes; and, second, that the company had failed to warn purchasers of the risk of unintended acceleration.[72]

One interesting question is whether poor cybersecurity protections for an IoT device would constitute a design defect or breach of an implied warranty.[73] In the mad rush to be first to market, companies unaccustomed to considering cybersecurity issues are slapping sensors and transmitters on everything from Barbie dolls to refrigerators.[74] Indeed, a common refrain is that "The 'S' in 'IoT' stands for 'security.'" Unsurprisingly, these easily-

---

[69] Corkery & Silver-Greenberg, *supra* note 1 (reporting cases where borrowers with disabled cars were unable to take children to the emergency room, were "stranded in dangerous neighborhoods," or had their cars "shut down while idling at stoplights").

[70] Emily Field, *Blood Sugar Monitor Maker Hit with Suit Over Car Crash*, LAW360, Aug. 31, 2016, https://www.law360.com/articles/834866/blood-sugar-monitor-maker-hit-with-suit-over-car-crash.

[71] *Id.*

[72] In re Toyota Motor Corp. Unintended Acceleration Marketing, Sales Practices, and Products Liability Litigation, 754 F. Supp. 2d 1145, 1192 (C.D. Cal. 2010).

[73] *See* Butler, *supra* note 30 (arguing that companies should be held liable for harms caused by hacked IoT devices); Elvy, *supra* note 30, at 85 ("The failure of an IOT manufacturer to secure an IOT device or the data generated by an owner's use of an IOT device should serve as the basis for breach of implied warranty claims under Article 2 [of the UCC].").

[74] *See* JAN-PETER KLEINHANS, INTERNET OF INSECURE THINGS: CAN SECURITY ASSESSMENT CURE MARKET FAILURES? (Dec 2017) ("A company that has built household appliances . . . for decades has a lot of experience in mechanical engineering and physical safety. Yet they do not necessarily know much about secure software development processes. . . . This can be inferred simply from the amount of amateurish and easily exploitable software vulnerabilities found in many smart household appliances.").

hacked IoT devices are generating a host of individual and worldwide data-related harms.[75] Due to the physicality of these systems, however, companies' poor cybersecurity practices are also generating a greater risk of physical harm.[76] Relay devices have been used to interrupt device-to-device systems to enable car theft[77]; security flaws in Apple's HomeKit smart home system allowed hackers to unlock front doors[78]; and a team of researchers were able to remotely take total control of a Jeep SUV while it was being driven.[79] The insecurity of the "Internet of Things Inside Our Body" [80] also risks deadly hacks, as highlighted by Vice President Dick Cheney's decision to disable his heart implant's wireless connectivity while he was in office and the recent FDA-mandated recall of more than 400,000 pacemakers due to a cybersecurity vulnerability.[81] Furthermore, as critical infrastructure like electrical grids, transportation services, and health and medical systems become incorporated into the IoT ecosystem, the more likely it is that disruption of those systems will threaten human safety.[82] In June 2017, for example, the NotPetya malware attack rendered data on compromised systems completely inaccessible, forcing banks to close, hospitals to cancel operations, and the radiation monitoring system at Ukraine's Chernobyl Nuclear Power Plant to go offline.[83]

---

[75] *See supra* text accompanying notes 58-61.

[76] FTC REPORT, *supra* note 30, at 12.

[77] In November 2017, British police released footage of a Mercedes with an IoT key fob being stolen via relay. Two thieves pull up outside of a house, each with a relay box (a device that receives and sends signals through walls, doors, and windows). One stands in front of the home, another by the locked car. The first thief's box receives a signal from the indoor key fob and transmits it to the second's; the second thief's box receives the signal and transmits it to the car. The second thief unlocks the car, turns it on, and they both drive away. *Police Release Footage of 'Relay Crime'*, ITV NEWS, Nov. 26, 2017, http://www.itv.com/news/central/2017-11-26/police-release-footage-of-relay-crime/.

[78] Samuel Gibbs, *Apple Fixes HomeKit Bug That Allowed Remote Unlocking of Users' Doors*, THE GUARDIAN, Dec. 8, 2017, https://www.theguardian.com/technology/2017/dec/08/apple-fixes-homekit-bug-remote-unlocking-doors-security-flaw-iphone-ipad-ios-112-smart-lock-home.

[79] Greenberg, *supra* note 59.

[80] Ian Kerr, *The Internet of People? Reflections on the Future Regulation of Human-Implantable Radio Frequency Identification*, *in* LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY AND IDENTITY 335 (Ian Kerr, Valerie Steeves & Carole Lucock Eds., 2009).

[81] *Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication*, FED. DRUG ADMIN. (Aug. 29, 2017), https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm.

[82] DeNardis & Raymond, *supra* note 14, at 486.

[83] Nicole Perlroth, Mark Scott & Sheera Frenkel, *Cyberattack Hits Ukraine Then Spreads Internationally*, N.Y. TIMES (June 27, 2017),

C. An Object and an Ongoing Service

Once, a buyer purchased a coffee maker, thermostat, or car from a seller; assuming the device worked properly, that would be the end of the relationship.[84] Now, however, the buyer of an IoT coffeemaker, thermostat, or car purchases a package of tangibles and intangibles: a physical device; embedded software, and the ongoing provision of one or more services.[85] A smart coffeemaker links with your bed to start brewing coffee as soon as you awaken. A smart thermostat learns a household's schedule and preferred temperatures to build an energy-saving heating plan and create a monthly customized energy report. An internet-connected car might provide built-in navigation, roadside assistance, or real-time alerts regarding engine, emission, or airbag status. Even the most seemingly independent IoT devices need regular security updates to address newly discovered zero-day vulnerabilities and malware. Thus, an IoT device's ability to collect individualized data and to communicate with a cloud-based service provider results in a product that is simultaneously a physical object and something that provides an ongoing, personalized service.

At first look, this may appear to be simply a slight extension of the goods/services continuum. Certainly, contracts that bundle the sale of goods and the provision of services have long existed (and long bedeviled courts and UCC scholars). Appliances often come with installation, upkeep, or warranty services; contracts for building a pool or shed might include descriptions of both the materials and work being purchased.[86] While there is some debate as to whether certain utilities themselves are goods or

---

https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html?mcubz=0&_r=0.

[84] Even acknowledging the services-goods continuum, most commodity goods tend to be closer to the "pure good" end of the spectrum.

[85] Elvy, *supra* note 30, at 144-45. This is related to what Radin has termed the "contract as product" understanding of contract law, which she defines as occurring when "the contract is part of the product, part of the collection of functional components, and not a separate text about that collection." Margaret Jane Radin, *Information Tangibility*, *in* ECONOMICS, LAW AND INTELLECTUAL PROPERTY 395, 410 (Ove Granstand, ed., 2003). A consumer no longer just buys a phone: she buys a phone with specific contractual terms, such as a requirement to litigate disputes in California under California law. *Id.* at 411-12. Similarly, with IoT devices, you are not only buying the device—you are buying the device, the service, and the terms of that service. *See id.* at 412-14 (discussing how this conflation is undermining the "idea that a contract is a text, separate from and 'about' (accompanying) some machine or functionality").

[86] Elvy, *supra* note 30, at 91.

services,[87] even utility companies that are considered service providers often demarcate elements of the infrastructure they and a property owner are respectively responsible for purchasing and maintaining. But there are elements of the IoT service/good combination that distinguish these from other bundled contracts.

First, while companies have always been able to glean information about their customers from interactions, IoT devices are collecting, crunching, and conveying individualized data on an entirely new scale. They send information about when you wake, how long you brush your teeth, when you turn your lights on or off, what shows you watch and how often you watch them,[88] what you search for in search engines, what websites you visit, and how long you spend reading them.[89]

Second, IoT devices permit a near-constant level of interaction between companies and consumers. Historically, most interactions bundled with the sale of a good tended to be relatively infrequent, known interactions. Installation services are quickly fulfilled; maintenance services occur at regularly scheduled intervals; warranty services are only triggered in the event of a malfunction or defect and are bounded by a known end date. And while utilities are provided nearly constantly, a property owner's interactions with a utility company are limited to monthly meter readings or as-needed repairs to portions of the system under their control. In contrast, many IoT devices depend upon a near-constant connection with a cloud-based service provider for their continued utility. The Amazon Echo, for example, connects with company servers every few minutes.[90]

This results in a situation where a difference in degree—both in the amount of consumer data collected and in the number of interactions—becomes a difference in kind, as a company knows far more about individual consumers and consumers are increasingly dependent on companies' continued provision of services for their items' continued

---

[87] Water is often understood to be a good, but categorizing electricity confounds courts and scholars. *See, e.g.*, Steven Ferrey, *Unresolved Judicial Conflict and Critical Infrastructure*, 3 TEX. A&M L. REV. 581 (2016) (highlighting how electricity is variously considered a good or a service in different areas of law, even within the same state).

[88] Companies may even use this information to mock you. In December 2017, Netflix tweeted, "To the 53 people who've watched A Christmas Prince every day for the past 18 days: Who hurt you?" Netflix US (@netflix), TWITTER (Dec. 10, 2017, 6:52 PM), https://twitter.com/netflix/status/940051734650503168.

[89] Kashmir Hill & Surya Mattu, *The House That Spied on Me*, GIZMODO (Feb. 7, 2018; 1:25 PM), https://gizmodo.com/the-house-that-spied-on-me-1822429852. All of this traffic is available not only to the individual cloud-based service providers, but also to the Internet Service Provider (ISP). *Id.*

[90] *Id.*

functioning.[91] As detailed in the next two Parts, this profoundly changes the relationship between companies and consumers, empowering the former at the expense of the latter.[92]

II. NEW OPPORTUNITIES FOR INDUSTRY OVERREACH

IoT companies are borrowing two tactics from digital tech companies' playbook: they are using terms of service to create new contractual governance regimes that displace consumer protection laws, and they are relying on technological self-help to enforce them. If anything, IoT companies are far more empowered than their digital precursors, as the surveillance enabled by IoT devices allow companies to include increasingly invasive terms in their contracts and the IoT devices' ongoing connectivity and obligatory security updates allow companies to condition the devices' continued utility on acquiescence to new terms. Furthermore, the physicality of IoT devices increases the likelihood of property damage and physical harm should a company discontinue service or otherwise "digitally repossess" the device. Collectively, IoT devices enable myriad opportunities for harmful industry overreach, with little government oversight and few routes of recourse.

A. The Law of the Surveilling Firm

As Margaret Radin detailed while discussing terms of service agreements in the intellectual property context, private firms are

---

[91] Granted, any given IoT device's reliance on an ongoing service varies. Elvy, *supra* note 30, at 100 ("[T]he range of operations of an IOT device is very much dependent on the services and software provided by companies.").

Some IoT devices' utility may be entirely contingent on the ongoing provision of a service. Without the ability to exchange information with a cloud-based service provider, an Amazon Echo, a Google Home, or another IoT hub is little more than an unusually expensive doorstop—as owners of the Revolv learned to their dismay when the company announced it would be shutting down support for the hub and its associated apps. Alissa Walker, *If You Use Revolv's Smart Hub, You Are Officially Screwed (Thanks Nest!)*, GIZMODO, Apr. 4, 2016, https://gizmodo.com/nest-owned-smart-hub-gets-permanently-killed-1768977505.

For other IoT devices, the lack of the service will merely render a once-"smart" item dumb. In 2016, for example, lighting company TCP stopped hosting a server that enabled their IoT lightbulbs' remote functionality. Kate Cox, *TCP Disconnects "Smart" Lightbulb Servers, Leaves Buyers in the Dark*, CONSUMERIST, Sep. 26, 2016, https://consumerist.com/2016/08/19/tcp-disconnects-smart-lightbulb-servers-leaves-buyers-in-the-dark/. The bulbs still provide light, but the capabilities that justified their steeper price tag no longer exist. *Id.*

[92] Elvy, *supra* note 30, at 91.

increasingly using contracts—especially boilerplate, shrink-wrap, and "click-wrap" contracts[93]—to supersede the law of the state.[94] Exculpatory clauses negate otherwise permissible claims for redress, purporting to relieve firms of liability for harm caused by negligent, reckless, and even intentional acts; mandatory pre-dispute arbitration clauses eliminate the right to a jury trial and aggregate remedies, such as class action suits; and choice of law or choice of forum clauses mandate litigating in jurisdictions where the law favors the firm or makes it more difficult for plaintiffs to bring suit.

Even when certain provisions would be deemed unconscionable or otherwise unenforceable if litigated, these contracts operate as a *de facto* governance regime.[95] Most people adversely affected by the contracts will not challenge the terms, because they are deterred by high litigation costs or the common assumption that contractual terms must be enforceable.[96] Even should some people win suits challenging certain provisions, contract damages in those relatively few cases are not sufficiently high to deter companies from continuing to employ generally lucrative terms.[97] Over time, the "law of the state," which, for all of its faults, nonetheless reflects myriad interests and presumably exists to benefit the general public, is

---

[93] "Click-wrap" contracts take many forms, but they usually require a consumer to agree to certain terms in order to proceed with accessing information or making a purchase online. The terms of service need not appear in the same pop-up, webpage, or window, but as a nod to the theoretical requirement that the consumers' consent is informed, the terms must be accessible before a consumer is required to accept them. Obviously, however, consumers rarely review those terms. As Kate Darling tweeted, in response to a persistent Twitter pop-up that required users to agree to a new privacy policy, "Father, hear my confession. I was forced to lie and click a button that said 'sounds good' to make a pop-up window go away." Kate Darling, TWITTER (May 17, 2017, 1:59 PM), https://twitter.com/grok_/status/864948428727570432.

[94] Radin, *supra* note 31, at 143 (characterizing this as "replacing the law of the state with the 'law' of the firm").

[95] A seminal case addressing contractual overreach in a consumer context is *Williams v. Walker-Thomas Furniture Co.*, 350 F.2d 445 (D.C. Cir. 1965) (voiding a contract as unconscionable). However, it is worth considering how many individuals likely had their goods unfairly repossessed before Williams brought suit challenging the contractual term.

[96] Radin, *supra* note 31, at 145; *see also* Charles A. Sullivan, *The Puzzling Persistence of Unenforceable Contract Terms*, 70 OHIO ST. L.J. 1127 (2009); Meirav Furth-Matzkin, *On the Unexpected Use of Unenforceable Contract Terms: Evidence from the Residential Rental Market*, 9 J. LEG. ANALYSIS 1 (2017) (discussing how landlords regularly include deceptive and clearly invalid terms in their contracts, which likely significantly affects tenants' decision to forgo valid legal rights and claims).

[97] Radin, *supra* note 31, at 145.

effectively superseded by the contractual "law of the firm," which benefits and reflects the interests of the firm.[98]

IoT companies are adopting similar practices to their digital precursors, but if anything they are even more insidious in the IoT context. IoT devices surveil and report on their users, enabling companies to include and identify violations of increasingly invasive terms. Additionally, necessary software and security updates allow companies to condition a device's continued functioning on consumer acquiescence to even less favorable terms.

1. Pervasive IoT Surveillance

According to Woody Hartzog, "When robots are fully realized, they will be nothing short of a perfected surveillance machine."[99] Robots are able to gather and store vast amounts of data, thanks to "cameras, motion and audio sensors, facial and object recognition technologies, and even biological sensors."[100] In part because of their physicality, human beings are surprisingly willing to share information with a robot, even information that they would not share with other individuals.[101] Furthermore, robots are able to collect information in the home,[102] a traditionally private space.[103]

But any robot can be made into an IoT device—and it will be the IoT device, with its ability to record and transmit data in real time, that will enable even more perfected surveillance, both in the home and in public spaces. People often purchase IoT items for their home with the expectation that they will connect with other devices and thereby make life more convenient; they may not realize how extensively those devices are

---

[98] *Id.* at 147. A similar evolution is occurring in the workplace context, as the "law of the employer" is increasingly supplanting the law of the state. ELIZABETH ANDERSON, PRIVATE GOVERNMENT (2017). "Smart" workplaces will undoubtedly exacerbate this trend.

[99] Hartzog, *supra* note 33, at 798.

[100] *Id.* at 797.

[101] *See, e.g.*, Calo, *Robots and Privacy*, *in* ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS 187, 188 (Patrick Lin, George Bekey, & Keith Abney, eds. 2012); Hartzog, *supra* note 33, at 794; Laurel D. Rick, *Wizard of Oz Studies in HRI: A Systematic Review and New Reporting Guidelines*, 1 J. HUMAN-ROBOT INTERACTION 119 (2012).

[102] For example, newer Roomba models map the interiors of their homes, raising the possibility that these maps may be sold to third parties. Maggie Astor, *Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared*, N.Y. TIMES, Jul. 25, 2017, https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html?_r=0.

[103] Calo, *Robots and Privacy*, *supra* note 101, at 188 (arguing that robots enable access to historically protected spaces).

reporting back to cloud-based service providers.[104] As detailed in a recent article about a monitored smart home, not an hour passed without devices contacting outside servers.[105] Amazon's Echo and Echo Dot contacted Amazon servers every few minutes; even the smart plugs—which merely control and monitor electrical usage—were "pinging home almost every hour."[106] Nor can consumers opt out of these surveillance systems: most purchase agreements require consumers to consent to data reporting and warranties are often conditioned on not tampering with the IoT device.[107]

Meanwhile, as the IoT ecosystem grows, so too does the surveillance state.[108] From trash bins gathering data from pedestrian smartphones[109] to billboards using facial recognition to advertise to women[110] to autonomous vehicles that gather information about others' driving habits,[111] state and industry actors are increasingly using IoT devices to collect information in public spaces. And new technology is enabling new levels of public/private cooperation and cooptation.[112] With some well-publicized exceptions,[113]

---

[104] *Cf.* Ignacio Cofone & Adriana Robertson, *Consumer Privacy in a Behavioral World*, 69 HASTINGS L. J. (forthcoming 2018) (discussing how consumers have difficulties aggregating the extent to which different pieces of information lead to privacy loss).

[105] Hill & Mattu, *supra* note 89.

[106] *Id.*

[107] *See, e.g.*, Kashmir Hill, *Nest Hackers Will Offer Toot to Keep the Google-Owned Company From Getting Users' Data*, FORBES, Jul. 16, 2014, https://www.forbes.com/sites/kashmirhill/2014/07/16/nest-hack-privacy-tool/#3b38af583464 (discussing how Nests report household information to Google and how the device can be altered to prevent it from sending personal data).

[108] *See* Bruce Schneier, *Security and the Internet of Things*, SCHNEIR ON SECURITY (Feb. 1, 2017, 8:24 AM), https://www.schneier.com/blog/archives/2017/02/security_and_th.html (: "The internet is no longer a web that we connect to. Instead, it's a computerized, networked, and interconnected world that we live in.").

[109] Datoo, *supra* note 53 (discussing London's smart garbage bins, which collected data from pedestrians' smart phones).

[110] Mike Pomranz, *Beer Billboard Uses Facial Recognition to Advertise Only to Women*, FOOD & WINE, Jun. 23, 2017, http://www.foodandwine.com/fwx/drink/beer-billboard-uses-facial-recognition-advertise-only-women.

[111] Autonomous vehicles must collect extensive data about their environment in order to operate and under current law, and that data can all be obtained by law enforcement. Cyrus Farivar, *Why Cops Won't Need a Warrant to Pull the Data Off Your Autonomous Car*, ARS TECHNICA, Feb. 3, 2018, 8:00 AM, https://arstechnica.com/tech-policy/2018/02/why-self-driving-cars-may-be-heaven-for-investigating-crimes-and-accidents/.

[112] *See* Jack Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation* (manuscript) at 33 (exploring this development in the context of speech regulation); Jack Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2324-29 (2014) (same).

[113] *See, e.g.*, Amy B. Wang, *Can Alexa Help Solve a Murder? Police Think So—But Amazon Won't Give Up Her Data*, WASH. POST, Dec. 28, 2016,

U.S. law enforcement is increasingly relying on access to IoT industry data.[114] There is a growing number of stories of IoT devices "tattling" on their owners, including a pacemaker that provided information for an arson charge[115] and a car that reported a hit-and-run accident.[116]

2. Invasive Contractual Terms

In addition to collecting lucrative data, ongoing IoT surveillance also enables companies to identify violations of once-unenforced terms. For example, car rental companies have long prohibited renters from driving outside of state lines. Absent an out-of-state accident, however, this requirement was often ignored by both the company and consumer, as both recognized that the term was generally unenforceable (if still a useful liability escape for the company should there be an out-of-state accident).[117]

---

https://www.washingtonpost.com/news/the-switch/wp/2016/12/28/can-alexa-help-solve-a-murder-police-think-so-but-amazon-wont-give-up-her-data/?utm_term=.d376e9272ac6.

[114] *See, e.g.*, Ferguson, *supra* note 4; Friedland, *supra* note 15. China is leading the development of big-data police states: it already constantly monitors the Uighurs, an ethnic minority, James A. Millward, *What It's Like to Live in a Surveillance State*, N.Y. TIMES, Feb. 3, 2018, https://www.nytimes.com/2018/02/03/opinion/sunday/china-surveillance-state-uighurs.html; and it is on track to create a mandatory, country wide social credit system by 2020, Rachel Botsman, *Big Data Meets Big Brother as China Moves to Rate Its Citizens*, WIRED, Oct. 21, 2017, http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion; Mara Hvistendahl, *Inside China's Vast New Experiment in Social Ranking*, WIRED, Dec. 14, 2017, https://www.wired.com/story/age-of-social-credit/. Additionally, China is exporting its surveillance technologies to other countries for use in law enforcement. Jun Mai, *Ecuador is Fighting Crime Using Chinese Surveillance Technology*, SOUTH CHINA MORNING POST, Jan. 22, 2018, http://www.scmp.com/news/china/diplomacy-defence/article/2129912/ecuador-fighting-crime-using-chinese-surveillance.

[115] Mariella Moon, *Judge Allows Pacemaker Data to Be Used in Arson Trial*, ENGADGET, Jul. 13, 2017, https://www.engadget.com/2017/07/13/pacemaker-arson-trial-evidence/.

[116] Jenn Gidman, *Hit-and-Run Suspect Ratted Out by Her Own Ford Focus*, USA TODAY, Dec. 8, 2015, https://www.usatoday.com/story/news/nation/2015/12/08/hit-and-run-suspect-ratted-out-her-own-ford-focus/76975658/. As Ford's Global VP for Marketing and Sales stated, "We know everyone who breaks the law, we know when you're doing it. We have GPS in your car, so we know what you're doing." However, the VP quickly retracted his statement after negative media coverage. Jim Edwards, *Ford Exec Retracts Statements About Tracking Drivers with the GPS in Their Cars*, BUSINESS INSIDER, Jan. 9, 2014, http://www.businessinsider.com/ford-jim-farley-retracts-statements-tracking-drivers-gps-2014-1.

[117] As Karen Levy has noted in the context of discussing blockchain-based contracts, contracts serve many functions that are not necessarily legal in nature, and as a consequence they are not always designed to be formally enforced. Karen E.C. Levy, *Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and the Social Workings of Law*, 3 ENGAGING SCI., TECH., & SOC'Y 1 (2017).

But GPS trackers now allow companies to monitor where a car is driven: a 2004 story details how one renter, who anticipated a $259.51 rental bill, had to pay $3,405.05, due to a $1-per-mile fine for having crossed state lines.[118] More recently, a woman's auto loan contract restricted her from driving outside of a four-county zone.[119] When she fled to a shelter outside of that zone to escape her abusive husband, the company sent a tow truck to retrieve the vehicle.[120]

IoT surveillance capabilities also invite companies to incorporate increasingly invasive terms, precisely because they can now be enforced. Car lessors are capable of monitoring whether borrowers regularly travel to work, presumably to anticipate whether that person will default on their loan[121]; it is easy to imagine a lessor conditioning the use of the car on continued employment.

3. Lawful Ransomware: Changing Contractual Terms

Ransomware is a kind of digital extortion: malware infiltrates a network, encrypts data, and demands payment in return for decryption and access to the data.[122] Ransomware attacks can be devastating: in early 2017, a variant of the WannaCry ransomware "crippled 200,000 computers in more than 150 countries."[123] It "forc[ed] Britain's public health system to send patients away, [froze] computers at Russia's Interior Ministry and [wrought] havoc on tens of thousands of computers elsewhere."[124] Despite the fact that most IoT devices' poor cybersecurity renders it vulnerable to ransomware attacks, IoT-focused ransomware has generally not been

---

[118] Christopher Elliott, *Business Travel; Some Rental Cars Are Keeping Tabs on the Drivers*, N.Y. TIMES, Jan. 13, 2004, http://www.nytimes.com/2004/01/13/business/business-travel-some-rental-cars-are-keeping-tabs-on-the-drivers.html?_r=0 (noting that "[t]he industry views telematics as a way to enforce its contracts").

[119] Corkery & Silver-Greenberg, *supra* note 1.

[120] *Id.*

[121] *Id.*

[122] Kim Zetter, *What Is Ransomware? A Guide to the Global Cyberattack's Scary Method*, WIRED (May 14, 2017, 1:00 PM), https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/.

[123] Russell Goldman, *What We Know and Don't Know About the International Cyberattack*, N.Y. TIMES (May 12, 2017), https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html?mcubz=0.

[124] Nicole Perlroth & David E. Sanger, *Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool*, N.Y. TIMES (May 12, 2017), https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html?mcubz=0.

viewed as a significant issue. An infected device can be easily rebooted, which eliminates the malware and thereby restores the device's functionality and access to cloud-stored data.[125]

But what if the entity holding your IoT device's functionality hostage is the cloud-based service provider itself? IoT companies can exploit consumers' need for connectivity and updates by conditioning needed updates on consent to new contractual terms in a manner that mirrors a ransomware attack. Should an owner object to new contractual terms, her only recourse may be to forego using the device or its associated services entirely.[126] For example, Sonos, a smart speaker company, recently announced that if customers refuse to agree to changes to the privacy and data collection policy that allow Sonos speakers to collect, use, and share their personal data, Sonos would not provide necessary software updates.[127] As a company spokesperson stated: "The customer can choose to acknowledge the policy, or can accept that over time their product may cease to function."[128]

While increased surveillance capabilities and the ongoing opportunities to modify their contracts will encourage companies to include previously unimaginable terms, the possibility of technological self-help allows companies to enforce them.

B. Privatized Perfect Enforcement

IoT devices combine the built-in ex ante enforcement of regulation by architecture and the automated ex post enforcement of regulation through technological self-help. The law of the firm prevails, with little opportunity for state oversight.

1. Architectural Enforcement: Ex Ante Regulation by Law of the Machine

Larry Lessig famously delineated four "modalities of regulation": law, social norms, markets, and architecture.[129] Lessig's insight was to highlight

---

[125] Ben Dickson, *The IoT Ransomware Threat is More Serious Than You Think*, IOT SECURITY FOUNDATION (Aug. 22, 2016), https://www.iotsecurityfoundation.org/the-iot-ransomware-threat-is-more-serious-than-you-think/ (arguing that it is the timing of ransomware attacks, rather than their irreversibility, that will render IoT ransomware effective).

[126] *See, e.g.*, *Terms of Service*, NEST, https://nest.com/nz/legal/eula/ ("You consent to this automatic update. If you do not want such Updates, your remedy is to terminate your Account and stop using the Services and the Product.").

[127] Whittaker, *supra* note 20.

[128] *Id.*

[129] LAWRENCE LESSIG, CODE VERSION 2.0 123 (2006).

that "code is law." Just as physical architecture constrains what we can do in the physical space and thereby regulates our actions, code regulates our actions in cyberspace.[130] In physical space, a locked door constrains one's ability to access a home; in cyberspace, passwords determine who can access protected data. An IoT device marries the two: now, Amazon Key, an internet-connected lock, will allow you (or Amazon) to unlock your door remotely.

Architectural regulation has a number of distinct traits. Unlike law, social norms, and markets—which are enforced by state actors, social actors, and market actors, respectively—architecture is self-executing.[131] A locked door doesn't exercise discretion, forgiveness, or understanding; it remains implacable and impassable regardless of exigencies of someone's need for access or sanctuary.[132] In the digital space, Digital Rights Management (DRM) technologies control the use, modification, and distribution of copyrighted works without any human enforcer. DRM prevents you from freely lending an Amazon e-book to friends, copying iTunes music onto a portable music player of your choice, or backing up a copy of a CD or DVD. Architectural enforcement is incontrovertible, inarguable, and self-sustaining.

Nor can you break down the digital walls. "Jailbreaking" devices—altering software or hardware that limits their use—at best voids warranties and at worst can carry fines or even criminal charges. The Digital Millennium Copyright Act (DMCA) criminalizes the creation or use of technologies that can disable DRM systems.[133] And, unsurprisingly, IoT companies are fighting those pushing for "right to repair" or "freedom to tinker" exceptions.[134]

---

[130] *Id.* at 124 ("The software and hardware that make cyberspace what it is constitute a set of constraints on how you can behave.").

[131] *Id.* at 342.

[132] *Id.* at 343 (contrasting architectural regulation with "[l]aw, norms, and the market[, which are] are constraints checked by judgement."); Christina Mulligan, *Perfect Enforcement of Law: When to Limit and When to Use Technology*, 14 RICH. J.L. & TECH. 13, 31 (2008) ("Any technology which prevents law breaking before the fact . . . risks creating harm by failing to allow for situations where law breaking is necessary.").

[133] 17 U.S. Code § 1201 – Circumvention of Copyright Protection Systems.

[134] American farmers, for example, are buying black market Ukrainian software to be able to repair broken tractors without having to go to John Deere dealerships, as is required by the John Deere license agreement. Jason Koebler, *Farmers Are Hacking Their Tractors with Ukrainian Firmware*, MOTHERBOARD, Mar. 21, 2017, https://motherboard.vice.com/en_us/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware. Right to repair advocates are pushing for legislation that would invalidate such agreements; unsurprisingly, John Deere is one of the strongest opponents. *Id.*; *see also* David Grossman, *"Right to Repair" is About a Whole Lot More Than iPhones*, POPULAR MECH., Feb. 16, 2017,

The self-enforcing nature of architectural regulation has a number of implications. Most relevantly for this paper, it enables perfect prevention,[135] or what Jonathan Zittrain has referred to as preemption.[136] A user cannot engage in an efficient breach: there is simply no possibility of taking action that doesn't comport with the terms of use.[137] For example, if you lose a physical key, you can call a locksmith and access your home or car; if you lose access to a digital key, you are out of luck. Architectural regulation is not resource-dependent, and it can be scaled along with the spread of the new technology, with little regard to its utility or justness.[138] Furthermore, architectural regulation can easily become entrenched. While laws, norms, and markets constrain "only when some person or group chooses to do so," "architectural constraints have their effect until someone stops them."[139]

The self-executing nature of architectural regulation significantly empowers the architect, as the entity that makes design choices now also has enforcement capabilities. In the case of new technologies, the architects are often private companies who exploit these design features to explicitly or surreptitiously control the use of their products to lock-in consumers; Apple, Google, and Amazon products don't play well with others. Various industry "ecosystems" don't arise organically due only to consumer

---

https://www.popularmechanics.com/technology/infrastructure/a25246/right-to-repair-legislation-under-fire-in-nebraska/ (noting that Apple is also fighting the proposed legislation). For a theoretical defense of these proposed laws, see Pamela Samuelson, *Freedom to Tinker*, 17 THEORETICAL INQ. L. 563 (2016).

[135] Mulligan, *surpa* note 132 (observing that there are three types of "perfect enforcement": perfect prevention, perfect surveillance, and perfect correction).

[136] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 103-17 (2008). Zittrain argues that, even with the idealized version of democratic and representative law creation, no law is ever perfect enough at the moment of its enactment to deserve perfect enforcement. Instead, all laws presume some level of non-compliance, due to misunderstanding, variants on the necessity defense, and non-prosecution—but preemption eliminates these needed sources of flexibility in legal enforcement.

[137] Similarly, in the criminal law context, there would be no possibility of taking unlawful action, even if one might have a justifiable defense.

[138] LESSIG, *supra* note 129, at 343 ("[T]o the extent we can bring about effects through the automatic constraints of real-space code, we need not depend on the continued agency, loyalty, or reliability of individuals. If we can make the machine do it, we can be that much more confident that the unseemly will be done.").

There is a growing literature considering due process and accountability problems raised by algorithmic decision-making. *See, e.g.*, Solon Barocas et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633 (2017); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016); Danielle Keats Citron, *Technological Due Process*, 85 WASH. U.L. REV. 1249 (2008); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predications*, 89 WASH. L. REV. 1 (2014); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predicative Privacy Harms*, 55 B.C. L. REV. 93 (2014);

[139] LESSIG, *supra* note 129, at 343.

preference for a certain company's products and services; they are intentional consequences of self-propagating architecture.

Granted, ham-fisted attempts to limit consumer choice through architectural regulation sometimes backfire, resulting in consumer outcry and flight. And human beings can sometimes be wonderfully clever at evading architectural constraints.[140] More often, however, architectural regulation goes unnoticed, largely because it can be relatively invisible. We are aware that laws are passed, that social norms change from community to community, and that prices are set. But regulation by architecture can be more insidious.[141] After 1948, communities built highways, railroad tracks, and zoning constraints to preserve segregated communities, enabling "what would clearly be an illegal and controversial regulation without even having to admit any regulation exists."[142] While the effects of these architectural decisions are still felt today, it is easy to forget that this segregation was constructed: instead, "[t]he continuing segregation of these communities is described as the product of 'choice.'"[143]

Finally, because ex ante regulatory decisions are hidden, and because human beings have a tendency to blame the individual most immediately involved in an accident that is partially caused by a robotic system,[144] architectural regulation can shift responsibility for the effects of the regulation from the entity who made the design choices to the affected individuals.[145] Consider the narrative of autonomous vehicle accidents. At the time of this writing, increasingly autonomous vehicles have been involved in a number of fender benders. Most recently, a driverless shuttle

---

[140] Newer Keruig coffee machines won't operate with non-Keurig coffee pods—but it didn't take long for someone to post a video of how to fool the device into accepting off-brand pods. Jennifer Abel, *Here's a Super-Easy Way to Get Around Keurig 2.0 DRM Restrictions*, CONSUMER AFF., Dec. 12, 2014, https://www.consumeraffairs.com/news/heres-a-super-easy-way-to-get-around-keurig-20-drm-restrictions-121214.html. Of course, this same ingenuity can be directed towards more nefarious ends.

[141] Of course, it can also be obvious, as anyone who has had speedbumps installed on a familiar route can attest.

[142] LESSIG, *supra* note 129, at 135.

[143] *Id*.

[144] *See* Ryan Calo, *Robots in American Law* (manuscript) (observing that judges have a tendency to attribute liability to the person "in the loop" over a robotic system); Madeleine Elish, *Moral Crumple Zones: Cautionary Tales in Human Robot Interaction*, Proc. We Robot 2016, Apr. 1, 2016 (highlighting how "the human in a highly complex and automated systems may become simply a component—accidentally or intentionally-that bears the brunt of the moral and legal responsibilities when the overall system malfunctions"), at 3-4.

[145] LESSIG, *supra* note 129, at 135.

bus was involved in a crash less than an hour into its first deployment.[146] This article is characteristic of how these accidents are described:

> A driverless shuttle bus being tested in Law Vegas was involved in a crash an hour into its first day on the job – although it wasn't the vehicle's fault. . . .
>
> The incident is the latest in a series of crashes involving driverless vehicles, the vast majority of which have been caused by the other vehicle's driver.
>
> Almost all the incidents recorded by Waymo, Google's autonomous vehicle arm, have been down to human drivers hitting the vehicles, and a major crash involving Uber's driverless cars in March was down to the driver of the other car. . . .
>
> "We were like 'oh my gosh, it's gonna hit us, it's gonna hit us!' and then, it hit us!" one of the passengers told local station KSNV. "The shuttle didn't have the ability to move back, either. [It] just stayed still."
>
> A spokesman for the City of Las Vegas said: "The shuttle did what it was supposed to do, in that [its] sensors registered the truck and the shuttle stopped to avoid the accident.
>
> "Unfortunately the delivery truck did not stop and grazed the front fender of the shuttle. Had the truck had the same sensing equipment that the shuttle has the accident would have been avoided."[147]

Rather than blame the designers who did not address this likely scenario or the company who sold the shuttle before these bugs were addressed, the common narrative is to blame other the other driver—in this case, the third-party operator of a delivery truck that wasn't equipped with the same sensors as the new and experimental autonomous vehicle. Because the design choices are invisible, architectural regulation enables regulators to avoid and misdirect responsibility.[148]

---

[146] James Titcomb, *Driverless Car Involved in Crash in First Hour of First Day*, THE DAILY TELEGRAPH, Nov. 9, 2017, http://www.telegraph.co.uk/technology/2017/11/09/driverless-car-involved-crash-first-hour-first-day/.

[147] *Id*.

[148] Similarly, using highways, railroad tracks, and zoning constraints allowed governments to preserve segregated communities and thereby enable "what would clearly be an illegal and controversial regulation without even having to admit any regulation exists." LESSIG, *supra* note 129, at 135.

2. Digital Repossession: Ex Post Regulation through Technological Self-Help

Historically, a company attempting to repossess an item after an alleged breach of contract would have two options: engage in self-help or involve the state.[149] Given the risk of physical violence that accompanied self-help repossession, courts developed a common law standard that self-help would only found it permissible if it could be achieved without breaching the peace.[150] If the holder of the disputed property protested its removal or kept the property in a locked building, the would-be reclaimant was obligated to involve the state, as "[o]nly the state could enter a private home or office against the owner's will, and then only within the limits established by the due process principles."[151] This common law prohibition on creating a "breach of the peace" was incorporated into U.C.C. articles 9 and 2A.[152] Even where a contract explicitly permits creditors to enter private dwellings for the purposes of repossession, courts have read the "breach of the peace" exception into the contract.[153] Similarly, many states prohibit landlords from engaging in self-help to repossess a disputed property, while those that permit self-help do so subject to a "breach of the peace" standard.[154]

Today, an IoT company has a third option when there is a contractual dispute or identified violation of terms: instead of attempting to physically retrieve an item, the company can remotely deactivate or discontinue service for the device, rendering it "dumb" or completely useless. In other words, the company can effectively repossess an item through digital means without trespassing or otherwise risking violence, avoiding breaches of the peace. This approach raises a number of concerns, chief among them the increased risk of physical harm for consumers, the invasiveness of the action, and the high chance of biased or abusive enforcement.

a. An Increased Risk of Physical Harm

As discussed above, the physicality of IoT devices means that they are able to affect the physical world, and by extension, cause or increase the risk of property damage and physical harm—especially when they do not

[149] As the name implies, "self-help" consists of private actions taken by parties to a controversy, either to prevent or resolve a dispute, without the involvement of a government actor or disinterested third party. Celia R. Raylor, *Self-Help in Contract Law: An Exploration and Proposal*, 33 WAKE FOREST L. REV. 839, 841 (1998).

[150] Cohen, *supra* note 31, at 1103.

[151] *Id.* at 1103.

[152] U.C.C. § 2A-525 (1990); U.C.C. §9-503 (1972).

[153] Cohen, *supra* note 31, at 1104 & n.51.

[154] *Id.* at 1104 n.49.

operate as expected. A deactivated IoT aquarium could result in the loss of expensive fish.[155] Baby monitors and senior lifelines permit parents of sick children and children of ailing parents to sleep soundly—but misplaced reliance on alert systems could lead to tragedy.[156] Smart fridges are marketed as being able to protect you from food spoliation, but a digitally repossessed one might increase your chances of food poisoning. If, as Ryan Calo quipped, robots are "software that can touch you,"[157] IoT devices are contracts that can hurt you.

b. Invasiveness

Nor is a higher risk of property damage or physical harm the only issue here. As Julie Cohen has observed, "Plainly, the nonviolent nature of electronic self-help—not to mention electronic 'regulation' of performance—does not negate its invasiveness from the consumer's perspective."[158] She imagines a high-tech repro team, with the ability to "beam" a contested sofa out of a living room, and argues that it would be difficult to claim that no intrusion had occurred.[159]

A company's ability to digitally repossess or remotely alter an item is not very different from Cohen's imagined invasive "beaming" it out: in both cases, the consumer can no longer make use of the item. And this is already occurring. In addition to examples discussed above, in accordance with their terms of service IoT companies are using software and security updates to alter how an IoT device functions without informing the user of those alterations. Nest requires users to consent to automatic "patches, bug fixes, updates, upgrades, and other modifications," purportedly "to improve

---

[155] Not only are IoT acquirums and monitors already widespread, one has been hacked in the attempt to acquire data from a casino. Alex Schiffer, *How a Fish Tank Helped Hack a Casino*, WASH. POST, Jul. 21, 2017, https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/?utm_term=.d5caa6cf64b8.

[156] *See, e.g.*, Ed Harding, *Foxborough Family Says Home Medical Alert System Failed Loved One*, WCVB, Aug. 27, 2014, http://www.wcvb.com/article/foxborough-family-says-home-medical-alert-system-failed-loved-one/8207243. Similarly, IoT fire alarms, carbon monoxide sensors, and motion-activated security cameras are only useful to the extent they're functional—a non-operable one actually increases risk.

[157] Ryan Calo, *The Case for a Federal Robotics Commission*, BROOKINGS (Sept. 2014).

[158] *Id.* at 1105; *see also id.* at 1102 ("Courts . . . have not explained, because they have not needed to, whether the judicially-developed 'breach of the peace' standard is *only* designed to minimize the likelihood of physical violence and harm to person and property, or is (or should be) more broadly concerned with preventing nonconsensual intrusion . . . .").

[159] *Id.* at 1105.

the performance of the Product Software and related services."[160] Nokia required its smart scale users to accept a software update that disabled one of the device's key features.[161] Apple is now facing a number of domestic and international lawsuits from consumers alleging that its software updates—which Apple has admitted slow down older iPhones with aging batteries—were designed to promote new phone sales.[162]

c. Biased and Abusive Enforcement

Because self-helpers judge the righteousness of their own cause, "[t]here is ample reason to worry that they will misconstrue the law along the way—not just, or even primarily, on account of band faith, but on account of motivated cognition and reliance on congenial interpretive methods or theories of law."[163] Biased enforcement is even more problematic when the relevant law is a contract drafted by that same entity.

Furthermore, self-helpers might also act in bad faith, especially in the absence of state oversight. In April 2017, an individual who purchased Garadget—an internet-connected garage door opener—reported problems and left an angry comment on the Garadget community board, followed by a one-star review on Amazon.[164] Denis Grisak, the inventor and distributor of Garadget, responded by denying the unit server connection.[165] Because the device had never been activated, the Garadget purchaser was not at risk of being locked out of his garage or having his garage door left permanently open—but another customer who had activated the device and then annoyed the company might have been.[166]

***

IoT devices allow companies to exploit the benefits of regulation by architecture and regulation by machine, with all of the opportunities for

---

[160] *Terms of Service*, NEST, https://nest.com/nz/legal/eula/.

[161] Daniel Cooper, *Nokia Will Disable the Key Feature of Its Priciest Scale*, ENDGAGET, Jan. 22, 2018, https://www.engadget.com/2018/01/22/nokia-disables-pulse-wave-velocity-body-cardio/.

[162] Steve Mullis, *Lawsuits Mount As Apple Manages Fallout From Revelation of Slowed iPhones*, NPR.ORG, Dec. 31, 2017, https://www.npr.org/2017/12/31/574792184/lawsuits-mount-as-apple-manages-fallout-from-revelation-of-slowed-iphones.

[163] David E. Pozen, *Self-Help and the Separation of Powers*, 124 YALE L. J. 2, 50 (2014).

[164] Gallagher, *supra* note 21.

[165] *Id.*

[166] *Id.*

overreach and abuse inherent to both. While this has long occurred with digital technology companies, it has more serious implications in the IoT context, however, discontinued service or digital repossession can increase the likelihood of property damage and physical harm.

This is hardly the first time new technology has altered relations between industry and individuals. As discussed in the next Part, tort law's history is studded with examples of legal shifts intended to address new harmful conduct; to address the new sources of harms raised by IoT devices, we may need another such legal change.

III. THE NEXT TORT LAW REVOLUTION

We are at the inflection point of the next tort law revolution. As a product that is both an object and an ongoing service, IoT devices create a new relationship between companies and consumers—and this new relationship empowers companies in ways that increase consumers' risks of property damage and physical harms, but that are not adequately addressed by current tort law doctrine. As with prior, technological-enabled relational shifts, the proliferation of IoT devices will necessitate a reconsideration of what duties industries owe to individuals who will be foreseeably harmed by their actions. After reviewing other, technologically-fostered historic shifts in tort law, this Part considers how existing law might evolve to hold companies accountable.

A. Historic Shifts in Tort Law

The history of tort law is punctuated with situations where new technologies alter relationships between industry and individuals, demanding the creation of expanded duties of care or new understandings of causation to address new, technologically-enabled conduct and harms. The concept of ultrahazardous activities, the creation of no-fault workers' compensation and motor vehicle insurance, the rise of mass tort litigation—all of these legal developments can be partially traced to underlying technological changes and accompanying social shifts.

This section considers two of the more momentous examples of technologically-enabled shifts in tort law, both of which dramatically expanded liability by creating more expansive duties of care and by acknowledging the validity of more attenuated causation analyses: the evolution of the conception of negligence and the products liability revolution.

1. Negligence: From a Duty to One to a Duty to the World

Personal injury claims were rare in pre-industrial America,[167] and when a case was brought, it was evaluated under something akin to a strict liability standard.[168] To the extent pre-industrial cases mention "negligence," the term usually entails a defendant's failure to fulfill a specific duty toward a specific other, such as a duty of a shopkeeper to deliver a purchased item in good condition.[169]

The Industrial Revolution—and the advent of machines with "a marvelous capacity for smashing the human body"—changed everything.[170] Locomotives, automobiles, steamboats, and factory and mining machines created "an accident crisis like none the world had ever seen."[171] Additionally, for the first time in history, the majority of these serious accidents were impersonal, "stranger" cases. Instead of being harmed by a family member, neighbor, or other known person, now people were being mangled by machines whose owners they didn't know, complicating the duty analysis. Simultaneously, a host of social and legal shifts made bringing personal injury suits easier and more appealing.[172]

As more and more personal injury suits were brought, courts began changing the standard under which claims were evaluated.[173] The modern

---

[167] Donald G. Gifford, *Technological Triggers to Tort Revolutions: Steam Locomotives, Autonomous Vehicles, and Accident Compensation*, 11 J. TORT LAW (forthcoming 2018), at 11-14 (discussing reasons).

[168] MORTON J. HORWITZ, THE TRANSFORMATION OF AMERICAN LAW, 1780-1860, at 85 (1977).

[169] *See, e.g.*, *id.* at 86-88; WHITE, *supra* note 27, at 15 ("Prior to the 1830s, with the exception of a handful of cases in New York, the term 'negligence' generally referred to 'neglect' or failure to perform a specific duty imposed by contract, statute, or common law.").

[170] LAWRENCE M. FRIEDMAN, A HISTORY OF AMERICAN LAW 467 (1985, 2d ed.).

[171] John Fabian Witt, *Toward a New History of American Accident Law: Classical Tort Law and the Cooperative First-Party Insurance Movement*, 114 HARV. L. REV. 690, 694 (2001).

[172] These included the emergence of deep-pocketed corporations, Gifford, *supra* note 167, at 20-21; the creation and expansion of liability insurance, *id.* at 21-22; the general abolition of the witness disqualification rule (which prohibited individuals with an interest in the outcome of a case—including the plaintiff—from testifying), *id.* at 22-23; *see also* Witt, *supra* note 171, at 753-54 (describing the history of the witness disqualification rule); and the appearance of a personal injury bar, Gifford, *supra* note 167, at 23-24.

[173] Edward White explicitly traces the development of modern negligence to the explosion in "stranger" cases, arguing that courts had to develop a new standard to address the new relationship between injurer and injured. WHITE, *supra* note 27, at 16 ("[T]he modern negligence principle in tort law seems to have been an intellectual response to the increased number of accidents involving persons who had no preexisting relationship with one another . . . ."). Other scholars have posited different explanations for this shift in liability standards. Morton Horwitz and Lawrence Friedman claim that the law evolved in

American conception of negligence was born: whereas once it had been sufficient to show that the defendant caused an injury, plaintiffs now needed to also demonstrate that the defendant had not acted with reasonable due care. This shift in what constitutes "negligence" is often described as a contraction of defendant liability,[174] as it is far more difficult to prove that a duty of care was breached than that an act caused an injury.[175] However, it can also be understood as an expansion of liability: No longer can one only be held liable for a specific duty owed in a particular kind of relationship; now, one has "a more general duty potentially owed to all the world."[176]

2. The Products Liability Revolution

Just as the rise of stranger cases spurred the development of the modern conception of negligence, under which we now owe a duty of care to the world, the rise of mass manufacturing and new transportation systems spurred the development of products liability law, under which manufacturers now owe a duty of care to anyone who might be harmed by their products.

Historically, consumer protections for product-caused harms were based on privity of contract: only those party to a contract of sale could bring suit

---

recognition of a need to protect fledging industries, namely factories, mines, and railroads. HORWITZ, *supra* note 168, at XX; FRIEDMAN, *supra* note 170, at 468; *see also* Gary T. Schwartz, *Tort Law and the Economy in Nineteenth-Century America: A Reinterpretation*, 90 YALE L.J. 1717, 1717 (1981) (describing this as the "prevailing view" and arguing that the shift to negligence was far less dramatic and intentional than Howitz's description). John Fabian Witt suggests that the emergence of a fault-based liability system can be traced to the influence of "nineteenth-century political liberalism." Witt, *supra* note 171, at 45-49. Donald Gifford attributes the rise of the modern negligence liability standard directly to the new technology and the harms and social practices it enabled. Gifford, *supra* note 167.

Medical malpractice underwent a similar shift during this time period, as judges restated the obligations of physicians towards patients. Sir William Blackstone's 1768 *Commentaries on the Laws of England* characterized malpractice as a private wrong that occurred when a patient was harmed by "the neglect or unskillful management of his physician." Allen D. Spiegel & Florence Kavaler, *America's First Malpractice Crisis, 1835-1865*, J. CMTY. HEALTH 283, 286 (1997). By the end of the nineteenth century, American judges were requiring physicians to possess a certain amount of skill and knowledge to provide treatment, to employ a reasonable standard of care, and to apply common medical knowledge in their practice. *Id.* at 289.

[174] *See, e.g.*, HORWITZ, *supra* note 168, at 99-100 (describing the legal change as providing "substantial subsidies for those who undertook schemes of economic development").

[175] Jules L. Coleman, *The Structure of Tort Law*, 97 YALE L.J. 1233, 1235 (1988) ("Under strict liability, the costs of faultless accidents fall on injurers; under negligence, they fall on victims.").

[176] Brown v. Kendall, 60 Mass. 292 (Mass. 1850); WHITE, *supra* note 27, at 16.

for harms caused by an object. As remote mass production created an increasingly attenuated relationship between the manufacturer and ultimate consumer, however, courts began to hold companies liable for the harms their products caused. In *MacPherson v. Buick Motor Co.*, Judge Cardozo argued that manufacturers of products that could "place life and limb in peril when negligently made" owed a duty of care to the world to anticipate and prevent likely harms.[177] Over time, products liability law and developed to address the legal gap created due to the increasingly attenuated relationship between the manufacturer and the ultimate consumer or others affected by the products.[178]

The Industrial Revolution and the associated rise of "stranger cases" prompted courts to expand the definition of negligence; the rise of mass production and sprawling transportation systems helped spur the products liability revolution. Given how IoT devices change the relationship between industries and individuals, a similar expansion in liability will likely accompany the expansion of the IoT ecosystem.[179]

B. Potential Tort Law Solutions

This section considers different potential ways in which current tort law concepts could evolve to hold companies accountable for the foreseeable harms associated with remotely altering or digitally repossessing IoT devices.

1. Service Defects

Because IoT devices are products, it is natural to first look to products liability law to address their associated problems. Certainly, much of

---

[177] MacPherson v. Buick Motor Co., 111 N.E. 1050, 1053 (N.Y. 1916); Jack M. Balkin, *The Three Laws of Robotics in the Age of Big Data*, 78 OHIO STATE L.J. (forthcoming 2018) at 28 (stating that *MacPherson* "abolished the privity rule and held that manufacturers had public duties, not only to direct consumers who purchased the products from intermediaries, but also duties to their family members and to bystanders who were injured by defective products").

[178] *See, e.g.*, Escola v. Coca Cola Bottling Co. of Fresno, 150 P.2d 436, 443 (Cal. 1944) (Traynor, J., concurring) ("As handicrafts have been replaced by mass production . . . the close relationship between the producer and consumer of a product has been altered. Manufacturing processes . . . and ordinarily either inaccessible to or beyond the ken of the general public.").

[179] To be sure, this will hardly be the only way in which new conduct enabled by IoT devices impacts tort law. IoT devices increasing the likelihood of a host of harms: their ability to collect personal data raises privacy harm concerns; their poor cybersecurity increases the risk of criminals accessing data or using IoT devices in DDOS attacks on businesses, governments, or critical internet infrastructure.

existing products liability law could easily be applied to IoT devices. When harm is caused as the result of a design defect, manufacturing defect, or inadequate warning,[180] it can be addressed through products liability law. When such harm is caused by a hacker, we can debate whether the harm should lie where it falls or be considered a kind of design defect or breach of implied warranty.[181] But what about when a company intentionally discontinues service for an IoT device, either in response to a contractual breach or as outright punishment? For products liability law to be applicable, we may need to develop a new category of products liability cases grounded in defective service.

As discussed above, products liability law developed in the context of a changed relationship between companies and consumers. Modern types of products liability claims—design defects, manufacturing defects, and marketing defects—can be understood as identifying different kinds of relationships between consumers and different entities in the products supply chain, where each different actor has a differing standard of liability for kinds of caused harm. Design defects exist when a product is inherently dangerous or useless, either because it fails to meet consumer expectations regarding safe products or the risks associated with its use outweigh the benefits. Manufacturing defects happen in the manufacturing process, often due to poor-quality materials or workmanship. Marketing defects—which are also known as failures to warn—occur when a product has a nonobvious risk that could be lessened by an adequate warning. Manufacturing defect cases tend to apply a strict liability standard; design and warning defect cases usually apply some variant of a negligence analysis.[182]

Some of the harms potentially caused by IoT devices result not from a failure of the physical device, but rather because a service that a consumer has come to depend upon is no longer provided. Accordingly, it might make sense to delineate "service defects" as a fourth kind of products liability claim, with compensatory and specific performance remedies.[183] A

---

[180] Indeed, a failure to provide adequate notice concerning remotely-made modifications to a product might be considered a warning defect.

[181] *See* Butler, *supra* note 30; Elvy, *supra* note 30, at 85.

[182] *See* Gifford, *supra* note CC, at 53-54.

[183] While courts have historically been reluctant to require specific performance of personal services, the underlying rationales are less applicable in the IoT context. Granted, not only is it difficult as an administrative matter to evaluate how well a service is performed, orders limiting personal freedoms implicate involuntary servitude. However, both rationales against requiring specific performance are inapplicable in this context. First, unlike the construction of a building or an employment contract, the services IoT companies provide are roughly fungible: the app used by one consumer is the same app used by another, even though their data may be particularized. Second, assuming that an IoT company offers these services to multiple customers, requiring performance for a specific individual hardly implicates the liberty interests of either the company or its

company could be required to provide written notice of the possibility of self-help enforcement in its initial contract,[184] and it could install all manner of warnings to notify the device's user of missed payments or other contractual violations that trigger the possibility of self-help. Alternatively, as already occurs with physical repossession, companies could be required to engage the state to ensure a certain amount of due process before digitally repossessing a device.

2. IoT Fiduciaries

Alternatively, rather than focusing on the product aspect of the IoT, we can instead focus on the service element and look to tort law categories focused on regulating service relationships. This section first considers the relevance of the concept of "information fiduciaries," then argues for developing IoT-specific fiduciary duties.

a. Information Fiduciaries

Tort law has long premised certain duties—particularly regarding the sharing of personal information—on particular, legally-defined relationships. In general, doctors cannot disclose patients' health data; therapists cannot share what is discussed in confidence[185]; accountants' and attorneys' communications with their clients are confidential. Were members of any of these professions to use their clients' information to enrich themselves at their clients' expense, they would be liable in tort,

---

employees. Alan Schwartz, *The Case for Specific Performance*, 89 YALE L.J. 271, 297 (1979) ("[R]equiring a sizable corporation that renders services to perform for a given promise does not violate the corporation's associational interests or the associational interests of its employees."). The case would be somewhat different if the IoT company was closing that portion of its business; in that situation, requiring specific performance would be unreasonable.

[184] Already, "existing law requires written notice of the possibility of electronic self-help" and "[e]very court that has considered a challenge to electronic self-help repossession of licensed software has indicated that in view of its drastic nature, electronic self-help requires prior contractual authorization." Cohen, *supra* note 31, at 1112. Cohen highlights that none of the cases concerning electronic self-help involved a non-negotiated, boilerplate or click-wrap contract, so these courts did not address whether notice in such a click-wrap contract—the kind that usually accompanies IoT devices—would be sufficient. *Id.*

[185] Excepting when their patient physically threatens another individual. *E.g.* Tarasoff v. Regents of the University of California, 17 Cal. 3d 425, 551 P.2d 334, 131 Cal. Rptr. 14 (Cal. 1976).

either for a breach of a duty of professional obligation or for professional malpractice.[186]

Doctors, therapists, accountants, and lawyers are all fiduciaries, entities who have a "position of superiority or influence, acquired by virtue of [a] special trust."[187] A fiduciary relationship is often recognized as existing when "one party, the beneficiary, is especially vulnerable and dependent upon another party, the fiduciary, who is expected to loyally employ specialized knowledge, skills, and power over some aspect of the beneficiary's affairs to further the beneficiary's interests."[188]

Jack Balkin has proposed recognizing entities "who, because of their relationship with another, [have] taken on special duties with respect to the information they obtain in the course of the relationship."[189] He argues that, "[b]ecause of their special power over others and their special relationships to others, information fiduciaries have special duties to act in ways that do not harm the interests of the people whose information they collect, analyze, use, sell, and distribute."[190] Under this definition, IoT companies would also be information fiduciaries. As Balkin stated: "Although we may come to trust the home robot and the smart house—indeed, we have to—the entity that we really have to trust is not the robot or the house. It is the company behind the robot and the house that collects the data from the robot and from the house's sensors. And that company, I argue, should be an information fiduciary."[191]

If applied to IoT companies, the concept of information fiduciaries could address many of the issues raised above. Companies would not be able to use data gathered by IoT devices to enrich themselves at the expense of device users, to identify violations of contractual terms, or to report certain categories of illegal activity to law enforcement.

However, the concept of information fiduciary is inherently limited, as it focuses on information-related harms. Recognizing that IoT companies are information fiduciaries hardly addresses the range of harms they may cause by virtue of their new relationship with IoT device users. To do that, we need to think more broadly about what duties IoT companies might owe consumers.

---

[186] Jack M. Balkin, *Information Fiduciaries and the First Amendment*, U.C. DAVIS L. REV. 1183, 1205 & n.105 (2016).

[187] Tornado Techs., Inc. v. Quality Control Inspection, Inc., 977 N.E.2d 122, 126 (Ohio Ct. App. 2012).

[188] Thomas L. Hafemeister & Joshua Hinckley Porter, *Don't Let Go of the Rope: Reducing Readmissions by Recognizing Hospitals' Fiduciary Duties to Their Discharged Patients*, 62 AM. U. L. REV. 513, 545-46 (2013).

[189] Balkin, *Information Fiduciaries*, *supra* note 186, at 1209.

[190] *Id.* at 1186.

[191] Balkin, *Three Laws*, *supra* note 177, at 25.

b. IoT-Specific Fiduciary Duties

While IoT companies are information fiduciaries, they might also be recognized as having a separate, categorical fiduciary relationship with IoT device users, with associated duties that reflect the nature of the services they provide and their unique ability to cause harm.[192]

The main duty could be characterized as a duty of loyalty. Like other fiduciaries, IoT companies could be required to act in the interests of the IoT device user. Again, they would not be able to use data gathered by IoT devices to enrich themselves at the expense of device users, to identify violations of contractual terms, or to report certain categories of illegal activity to law enforcement. But the duty of loyalty in this context could also extend to not terminating service for an IoT device absent adequate warning or not altering how a device operates without sufficient notice.

Relatedly, IoT companies could have a duty not to overreach in their contracts. This duty could be extrapolated from *Williams v. Walker Thomas Furniture*, which implied that companies owed a duty of good faith to their consumers.[193] In *Williams*, plaintiffs purchased household items on boilerplate installment contracts, which provided that "all payments . . . shall be credited pro rata on all outstanding leases, bills and accounts due the Company by [purchaser] at the time each such payment is made."[194] As a result, the defendant kept a balance on each item purchased under installment, so that if the plaintiff ever defaulted on a payment, the defendant would be able to repossess each item regardless of how much had been paid off. The appellate court found that the district court had not adequately considered whether the contract was unconscionable because it did not adequately provide the buyer with an opportunity for meaningful choice in light of the "gross inequality of bargaining power" and remanded.[195] While *Williams* is taught as a contracts case, it implies that companies have a tort-like duty not to overreach in their contractual terms, especially when consumers have limited choice in negotiating those terms.

In the IoT context, a duty not to overreach would prohibit companies from including overly invasive contractual terms, holding IoT devices

---

[192] Doctors, for example, are information fiduciaries, but the duty not to share patient data is but one of many duties doctors owe their patients: they must possess a certain amount of knowledge and skill to provide treatment, they must take care in diagnosis and deciding what treatment is appropriate, they must obtain informed consent to treatment, and they must act with care in the administration of that treatment. Similarly, IoT companies might be considered to owe a variety of duties to IoT device users.

[193] 350 F.2d 445 (D.C. Cir. 1965).

[194] *Id.* at 447.

[195] *Id.* at 449-50.

hostage by conditioning their continued utility on acceptance of different terms, and prohibiting companies from discontinuing service or engaging in digital repossession absent some form of due process or sufficient notice. While unlikely to be adopted, a broad duty against overreach might even require companies not to use architectural regulation to create "walled gardens"—closed software systems, like Amazon's Kindle eReaders, which don't allow consumers to read their purchased ebooks on other devices—or to condition all warranties on not jailbreaking a device.

IoT companies would also have a duty of care; specifically, a duty not to foreseeably cause harm to their consumers by discontinuing service, remotely altering a device, or otherwise engaging in digital repossession.

Granted, disabling devices will usually increase the likelihood of harm, rather than being a direct cause of harm. A disabled front door lock on a home won't hurt the occupant—but it increases the likelihood that an occupant will be burglarized or assaulted; a car that stops working at a stoplight increases the likelihood that the driver will be injured as she attempts to leave the intersection. Accordingly, IoT companies will likely argue that the intervening event will break the chain of causation linking their (possibly negligent) action to the consumers' harm.[196]

However, the fact that there may be an intervening cause of harm does not imply that all resulting harm is necessarily unforeseeable. In *Posecai v. Wal-Mart Stores*, a plaintiff brought suit after being robbed in the parking lot of Sam's Club (which is owned by Wal-Mart Stores).[197] She alleged that Wal-Mart was negligent for failing to provide adequate security in its parking lot, given that the store was located in a high crime area. The Supreme Court of Louisiana "join[ed] other states in adopting the rule that although business owners are not the insurers of their patrons' safety, they do have a duty to implement reasonable measures to protect their patrons from criminal acts when those acts are foreseeable. . . . This duty only arises under limited circumstances, when the criminal act in question was reasonably foreseeable to the owner of the business."[198] Further, courts must use a balancing test to determine the appropriate duty of care: "The

---

[196] The tort law concept of "intervening" or "superseding" causes developed to address situations where something unforeseeable occurs and thereby breaks the chain of causation. In *Stahlecker v. Ford Motor Company*, for example, a woman's car failed in a remote area, and the woman was raped and murdered. 266 Neb. 601, 667 N.W.2d 244 (2003). Her parents sued the car company on her behalf, on the grounds that the car's inoperability had caused their daughter's death. The court dismissed the case, reasoning that the murderer's actions were "independent and intervening" and that the car company "had no reason to expect intentional tortious or criminal acts by a third person" and so were not liable for the harm caused. *Id.*

[197] 752 So. 2d 762 (La. 1999).

[198] *Id.* at 766.

greater the foreseeability and gravity of the harm, the greater the duty of care that will be imposed on the business."[199]

A similar balancing test, that weighs both the foreseeability of harm and its likely gravity, would be useful in the IoT context. An inoperative Fitbit will not cause much harm; an inoperative Nest might; an inoperative pacemaker almost certainly will.

CONCLUSION

As IoT devices proliferate, cloud-based service providers are increasingly able to create and impose their own contractual and architectural governance regimes. They can use terms of service to displace the law of the state, and they can employ regulation by architecture and technological self-help to enforce those terms. Furthermore, the physicality of IoT devices increases the likelihood of consumer property damage and physical harm when companies discontinue service or otherwise engage in digital repossession.

Because IoT devices are both a product and an ongoing service, they alter the nature of the relationship between industry and individuals. Consumers are increasingly dependent on companies' continued provision of services for their devices' continued functioning, while companies have a newfound power to engage in unmonitored overreach and even abusive practices. While the resulting harms are not new, the causation analysis is. This paper considers the social, technological, and legal aspects of this changed relationship and explores how products liability and fiduciary legal regimes might evolve to hold companies accountable when their actions increase the risk of consumer harm.

---

[199] *Id.* at 768. Although the *Posecai* court did not find plaintiff's harm foreseeable, and while many courts have been wary of extending it, most reiterate the standard and some have relied on *Posecai* to find questions of fact regarding whether business owners might have reasonably foreseen harms from third parties. Patton v. Strogen, 908 So.2d 1282 (La. 2005); Williams v. Louisiana, 786 So.2d 927 (La. 2001).