THE INTERNET OF TORTS: EXPANDING CIVIL LIABILITY STANDARDS TO ADDRESS CORPORATE REMOTE INTERFERENCE

REBECCA CROOTOF†

ABSTRACT

Thanks to the proliferation of internet-connected devices that constitute the "Internet of Things" ("IoT"), companies can now remotely and automatically alter or deactivate household items. In addition to empowering industry at the expense of individuals, this remote interference can cause property damage and bodily injury when an otherwise operational car, alarm system, or implanted medical device abruptly ceases to function.

Even as the potential for harm escalates, contract and tort law work in tandem to shield IoT companies from liability. Exculpatory clauses limit civil remedies, IoT devices' bundled object/service nature thwarts implied warranty claims, and contractual notice of remote interference precludes common law tort suits. Meanwhile, absent a better understanding of how IoT-enabled injuries operate and propagate, judges are likely to apply products liability and negligence standards narrowly, in ways that curtail corporate liability.

---

† Assistant Professor of Law, University of Richmond School of Law; Affiliated Fellow, Information Society Project. I am extraordinarily grateful to BJ Ard and Jack Balkin for a running conversation about the interaction between law and technology, which informs this entire piece. This paper has been much improved by feedback from Douglas Bernstein, Molly Brady, Kiel Brennan-Marquez, Lea Brilmayer, Ryan Calo, Jud Campbell, Danielle Citron, Arica Crootof, Michael Froomkin, Kristelia Garcia, Jim Gibson, Sue Glueck, Samantha Godwin, David Grewal, Nik Guggenberger, Woody Hartzog, Oona Hathaway, Claudia Haupt, Erik Hovenkamp, Elizabeth Joh, Margot Kaminski, Sonia Katyal, Doug Kysar, Mark Lemley, Aaron Perzanowski, Jennifer Rothman, Rory Van Loo, George Wang, and Andrew Woods. My thanks also to participants in Data & Society's workshop, the Center for Applied Cybersecurity Research speaker series, the ISP Fellows Writing Workshop, and We Robot 2018 for helpful commentary on early drafts; to law faculty at Drexel, Maryland, Richmond, Penn State University Park, Seton Hall, UCLA, UC Davis, the University of Southern California, UC Irvine, and UNC for incisive and clarifying questions; to Sasha Dudding, Nathan Leys, Wendy Serra, and Shili Shao for creative research assistance; and to Farrah Bara, Taylor Brennan, Daniel Lautzenheiser, Grace Ramirez, Alex Tate, Nicole Wittstein, and other members of the *Duke Law Journal* for their close reads and thoughtful editing suggestions.

But this is hardly the first time a new technology has altered social and power relations between industries and individuals, creating a potential liability inflection point. As before, we must decide what to incentivize and who to protect, with an awareness that the choices we make now will shape future assumptions about IoT companies' obligations and consumer rights. Accordingly, this Article proposes reforms to contract and tort law to expand corporate liability and minimize foreseeable consumer injury.

TABLE OF CONTENTS

INTRODUCTION

Missing a payment on your leased car was once the first step of an extended, multistage negotiation between you and a lender, bounded by enforcement costs, contract law, and consumer protection rules.[1] Today, however, car companies are using starter-interrupt devices to remotely "boot" cars just days after a payment is missed.[2] This self-help practice is currently lawful and provides significant cost savings to businesses, but it creates an obvious risk of injury when an otherwise operational car does not work as expected. There have been reports of parents unable to take children to the emergency room, individuals marooned in dangerous neighborhoods, and people whose cars were disabled while idling in an intersection.[3]

This is but one of many examples of how internet-connected devices, collectively referred to as the "Internet of Things" ("IoT"), allow companies to engage in remote interference—the practice of employing an over-the-air update to remotely alter or deactivate a physical device. After identifying this contractually legitimized vector for harm and discussing why our current civil liability regime is ill-suited to regulate it, this Article proposes legal reforms to expand corporate liability and minimize foreseeable user injury. Enacting

1. Usually, the practical difficulties and costs associated with repossession result in lenders waiting to take action until after two or more consecutive missed monthly payments. Some states require creditors to give notice before repossessing a car, *see, e.g.*, FLA. STAT. § 537.012(2) (2017), MASS. GEN. LAWS ch. 255B, § 20A(c) (2017); others grant car lessors in default the right to reinstate their loans or otherwise cure the default, *see, e.g.*, MASS. GEN. LAWS ch. 255B, § 20A(c) (2017), ME. STAT. tit. 9-A, § 5-110 (2017). While many states permit lenders to repossess a car a day after a loan default, they are constrained by an obligation to not breach the peace. *See, e.g.*, GA. CODE ANN. § 11-9-609 (2017); N.J. STAT. ANN. § 12A:9-609 (2013).

2. *See* Michael Corkery & Jessica Silver-Greenberg, *Miss a Payment? Good Luck Moving That Car*, N.Y. TIMES (Sept. 24, 2014, 9:33 PM), https://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car [https://perma.cc/2YF4-EHZB] (describing a lender who "remotely activated a device . . . that prevented [a lessor's] car from starting").

3. *Id.*

these suggestions will foster a powerful regulatory and social-norms feedback loop, shaping our future assumptions about IoT companies' obligations and consumer rights.

Thanks to recent technological advances, it is increasingly easy to add sensors and wireless capabilities into more and more items, allowing companies to transform innumerable once-"dumb" items into "smart" IoT devices.[4] As this Article is concerned with the issue of consumer physical harm, it focuses on IoT devices intended for individual and household use. These include both relatively independent gadgets—like an implantable medical device, wearable step tracker, smart appliance, or vehicle—and integration systems—like a smart-home hub that networks lights, entertainment, and environmental controls.[5]

The ongoing connection between these devices and IoT companies[6] allows for corporate remote interference, which can benefit both industry and individuals: over-the-air updates can address bugs, protect against discovered malware, correct cyber vulnerabilities, enable new capabilities,[7] or even save lives.[8] The ability to remotely alter IoT devices also reduces industry costs of complying with

4. This bent has sparked Twitter feeds like @internetofshit, which catalogs excessively connected products, including IoT doghouses, coffee mugs, sex toys, jean jackets, condoms, and fidget spinners. *See generally* Internet of Shit (@internetofshit), TWITTER, https://twitter.com/internetofshit?lang=en [https://perma.cc/JFJ6-3RYZ].

5. The full Internet of Things includes implantables, devices, vehicles, building and logistical systems, and other physical items with sensors, software, and network connectivity that enable data collection and sharing.

6. While acknowledging that it will not always be accurate or appropriate to lump different entities together, this Article uses "IoT companies" as shorthand that includes IoT device manufacturers, distributers, and cloud-based service providers.

7. Tesla, for example, anticipates using software updates to gradually improve cars' self-driving capabilities. *See generally* Sheikh v. Tesla, No. 17-CV-02193-BLF, 2018 WL 5794532 (N.D. Cal. Nov. 2, 2018) (upholding the settlement agreement in a class action lawsuit against Tesla for its delayed rollout of Enhanced Autopilot features).

8. In response to a May 2018 Consumer Reports' allegation that Tesla Model 3's stopping distance was worse than any other contemporary car, Tesla pushed an over-the-air software update that improved the car's braking distance by nineteen feet, undoubtedly saving lives. Sean O'Kane, *Tesla Can Change So Much with Over-the-Air Updates That It's Messing with Some Owners' Heads*, VERGE (June 2, 2018), https://www.theverge.com/2018/6/2/17413732/tesla-over-the-air-software-updates-brakes [https://perma.cc/5XGX-A9HV]; *see also* 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 [https://perma.cc/7DN8-2H4D].

changing regulations,[9] monitoring compliance with terms and conditions, and enforcing consequences for contractual breaches.[10] Companies may pass these savings on to consumers in the form of cheaper products or a greater willingness to extend credit to riskier borrowers.[11] For example, the ability to remotely boot a car reduces the need for physical repossessions, minimizing the potential for embarrassment, trespass, or breaches of the peace and the attendant physical risks to repossession agents, consumers, and bystanders.[12]

The benefits of corporate remote interference are widely touted, but the drawbacks are less obvious. Some scholars and commentators are detailing how connected items create consumer-privacy issues and underappreciated economic harms,[13] and others are discussing how IoT devices' malfunctions or weak cybersecurity create an increased risk of

9. This, in turn, makes it easier to regulate internet-connected devices, as Jonathan Zittrain predicted a decade ago. JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 103 (2008).

10. *E.g.*, Corkery & Silver-Greenberg, *supra* note 2.

11. Starter-interrupt devices, for example, enable high-risk borrowers to qualify for cars they might not otherwise have been able to lease. *See id.*

12. Granted, consumers might experience remote interference as far more invasive than traditional repossessions. In many states, repossession agents cannot trespass on private property, even to retrieve secured collateral. Remote interference permits a company to "reach inside" an individual's home to alter household devices. As Professor Julie Cohen has observed while discussing industry interference with digital files, "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." Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089, 1105 (1998); *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 persons and property, or is (or should be) more broadly concerned with preventing nonconsensual intrusion . . . ."). As a hypothetical, she imagines a high-tech repo team with the ability to "beam" a contested item out of a living room and argues that it would be difficult to claim that no intrusion had occurred. *Id.* at 1106. An IoT company's ability to remotely interfere with an item is akin to Cohen's imagined invasive "beaming" it out: in both cases, the consumer can no longer make use of a purchased item in their home.

13. *See generally, e.g.*, 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); Margot E. Kaminski, Matthew Rueben, William D. Smart & Cindy M. Grimm, *Averting Robot Eyes*, 76 MD. L. REV. 983, 984 (2017); Christina Mulligan, *Personal Property Servitudes on the Internet of Things*, 50 GA. L. REV. 1121, 1163–65 (2016) [hereinafter Mulligan, *Personal Property Servitudes*]; Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85 (2014); Richard L. Rutledge, Aaron K. Massey, Annie I. Antón & Peter Swire, Clarifying the Internet of Things by Defining the Internet of Devices (2010) (unpublished manuscript), https://peterswire.net/wp-content/uploads/Clarifying-the-Internet-of-Things-by-Defining-the-Internet-of-Devices.pdf [https://perma.cc/L4NR-88NA].

physical harm.[14] These topics deserve attention—not least because standing rules and the economic-loss doctrine bar many suits that would otherwise result in liability for IoT companies—but the focus on privacy, cybersecurity, and criminal hacks has obscured the increased risk of physical harm from nonaccidental corporate acts.

This is the first law review article to discuss how the benefits of unconstrained corporate remote interference may come at the expense of consumers' physical safety.[15] Because IoT devices interact with and affect our physical environment, corporate remote interference can foreseeably cause physical harm. Your oven turning on unexpectedly

14. *See, e.g.*, BENJAMIN C. DEAN, CENTER FOR DEMOCRACY & TECHNOLOGY, STRICT PRODUCTS LIABILITY AND THE INTERNET OF THINGS 1 (2018) (discussing how insecure IoT devices may enable new vectors for physical harms); FEDERAL TRADE COMMISSION, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 12 (2015) [hereinafter FTC REPORT] ("[U]nauthorized persons might exploit security vulnerabilities to create risks to physical safety in some cases."); U.S. CHAMBER INSTITUTE FOR LEGAL REFORM, TORTS OF THE FUTURE: ADDRESSING THE LIABILITY AND REGULATORY IMPLICATIONS OF EMERGING TECHNOLOGIES 42–43 (2017); Sara Sun Beale & Peter Berris, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, 16 DUKE L. & TECH. REV. 161, 163–66 (2018) (describing instances where IoT devices or systems have been hacked or could be hacked to cause physical and financial harm, including hacks into the healthcare system, automated railways, smart automobiles, aviation technology, and dams); Butler, *supra* note 13; Stacy-Ann Elvy, *Hybrid Transactions and the INTERNET of Things: Goods, Services, or Software*?, 74 WASH. & LEE L. REV. 77, 118 (2017); Charlotte A. Tschider, *Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age*, 96 DENVER L. REV. 87, 109 (2018); *see also* Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1909–12 (2019) (discussing how IoT household devices can be hijacked by domestic abusers, creating a new avenue for invasion of sexual privacy).

15. Of course, harmful remote interference is far from the only issue associated with the growing IoT ecosystem. Recent scholarship has highlighted IoT devices' extensive cybersecurity problems. *See, e.g.*, Bruce Schneier, *Security and the Internet of Things*, SCHNEIER ON SECURITY (Feb. 1, 2017, 8:24 AM), https://www.schneier.com/blog/archives/2017/02/security_and_th.html [https://perma.cc/BET8-UXXA] (stating that, because "[a]ll computers are hackable," we "need to reverse the trend to connect everything to the internet"). Others have highlighted the IoT's attendant national security and international security risks. *See generally* Laura DeNardis & Mark Raymond, *The Internet of Things as a Global Policy Frontier*, 51 U.C. DAVIS L. REV. 475 (2017) (discussing global policy concerns); Ido Kilovaty, *Freedom To Hack*, 80 OHIO STATE L.J. 455 (2019) (proposing legal remedies to address IoT security concerns). Scholars have also raised concerns about how the IoT enables expanded law enforcement and industry surveillance, *see, e.g.*, ZITTRAIN, *supra* note 9, at 109–10; Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 812 (2016); 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. VA. L. REV. 891, 907–11 (2017), and increases opportunities for surreptitious consumer manipulation, *see, e.g.*, Ryan Calo, *Tiny Salespeople: Mediated Transactions and the Internet of Things*, 2013 IEEE SECURITY & PRIVACY 70, 70 (2013). *See generally* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014) (detailing how collected information can be used to manipulate consumer choice).

increases the risk of a house fire;[16] your car turning off unexpectedly increases the risk that you will be stranded in a dangerous area.[17] You trust an IoT baby monitor, senior lifeline, home-security system, or fire alarm to notify you of a problem—but should a software update disable the alert system without warning, your reliance could lead to tragedy.[18] Your garage or front door could be left open, inviting theft or assault, in retaliation for a bad review of a smart lock on Amazon.[19] And implantable IoT medical devices—like pacemakers and insulin pumps—make the physical risks of remote deactivation all the more visceral.[20]

In short, this technology increases consumer risk without a corresponding increase in corporate liability. Given how IoT devices increasingly affect our environment and bodies, the potential magnitude and kinds of harm from corporate remote interference are significant; given that the digital nature of the IoT enables relatively costless and automated action, the potential scale of these harms is staggering. Meanwhile, IoT companies are creating, monitoring, and enforcing contractual-governance regimes with few legal incentives to ensure foreseeable harms are avoided. Finally, absent a better understanding of how IoT-enabled injuries operate and propagate, judges will likely apply products liability and negligence standards in ways that minimize corporate liability. Thus, the actual harm individual consumers experience is familiar—after all, repossessed cars have never been able to take children to emergency rooms, and

16. Ashley Carman, *Smart Ovens Have Been Turning on Overnight and Preheating to 400 Degrees*, VERGE (Aug. 14, 2019, 2:54 PM), https://www.theverge.com/2019/8/14/20802774/june-smart-oven-remote-preheat-update-user-error [https://perma.cc/ZE2Z-ASUW].

17. Stephen Ellison, *Tesla's App Goes Down for Hours, Leaving Some Stranded*, NBC (Sept. 2, 2019, 8:41 PM), https://www.nbcbayarea.com/news/local/Teslas-App-Goes-Down-For-Hours-Leaving-Some-Stranded-559215411.html [https://perma.cc/7RMS-4GR7].

18. *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 [https://perma.cc/UMJ6-GUDE] (reporting that a woman, wearing a medical alert system designed to automatically sense and report falls, fell without an alert being issued and later died of unknown causes).

19. *See infra* notes 104–06 and accompanying text (discussing how the owner and distributer of an IoT garage-door opener responded to a poor Amazon review by deactivating the customer's device).

20. *See, e.g.*, 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 341–43 (Ian Kerr, Valerie Steeves & Carole Lucock eds., 2009). *See generally* Scott J. Shackelford, Michael Mattioli, Steve Myers & Austin Brady, *Securing the Internet of Healthcare*, 19 MINN. J.L. SCI. & TECH. 405, 407 (2018) (discussing the cybersecurity and privacy "vulnerabilities replete in the supply chain for medical devices").

malfunctioning alert systems or medical devices have long caused injuries. But our current civil liability system is ill-equipped to address this new vector for harm. To correct this imbalance, this Article proposes expanding liability for harms resulting from corporate remote interference.

Part I introduces IoT devices and discusses how these internet-connected objects foster a new ongoing and intimate relationship between IoT companies and users, characterized both by an increased power differential and an increased risk of harm.[21] Companies can harness IoT devices' extensive surveillance capabilities[22] to monitor consumer compliance with contractual terms—written by and for the company[23]—and employ strategic remote interference to extort concessions and engage in self-help enforcement.[24] Critically, and in contrast to prior forms of electronic self-help, corporate remote interference with IoT devices can cause property and bodily harm. If, as Ryan Calo has quipped, robots are "software that can touch you,"[25] IoT devices are contracts that can hurt you.

Part II discusses how contract and tort law work in tandem to shield companies from liability for the harms caused by their remote interference.[26] Unsophisticated consumers agree to nonnegotiated

---

21. *See* Elvy, *supra* note 14, at 91–93 (describing the new type of continuous and asymmetric relationship between IoT companies and their customers). This relationship is further complicated by the fact that devices are increasingly licensed, rather than sold. For considerations of the various social and legal implications of increasingly licensed items, see generally JOSHUA A.T. FAIRFIELD, OWNED: PROPERTY, PRIVACY AND THE NEW DIGITAL SERFDOM (2017); AARON PERZANOWSKI & JASON SCHULTZ, THE END OF OWNERSHIP: PERSONAL PROPERTY IN THE DIGITAL ECONOMY (2016); Christina Mulligan, *Licenses and the Property/Contract Interface*, 93 IND. L.J. 1073 (2018); Mulligan, *Personal Property Servitudes*, *supra* note 13; Molly Shaffer Van Houweling, *The New Servitudes*, 96 GEO. L.J. 885 (2008).

22. *See, e.g.*, 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 [https://perma.cc/H7WV-HDZH].

23. *See infra* Part I.A.1 (discussing how GPS trackers are being used to determine if rental and leased cars are driven outside of permitted areas).

24. *See infra* Part I.A.3 (recounting how remote interference enables corporate self-help).

25. RYAN CALO, BROOKINGS, THE CASE FOR A FEDERAL ROBOTICS COMMISSION 5 (2014).

26. Contracts, intellectual property, and cyberlaw scholars have mapped out issues raised when companies use terms of service and technological self-help to sidestep consumer protections in the digital context. *See generally, e.g.*, MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2012) [hereinafter RADIN, BOILERPLATE]; Cohen, *supra* note 12, at 1103; Margaret Jane Radin, *Regulation by Contract, Regulation by Machine*, 160 J. INST. THEO. ECON. 143 (2004) [hereinafter Radin, *Regulation by Contract*]. This Article builds on this scholarship in describing how IoT devices increase both companies' ability to surveil consumers and the risk of physical harm.

terms of service, which notify them of the possibility of remote interference and purport to limit corporate liability for its consequences.[27] Even if a court determines that a liability-limiting clause is invalid as unconscionable or contrary to public policy, IoT devices' bundled goods/services nature thwart breach of warranty claims,[28] while the contractual notification precludes other common law tort suits.[29] Meanwhile, none of the products liability standards map well onto these situations, and the duty analysis for a negligence claim is confused by tempting but misleading analogies. Further, for both products liability and negligence actions, the causal chain may appear tenuous. Not only can corporate remote interference facilitate accidental and criminal intervening sources of harm, it also shifts responsibility to those intervening sources.[30] This allows companies to evade the reputational costs that might otherwise attend dramatic injuries resulting from remote interference, limiting the market's ability to address this problem—indeed, if anything, it encourages a market for lemons.[31] In short, remote interference has foreseeable, harmful consequences, but our current civil liability regime is unlikely to hold IoT companies sufficiently accountable.

But, as discussed in Part III, law can evolve. Civil liability standards regularly change in the wake of technological development, new sources of harm, and attendant shifts in power and social relations.[32] The proliferation of IoT devices heralds another possible

27. *See infra* Part II.A.1 (providing examples of IoT exculpatory clauses).

28. *See infra* Part II.A.2 (explaining why U.C.C. implied warranties will not attach to many IoT devices).

29. *See infra* Part II.A.3 (arguing that notification will bar trespass to chattels and conversion claims).

30. *See infra* Part II.D.2 (discussing how autonomous-vehicle accidents are often attributed to others involved in the accidents, rather than to the companies who fielded a vehicle that cannot engage in actions that would be expected of a human driver).

31. *See generally* George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488 (1970) (arguing that "good" products are crowded out by "bad" ones when consumers cannot distinguish between high- and low-quality (or safe and unsafe) versions).

32. Tort law scholars and legal historians regularly discuss the social and legal impacts of new technologies; this Article continues that tradition with a focus on the relational and power shifts facilitated by IoT devices. *See generally* LAWRENCE M. FRIEDMAN, A HISTORY OF AMERICAN LAW (2d ed. 1985); MORTON J. HORWITZ, THE TRANSFORMATION OF AMERICAN LAW, 1780-1860 (1977); G. EDWARD WHITE, TORT LAW IN AMERICA: AN INTELLECTUAL HISTORY (1980); P.H. WINFIELD, A TEXTBOOK OF THE LAW OF TORT (5th ed. 1950); JOHN FABIAN WITT, THE ACCIDENTAL REPUBLIC: CRIPPLED WORKINGMEN, DESTITUTE WIDOWS, AND THE REMAKING OF AMERICAN LAW (2004) [hereinafter WITT, ACCIDENTAL REPUBLIC]; Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the*

liability inflection point,[33] the outcome of which will determine our future basic assumptions about IoT companies' obligations and consumer rights. In one potential timeline, consumers will continue to bear the brunt of harms resulting from corporate remote interference, and consumer expectations regarding corporate duties—or lack thereof—will develop accordingly. In another, preferable future, liability will be allocated in a more balanced way, and consumers will reasonably expect companies to take steps to prevent foreseeable harms.

Part III concludes by outlining various routes toward expanding corporate liability for harms resulting from remote interference. In some situations, it may be sufficient to adopt more expansive understandings of existing tech-neutral doctrine; in others, it may be clarifying to articulate tech-specific rules. This Article discusses the relative benefits of strengthening the unconscionability and public policy doctrines to limit the reach of exculpatory clauses; recognizing broader relational duties, which might take the form of a new implied warranty, a new products liability claim, or a new informal fiduciary duty; and extending proximate cause standards.[34] It closes with a

Dawn of the Information Age, 80 S. CAL. L. REV. 241 (2007); Donald G. Gifford, *Technological Triggers to Tort Revolutions: Steam Locomotives, Autonomous Vehicles, and Accident Compensation*, 11 J. TORT L. 71, 123–29 (2018); Kyle Graham, *Of Frightened Horses and Autonomous Vehicles: Tort Law and Its Assimilation of Innovations*, 52 SANTA CLARA L. REV. 1241 (2012); 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 (2001) [hereinafter Witt, *Toward a New History*].

33. Professor Douglas Kysar has discussed how new technologies and social facts may spur the development of new liability theories:

> Just as railroad and workplace carnage forced recognition of new forms of risk in the latter half of the nineteenth century, just as automobile and product-caused accidents illuminated extended chains of responsibility in the twentieth century, climate change will challenge prevailing conceptions of wrongdoing in the twenty-first century.

Douglas A. Kysar, *What Climate Change Can Do About Tort Law*, 41 ENVTL. L. 1, 6 (2011). Similarly, the changed corporation–consumer relationship enabled by IoT devices may justify an expanded liability analysis.

34. In doing so, this Article contributes to a growing body of scholarship on how increasingly connected, automated, and even autonomous systems challenge or alter liability standards. *See generally, e.g.*, Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513 (2015); Rebecca Crootof, *International Cybertorts: Expanding State Accountability in Cyberspace*, 103 CORNELL L. REV. 565 (2018); Rebecca Crootof, *War Torts: Accountability for Autonomous Weapons*, 164 U. PA. L. REV. 1347 (2016); Mark A. Geistfeld, *A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation*, 105 CALIF. L. REV. 1611 (2017); F. Patrick Hubbard, *"Sophisticated Robots": Balancing Liability, Regulating, and Innovation*, 66 FLA. L. REV. 1803, 1839–43 (2014); Curtis E. A. Karnow, *The Application of Traditional Tort Theory to Embodied Machine Intelligence*, *in* ROBOT LAW 51 (Ryan Calo, A. Michael Froomkin & Ian Kerr eds., 2016); Gary E. Marchant & Rachel A. Lindor, *The Coming*

discussion of how courts, legislatures, and agencies at both the state and federal levels can complement each other in implementing these recommendations.

Calibrated correctly, our civil liability regime can evolve to preserve the benefits of remote interference and ensure that IoT companies are incentivized to better protect consumers.

I. A NEW CORPORATION–CONSUMER RELATIONSHIP

While there is no agreed-upon definition for the "Internet of Things,"[35] everyone can agree there are a lot of them. And the already mind-boggling number of internet-connected devices is expected to skyrocket as companies slap sensors and wireless capabilities onto more and more items. 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 twenty-five to fifty billion such devices.[36] Others predict that there will be more than one trillion IoT devices by 2025.[37] As this Article considers the problem of consumer harm, it focuses on the millions of IoT devices marketed for individual or household use rather than public or industrial IoT systems, such as smart city or

Collision Between Autonomous Vehicles and the Liability System, 52 SANTA CLARA L. REV. 1321 (2012); Bryant Walker Smith, *Automated Driving and Product Liability*, 2017 MICH. ST. L. REV. 1 (2017) [hereinafter Smith, *Automated Driving*]; Bryant Walker Smith, *Proximity Driven Liability*, 102 GEO. L.J. 1777 (2014) [hereinafter Smith, *Proximity Driven Liability*]; David C. Vladeck, *Machines Without Principals: Liability Rules and Artificial Intelligence*, 89 WASH. L. REV. 117 (2014); William D. Smart, Cindy M. Grimm & Woodrow Hartzog, An Education Theory of Fault for Autonomous Systems (Aug. 29, 2017) (unpublished manuscript), http://people.oregonstate.edu/~smartw/library/papers/2017/werobot2017.pdf [https://perma.cc/G56E-AHNJ].

35. A Federal Trade Commission ("FTC") report describes the IoT 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." FTC REPORT, *supra* note 14, at 6. A McKinsey report defined it as "sensors and actuators connected by networks to computing systems . . . . exclud[ing] systems in which all of the sensors' primary purpose is to receive intentional human input." MCKINSEY GLOBAL INSTITUTE, THE INTERNET OF THINGS: MAPPING THE VALUE BEYOND THE HYPE 1 (2015) [hereinafter MCKINSEY REPORT]. Delightfully, some have described IoT devices as "enchanted objects"—"ordinary things made extraordinary." DAVID ROSE, ENCHANTED OBJECTS: DESIGN, HUMAN DESIRE, AND THE INTERNET OF THINGS 7 (2014).

36. MCKINSEY REPORT, *supra* note 35, at 17.

37. Bill Wasik, *In the Programmable World, All Our Objects Will Act as One*, WIRED (May 14, 2013), https://www.wired.com/2013/05/internet-of-things-2 [https://perma.cc/UG4T-RXV7].

factory logistical, monitoring, or maintenance systems.[38] This subset of IoT devices represents a significant percentage of the IoT ecosystem: it is estimated to have an economic impact of $370 billion to $1.9 trillion per year by 2025.[39]

An IoT device's distinctive fusion of traits—its ability to collect personal data, its capacity for ongoing communication with an IoT company, and its physicality—combine to form a product that is simultaneously an object and a service.[40] An IoT speaker might double as a smart-home hub or link with a voice-activated, cloud-based service to provide requested content. A smart thermostat develops customized energy-saving heating plans and a monthly energy report. An internet-connected vehicle offers built-in navigation, roadside assistance, or real-time alerts regarding engine, emission, or airbag status. Water bottles can track your daily water intake, egg monitors can send reminders that eggs are going bad, and tires can alert you if they become deflated.[41] Medical wearables and implantables allow for

38. This Article regularly refers to Nest, Google's smart-home hub, GOOGLE NEST, https://store.google.com/us/category/connected_home?hl=en-US&GoogleNest&utm_source=nest_redirect&utm_medium=google_oo&utm_campaign=GS102776&utm_term=control [https://perma.cc/EDW5-5KJQ]; Alexa Voice Service, Amazon's cloud-based voice service that links with innumerable devices, *Alexa Voice Service*, AMAZON ALEXA, https://developer.amazon.com/alexa-voice-service [https://perma.cc/S86P-G6TD]; and Tesla, an automotive and energy car company that specializes in increasingly autonomous vehicles, TESLA, https://www.tesla.com [https://perma.cc/8UWB-N5TN].

39. MCKINSEY REPORT, *supra* note 35, at 7.

40. Elvy, *supra* note 14, at 144–45 (describing how the IoT has "usher[ed] in an era" of devices that are both services and goods, and no longer "static objects"). 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 Grandstrand, ed., 2003) [hereinafter Radin, *Information Tangibility*]. You no longer simply buys a phone: you buy 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").

41. Note that, despite being about IoT devices, this paper does not use "a fridge ordering milk" as an example. At least, not anymore. Pzremek Palka, *How To Write a Law and Technology Paper?*, PRZEMYSLAW.TECHNOLOGY (Nov. 30, 2018), https://przemyslaw.technology/2018/11/30/how-to-write-a-law-and-technology-paper [https://perma.cc/PF2X-YCT2].

better drug management and the early identification of a need for intervention.[42]

As a result, and as detailed more fully below, when you engage with an IoT device, you do more than just use an item; you enter into an ongoing and surprisingly intimate relationship with an IoT company, characterized by a new power dynamic—and a new risk of property and bodily harm.

A. An Exacerbated Power Imbalance

New technologies giveth, and new technologies taketh away. But while it is increasingly understood that IoT-enabled services come at the cost of one's privacy, it is less recognized that they also come at the cost of one's agency.[43]

IoT devices' touted provision of individualized services requires individualized data gathering, which in turn enables individualized manipulation and individualized enforcement via corporate remote interference.[44] Not only can IoT companies use software and hardware to limit how consumers can use a device,[45] but they can also monitor compliance with their terms of service, which allows them to strategically time remote interference to extort concessions or engage

---

42. *See generally* Syagnik Banerjee, Thomas A. Hemphill & Phil Longstreet, *Is IOT a Threat to Consumer Consent? The Perils of Wearable Devices' Health Data Exposure* (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038872 [https://perma.cc/2WGG-FKE7].

43. Numerous scholars are exploring the implications of increased surveillance for privacy law and consumer protection law. *See supra* notes 13–15. *See generally* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1904 (2013). This Article is primarily concerned with how IoT companies are leveraging their surveillance capabilities to exert more control over consumers.

44. *See infra* Part I.A.3 (discussing how IoT companies can hold consumer devices hostage to elicit agreement to new contractual terms and engage in individualized remote interference).

45. Scholars have long detailed how design decisions enable corporate control and limit consumer uses. *See, e.g.*, HENRI LEFEBVRE, THE PRODUCTION OF SPACE 224 (Donald Nicholson Smith trans., 1991) (1984) (observing that what is possible within a space depends on what its designers want to permit and encourage); LAWRENCE LESSIG, CODE VERSION 2.0 81–84, 123–37, 323–24, 327–29 (2006) (describing the distinctive characteristics and impacts of architectural regulation, with a focus on computer code); LUCY A. SUCHMAN, HUMAN-MACHINE RECONFIGURATIONS 186–92, 257–84 (2d ed. 2007) (discussing how users' interactions with technologies are structured by their design); Julie E. Cohen, *Cyberspace as/and Space*, 107 COLUM. L. REV. 210, 225–27 (2007) (arguing that the design of online environments constrict users' behavior in much the same way as the design of physical environments); Steve Woolgar, *Configuring the User: The Case of Usability Trials*, *in* A SOCIOLOGY OF MONSTERS: ESSAYS ON POWER, TECHNOLOGY, AND DOMINATION 59, 67–69 (John Law ed., 1991) (noting how technological designs limit users' activities).

in self-help. Indeed, given their new powers to monitor, companies may include previously unthinkable, stringent rules into their contracts, further directing when and how consumers can use their purchased devices.

Between contracts replacing "the law of the state with the 'law' of the firm"[46] and new technology enabling the law of the surveilling firm, corporate remote interference systematically empowers IoT companies at the expense of IoT-device users.[47]

1. *Intensified Corporate-Compliance Monitoring*. Companies have always been able to glean information about their customers from interactions, but IoT devices are collecting, crunching, and conveying individualized data on an entirely new scale. They amass a wealth of aggregate and individually linked data about the most private aspects of our lives,[48] granting IoT companies insight into our routines, habits, and proclivities; household IoT devices gather and share information about when you wake up, how long you brush your teeth, when you

46. Radin, *Regulation by Contract*, *supra* note 26, at 143.

47. *Id.* at 147. Simultaneously, to the extent states co-opt corporate power, internet-connected devices "significantly reduce[] the number and variety of people and institutions required to apply the state's power on a mass scale." ZITTRAIN, *supra* note 9, at 118; *see, e.g.*, Peter Campbell, *Volvo Cars Caps Vehicle Speed To Prevent Road Deaths*, FIN. TIMES (Mar. 4, 2019), https://www.ft.com/content/3c2f66bc-3e61-11e9-9bee-efab61506f44 [https://perma.cc/K3FM-DFFY] (reporting on blanket, GPS-linked electronic speed-limiting and that Volvo is considering using it to cap vehicle speed near schools and hospitals).

48. Furthermore, most IoT devices marketed for individual and home use collect information in the home, a traditionally private space. *See, e.g.*, Ryan Calo, *Robots and Privacy*, *in* ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS 187, 188 (Patrick Lin, George Bekey & Keith Abney eds., 2012).

Certainly, it is technologically possible to have household IoT devices that do not collect individualized information, do not share it with IoT companies, and are not subject to remote corporate control. Konnex, for example, is an open standard used for commercial and domestic building automation that is not linked to an IoT company and does not permit third-party access or control.

Given the value generated by data sets, however, IoT companies have market incentives to collect as much information about their users as possible; given various liability risks, they also have legal incentives to maintain control over the IoT devices. 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. *See, e.g.*, Kashmir Hill, *Nest Hackers Will Offer Tool To Keep the Google-Owned Company from Getting Users' Data*, FORBES (July 16, 2014), https://www.forbes.com/sites/kashmirhill/2014/07/16/nest-hack-privacy-tool/#3b38af583464 [https://perma.cc/W2RC-FVC3] (reporting on how Nests report household information to Google and how the device can be altered to prevent it from sending personal data).

turn your lights on or off, and what shows you watch.[49] Although much of the data is explicitly or implicitly volunteered—after all, individuals choose to wear fitness trackers or install smart-home hubs[50]—data about our lives is increasingly being collected without our knowledge by our own IoT devices,[51] by others' devices,[52] and by public devices.[53] IoT and other data-mining companies generate additional information through data aggregation and extrapolation.[54] Between the amount and kind of data collected, IoT companies now know more personal details about individual device users than the nosiest small-town shopkeeper or the most tech-enabled brick-and-mortar store.[55]

Further, because all IoT devices have transmitters that permit information sharing,[56] they are in regular communication with

49. Hill & Mattu, *supra* note 22. IoT companies may even use gathered 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 [https://perma.cc/SS7V-RYY2].

50. Friedland, *supra* note 15, at 898.

51. Ferguson, *supra* note 15, 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 (Sept. 12, 2016), https://gizmodo.com/smart-sex-toy-maker-sued-for-sneakily-collecting-intima-1786559792 [https://perma.cc/7UVA-WTBF] ("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."); Arvind Narayanan (@random_walker), TWITTER (Sept. 27, 2019, 6:08 AM), https://twitter.com/random_walker/status/1177570679232876544 [https://perma.cc/TZY2-GTJX] (discussing three papers that detail how smart TVs and related devices track users).

52. Ferguson, *supra* note 15, 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.").

53. Meg Leta Jones, *Privacy Without Screens & the Internet of Other People's Things*, 51 IDAHO L. REV. 639, 647 (2015) ("There is no opportunity for notice and choice in smart publics or any smart shared space."); *see also* Siraj Datoo, *This Recycling Bin Is Following You*, QUARTZ (Aug. 8, 2013), https://qz.com/112873/this-recycling-bin-is-following-you [https://perma.cc/AVP8-UVF6] (noting that London's smart garbage bins collect data from pedestrians' smart phones to create targeted advertisements).

54. 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 15, at 822.

55. *See, e.g.*, Paul Michael, *8 Ways Retailers Are Tracking Your Every Move*, TIME (Sept. 23, 2016), http://time.com/money/4506297/how-retailers-track-you [https://perma.cc/Z28J-76MM] (reporting on how stores geofence smartphones to identify when individuals approach, enter, and leave stores).

56. These connectivity structures can take a variety of forms: IoT devices can connect with and transmit data to other devices, to service providers, or to a hub or gateway, which then connects to service providers. David Hamilton, *The Four Internet of Things Connectivity Models Explained*, WEB HOST INDUSTRY REVIEW (Apr. 29, 2016), *available at*

corporate service providers, allowing for real-time monitoring. As detailed in a recent article about a monitored, IoT-connected home, smart-home devices persistently contact outside servers.[57] Amazon's Echo hub connected with company servers every few minutes,[58] and the smart plugs—which merely control and monitor electrical usage—were "pinging home almost every hour."[59] The latest Roomba creates maps of owners' homes, which it then shares with parent companies iRobot and Google.[60] Even seemingly independent IoT devices, like wearable step trackers, pacemakers, and vehicles, frequently exchange information with companies to report on usage and receive security updates.

This near-constant data gathering and transfer enables a new level of postsale corporate surveillance. Previously, most postsale services bundled with the sale of a good tended to be limited to 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 even though subscription plans and utilities are provided on a near-constant basis, consumers' relationships with utility companies are limited. Subscribers and property owners are charged at regular intervals, punctuated with relatively rare as-needed repairs to portions of the system under the company's control. Thus, while "[l]eases, service contracts, loyalty programs, customer marketing, and even end-user license agreements are forms of an ongoing relationship, even with users other than the original buyers,"[61] the IoT corporation–consumer relationships are distinctively intimate and ongoing.

IoT-device-enabled surveillance grants companies a newfound ability to identify violations of once under-enforced or unenforceable contractual terms. For example, car rental companies regularly restrict

---

http://www.inetservicescloud.com/the-four-internet-of-things-connectivity-models-explained [https://perma.cc/ZZY3-C7RG].

57. Hill & Mattu, *supra* note 22.

58. *Id.*

59. *Id.*

60. Maggie Astor, *Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared*, N.Y. TIMES (July 25, 2017), https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html?_r=0 [https://perma.cc/9TZ8-SN9P]; James Vincent, *Google Wants to Improve Your Smart Home with iRobot's Room Maps*, VERGE (Oct. 31, 2008), https://www.theverge.com/2018/10/31/18041876/google-irobot-smart-home-spatial-data-mapping-collaboration [https://perma.cc/SVY8-5LEQ].

61. Smith, *Proximity Driven Liability*, *supra* note 34, at 1804.

out-of-state driving.[62] Absent an incident, however, this rule was often ignored by both the company and consumer, as it was generally unenforceable (if still a useful liability shield for the company in the case of an out-of-state accident). But GPS trackers now allow companies to monitor where and how fast a car is driven. One renter, who anticipated a $259.51 rental bill, had to pay $3405.05 due to a one-dollar-per-mile fine for having crossed state lines;[63] another was charged a $450 fine for three instances of speeding.[64] More recently, a woman's auto loan contract restricted her from driving outside of a four-county perimeter.[65] 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.[66]

IoT companies also market their compliance surveillance to other industries. For example, a smart intercom company's New York City advertising campaign emphasizes that landlords can use their technology to photograph visitors, allowing them to determine if tenants are illegally subletting units—which would then allow them to evict tenants and take steps to circumvent rent-control laws.[67]

IoT companies' newfound ability to engage in individualized surveillance marks a seismic shift in the enforceability of contractual provisions. Indeed, it invites companies to incorporate increasingly stringent and invasive terms into their contracts—precisely because

62. *See, e.g.*, *Fox Rent A Car – Frequently Asked Questions*, FOX RENT A CAR, https://www.foxrentacar.com/en/faqs.html [https://perma.cc/B2SU-LGNF] (providing information regarding the states within which a vehicle may be driven, depending on where it is rented).

63. 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 [https://perma.cc/TA4S-ZUNE] ("The industry views telematics as a way to enforce its contracts . . . .").

64. Catherine Greenman, *The Car Snitched. He Sued.*, N.Y. TIMES (June 28, 2001), https://www.nytimes.com/2001/06/28/technology/the-car-snitched-he-sued.html [https://perma.cc/8PFC-SPY7].

65. Corkery & Silver-Greenberg, *supra* note 2.

66. *Id.*

67. Alfred Ng, *Smart Home Tech Can Help Evict Renters, Surveillance Company Tells Landlords*, CNET (Oct. 25, 2019, 5:00 AM), https://www.cnet.com/news/install-smart-home-tech-evict-renters-surveillance-company-tells-landlords [https://perma.cc/T2BT-9BDR] (reporting that an email advertised, "Use the GateGuard AI Doorman Intercom to catch illegal sublets, non-primaries, Airbnbs, so you can vacate a unit," and "Combine a $950/mo studio and a $1400/mo one-bedroom into a $4200 DEREGULATED two-bedroom").

those terms can now be enforced.[68] Lenders can already monitor when a leased vehicle is at the lessor's place of employment;[69] it is easy to imagine a lender conditioning the use of the car on employment attendance.

2. *Facilitating (Automated) Corporate Remote Interference*. "Remote interference" is the act of altering how an IoT device works at a distance, either by pushing through an over-the-air software update or discontinuing a service. Companies can remotely alter a device's software to add new functions, such as when Tesla pushed an update that helped unfreeze the charge port in cold weather;[70] to remove other functions, as occurred when Nokia required users to accept a software update that disabled a key feature of its smart scales;[71] or to completely deactivate a device or larger system, as when a starter-interrupt device "boots" a leased car.[72] Terminating a service may also constitute remote interference.[73] Without the ability to exchange information with a service provider, an IoT smart-home hub is little more than an unusually expensive paperweight—as users of the Revolv learned to their dismay when the company announced it would be shutting down support for the hub and its associated apps.[74] For other IoT devices, the lack of a service will simply render a once-smart item dumb. In 2016, for example, lighting company TCP stopped hosting a server that enabled their IoT lightbulbs' remote

68. *See, e.g.*, Kristelia A. García, *Technological Rights Accretion*, 36 YALE J. ON REG.: NOTICE & COMMENT (Sept. 19, 2018), http://yalejreg.com/nc/technological-rights-accretion-by-kristelia-a-garcia [https://perma.cc/Y6CX-35AS] (discussing an app that "purports to use blockchain technology to enable visual artists to 'track' art they sell such that if and when it is later resold, they are able to enforce a so-called 'resale royalty,'" a contractual term "that has been repeatedly considered and explicitly rejected by Congress").

69. Corkery & Silver-Greenberg, *supra* note 2 (noting that a lender "typically shuts down cars when they are parked at the borrower's house or workplace").

70. Fred Lambert, *Tesla Releases Software Update To Help Unfreeze Charge Port*, ELECTREK (Dec. 27, 2018), https://electrek.co/2018/12/27/tesla-software-update-unfreeze-charge-port [https://perma.cc/8M8M-GZ6E].

71. Daniel Cooper, *Nokia Will Disable the Key Feature of Its Priciest Scale*, ENGADGET (Jan. 22, 2018), https://www.engadget.com/2018/01/22/nokia-disables-pulse-wave-velocity-body-cardio [https://perma.cc/85CX-TWPJ].

72. Corkery & Silver-Greenberg, *supra* note 2.

73. Elvy, *supra* note 14, at 100 ("[T]he range of operations of an IOT device is very much dependent on the services and software provided by companies.").

74. 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 [https://perma.cc/5TM3-E5EM].

functionality.[75] The bulbs still provide light, but the capabilities that justified their steeper price tag no longer exist.[76] In contrast, for other devices, certain services are relatively superfluous. For example, the termination of a radio streaming service has little impact on a car's overall utility.

An IoT company's right to engage in remote interference is often enshrined in its terms of service.[77] Google Nest smart-home products, for example, require users to consent in advance to automatic "patches, bug fixes, updates, upgrades and other modifications to improve the performance of the Product Software and related services."[78] While the benefits of corporate remote interference are often advertised,[79] it also creates significant and underappreciated negative externalities.

Because IoT devices are digital, automating remote interference is relatively costless. If anything, it may result in cost savings, incentivizing companies to automate. But automating remote interference raises the same concerns that attend any discussion of algorithmic, "perfect" enforcement,[80] including the creation of a

75. Kate Cox, *TCP Disconnects "Smart" Lightbulb Servers, Leaves Buyers in the Dark*, CONSUMERIST (Sept. 26, 2016), https://consumerist.com/2016/08/19/tcp-disconnects-smart-lightbulb-servers-leaves-buyers-in-the-dark [https://perma.cc/TAQ2-JNL8].

76. *Id.*

77. *See, e.g.*, *Alexa Terms of Use*, AMAZON (May 17, 2018) [hereinafter *Alexa Terms*], https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740 [https://perma.cc/3HEL-LTH8] ("We may change, suspend, or discontinue Alexa, or any part of it, at any time without notice."); *Software Updates*, TESLA, https://www.tesla.com/support/software-updates [https://perma.cc/VXX9-PWCL] ("[Tesla] cars regularly receive over-the-air software updates that add new features and enhance existing ones over Wi-Fi. When updates become available, you'll receive a notification on your center touchscreen display, with the option to install the update immediately or schedule for later."); *Terms of Use for Hue*, PHILIPS HUE [hereinafter *Philips Hue Terms*], https://www2.meethue.com/en-us/product-terms [https://perma.cc/A24U-U6E3] ("Signify may update or change software for seamless Services, and may do so remotely without notifying you."); *Uconnect Terms and Conditions*, UCONNECT, ¶ 17 [hereinafter *Uconnect Terms*], https://www.driveuconnect.com/terms-and-conditions.html [https://perma.cc/R9U8-7XMA] ("At any time we may need or be required to update or change the software on your vehicle, and may do so remotely without notifying you. You agree that we may perform these software updates or changes remotely without any further consent required . . . .").

78. *End-User License Agreement*, NEST [hereinafter *Nest License Agreement*], https://nest.com/nz/legal/eula [https://perma.cc/3M6Z-W48Q].

79. *See supra* notes 7–12 and accompanying text.

80. *See generally, e.g.*, Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008) (discussing the drawbacks of automating administrative decision-making); Meg Leta Jones & Karen Levy, Sporting Chances: Robot Referees and the Automation of Enforcement (Nov. 18, 2018) (unpublished manuscript), https://ssrn.com/abstract=3293076 [https://perma.cc/VA7B-UBUD] (extrapolating from the resistance to the use of automated

Kafkaesque bureaucratic enforcement regime.[81] Automated decision-making is self-executing, and therefore incontrovertible, inarguable, and self-sustaining.[82] It minimizes opportunities for efficient breach, mutually beneficial negotiation, and compromise.[83] For example, when the transaction costs associated with repossession were high, lenders often contacted consumers before a repossession to negotiate immediate partial payment or a longer-term loan with a higher interest rate. With automated remote interference, however, company representatives have less incentive to communicate with consumers. Further, no system is error free, but automation locks in and amplifies errors.[84] One individual has alleged that his car has been "routinely shut down[,] even when he was current on his $362 monthly car payment."[85] Instead of being able to demonstrate proof of payment to a repossession agent, he was reduced to using a screwdriver to rig the starter in to get home.[86] Automating the use of starter-interrupt devices would multiply these kinds of errors, while simultaneously making difficult for affected parties to communicate with someone to correct them.

3. *Enabling Corporate Self-Help*. Traditionally, 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.[87] However, given the risk of physical violence that accompanied self-

officiating systems in professional sports to identify the benefits of imperfect human decision-makers).

81. *See, e.g.*, Colin Lecher, *What Happens When an Algorithm Cuts Your Health Care*, VERGE (May 21, 2018), https://www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy [https://perma.cc/GX3W-F3MZ].

82. LESSIG, *supra* note 45, at 342.

83. Mulligan, *Personal Property Servitudes*, *supra* note 13, at 1161–62 (observing that applying digital rights management technologies "to real-world objects, such as cars, weapons, or computers" eliminates opportunities for efficient breaches and "risks making rights-infringing, but necessary, decisions impossible").

84. *Cf.* ZITTRAIN, *supra* note 9, at 114–16 (discussing the risk that algorithmically enabled perfect enforcement locks in mistakes in the context of copyright and First Amendment law); Mulligan, *Personal Property Servitudes*, *supra* note 13, at 1165 ("[T]he failures of [digital rights management technologies] are legion, particularly when the technology fails on its own terms and blocks people from accessing content they have a license to access.").

85. Corkery & Silver-Greenberg, *supra* note 2.

86. *Id.*

87. 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. Taylor, *Self-Help in Contract Law: An Exploration and Proposal*, 33 WAKE FOREST L. REV. 839, 841 (1998).

help repossession, it is only lawful if it can be done without breaching the peace.[88] If the holder of the disputed property protests its removal[89] or keeps the property in a locked building,[90] the would-be reclaimant is obliged 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."[91] Even in jurisdictions where a contract explicitly permits creditors to enter private dwellings for the purposes of repossession, courts regularly read the "breach of the peace" exception into the contract.[92] 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.[93]

Today, the possibility of remote interference creates a third option when there is a contractual dispute: instead of attempting to physically retrieve an item, an IoT company can employ remote interference to effectively "digitally repossess" some features or an entire item—an act that, absent the contract, would be considered criminal.[94]

Of course, self-help corporate remote interference may be acceptable in some scenarios. For example, a company can raise rates for a subscription service and stop providing the service should a customer refuse to pay, even if that renders an IoT device useless.[95] The benefits of self-help in such circumstances outweigh the various costs

88. Cohen, *supra* note 12, at 1103.

89. Both Connecticut and New York courts have held that conduct resulting in verbal objections alone can constitute prohibited breaches of the peace. Aviles v. Wayside Auto Body, Inc., 49 F. Supp. 3d 216, 226 (D. Conn. 2014) ("[A] repossessor may breach the peace if they repossess a vehicle in the face of oral protest from the owner of the vehicle."); Boles v. Cty. of Montgomery, No. 6:11–cv–522, 2014 WL 582259, at *9 (N.D.N.Y. 2014) ("It is clear that a mere verbal objection to the removal of property constitutes a breach of the peace.").

90. Most states allow repossessors to enter driveways that are open to the public. *See, e.g.*, CAL. BUS. & PROF. CODE § 7508.2(d) (prohibiting entry into "any private building or secured area"). Massachusetts, however, does not allow any entrance onto private property. MASS. GEN. LAWS ch. 255B, § 20B (2017).

91. Cohen, *supra* note 12, at 1103. This common law prohibition on creating a "breach of the peace" was incorporated into U.C.C. articles 9 and 2A. U.C.C. § 2A-525 (AM. LAW INST. & UNIF. LAW COMM'N 1990); U.C.C. § 9-503 (2010).

92. Cohen, *supra* note 12, at 1104 n.51.

93. *Id.* at 1104 n.49.

94. *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2018).

95. Should discontinuing a service create a foreseeable risk of harm, there may be a heightened notice requirement. *See infra* Part II.C (discussing how certain entities—namely, utilities and landlords—must provide notice of discontinued service commensurate with the potential risk of harm).

of state involvement to both parties and to the state.[96] However, 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 bad faith," but rather because they are unconsciously motivated to reach a particular response.[97] Self-interested enforcement is even more problematic when the relevant law is drafted by the enforcing entity—as is the case when IoT companies act in accordance with their terms of service.

IoT companies are already using remote interference or the threat of remote interference to hold IoT devices hostage and compel consumer action or extract concessions. One such example is conditioning product use on agreement to unilateral contractual modifications.[98] Should a user object, their only recourse is to forego using the device.[99] For example, Sonos, a smart-speaker company, recently announced that it would not provide expected and necessary software updates unless consumers agreed to changes to the privacy and data-collection policy, which expand the company's ability to use the speakers to collect, use, and share personal data.[100] As a company spokesperson stated: "The customer can choose to acknowledge the policy, or can accept that over time their product may cease to

96. *Cf.* David E. Pozen, *Self-Help and the Separation of Powers*, 124 YALE L.J. 2, 49 (2014) ("Self-help would not pose such a knotty problem for legal designers if it did not yield valuable benefits."). The possibility of self-help may deter "wrongdoing from occurring in the first place, reduce administrative costs, promote autonomy- or sovereignty-related values, and facilitate speedier redress." *Id.* At a deeper level, self-help might foster "cooperative relations, mitigate feelings of alienation from the law, or generate deeper internalization of first-order legal norms." *Id.*

97. *Id.* at 50 (noting that self-helpers may be biased by "motivated cognition and reliance on congenial interpretive methods or theories of law").

98. *See generally* NANCY KIM, WRAP CONTRACTS (2013) (discussing how wrap contracts unfairly burden consumers and create a coercive contracting environment). For a humorous take on the issue, see Nitrozac & Snaggy, *The Internet of Ransomware Things*, JOY OF TECH, http://www.geekculture.com/joyoftech/joyarchives/2340.html [https://perma.cc/RM63-D9WY] (illustrating how IoT devices might be held hostage; for example, a coffee maker threatens, "20 bucks in my PayPal account or I'll only brew decaf!").

99. *See, e.g.*, *Nest License Agreement*, *supra* note 78 ("You consent to this automatic update. If you do not want such Updates, your remedy is to stop using the Product."); *Uconnect Terms*, *supra* note 77, ¶ 25 ("Sprint reserves the right to modify the Uconnect Services (including remote updates on the Device)" and its terms of service "at any time without notice or liability to you in its sole discretion. If you do not agree with the modifications, your sole and exclusive remedy is to not use the Uconnect Services.").

100. 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 [https://perma.cc/N7WC-YTHB].

function."[101] Alternatively, an IoT company may engage in secretly coercive remote interference, such as when Apple pushed an operating-server update including a hardware-management feature that slowed down processors in phones with aging batteries, apparently to boost sales of its newer iPhone models.[102]

The power to enforce includes the power to decide *when* to enforce. Networked devices and personalized surveillance enable strategically manipulative action; the more companies know about individuals and the more devices they can control, the more influentially they can time when and how they address contractual breaches. Your car can be disabled just before work or a flight, or you might receive a notification that your smart thermostat was turned off or your front door unlocked while you are on vacation.[103]

In the absence of state oversight, bad-faith actors are freer to abuse these new self-help powers. 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.[104] Denis Grisak, the product's inventor and distributer, responded by denying the unit server connection.[105] Because the Garadget purchaser had not activated the device, he was not at risk of being locked out of his garage or having his garage door left open—but another customer who had activated the device and then annoyed the company might have been.[106] Absent a shift in governance, it will become increasingly commonplace for IoT companies to exploit this coercive capability.[107]

---

101. *Id.*

102. Steve Mullis, *Lawsuits Mount as Apple Manages Fallout from Revelation of Slowed iPhones*, NPR (Dec. 31, 2017, 8:12 AM), https://www.npr.org/2017/12/31/574792184/lawsuits-mount-as-apple-manages-fallout-from-revelation-of-slowed-iphones [https://perma.cc/JZ4R-FZJ6].

103. *Cf.* Ben Dickson, *The IoT Ransomware Threat Is More Serious Than You Think*, IOT SEC. FOUND. (Aug. 22, 2016), https://www.iotsecurityfoundation.org/the-iot-ransomware-threat-is-more-serious-than-you-think [https://perma.cc/6QFU-TJ4L] (arguing that it is the timing of ransomware attacks, rather than their irreversibility, that will render IoT ransomware effective).

104. Sean Gallagher, *IoT Garage Door Opener Maker Bricks Customer's Product After Bad Review*, ARS TECHNICA (Apr. 4, 2017, 11:35 AM), https://arstechnica.com/information-technology/2017/04/iot-garage-door-opener-maker-bricks-customers-product-after-bad-review [https://perma.cc/F883-ZR76].

105. *Id.*

106. *Id.*

107. *See, e.g.*, Tim Cushing, *Software Company Shows How Not To Handle Negative Review*, TECHDIRT (Dec. 22, 2016, 8:20 AM), https://www.techdirt.com/articles/

We have seen how connected products enable contractually permitted industry control before.[108] Companies have long employed terms of service and digital rights management technologies to limit consumer options—say, to keep consumers from sharing music files or independently repairing a device.[109] Famously, Amazon remotely deleted e-books from users' Kindle e-readers, including George Orwell's "1984," of all possible texts![110] Unrelenting self-help enforcement, mediated through technology, is problematic enough in the digital realm. But in the IoT context, it also increases the risk of physical injury to consumers.

B. A New Vector for Harm

IoT devices are "embodied"[111]: they have a presence in and ability to interact with the physical world.[112] And with physicality comes the

---

20161220/12411836320/software-company-shows-how-not-to-handle-negative-review.shtml [https://perma.cc/H2RX-62Y7].

108. *Cf.* K. Sabeel Rahman, *Regulating Informational Infrastructure: Internet Platforms as the New Public Utilities*, 2 GEO. L. TECH. REV. 234, 237 (2018) ("Those who control the terms of access to, and administration of, infrastructure are in a position to dominate those who depend on that infrastructure.").

109. Right-to-repair advocates argue that "manufacturers have increasingly used restrictive warranties, digital locks, and more to make it hard, or in some cases even impossible, for consumers to fix everything from iPhones to John Deere tractors." Louise Matsakis, *Security Experts Unite over the Right To Repair*, WIRED (Apr. 30, 2019), https://www.wired.com/story/right-to-repair-security-experts-california [https://perma.cc/X7A9-GSY6]. For example, American farmers have been reduced to 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 and enforced by the tractor's software. Jason Koebler, *Farmers Are Hacking Their Tractors with Ukrainian Firmware*, MOTHERBOARD (Mar. 21, 2017, 3:17 PM), https://motherboard.vice.com/en_us/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware [https://perma.cc/DN9G-8ECP]. For a defense of right-to-repair laws, see generally Pamela Samuelson, *Freedom to Tinker*, 17 THEORETICAL INQ. L. 563 (2016) (arguing that the "freedom to tinker" ought to be protected under IP law).

110. Amazon remotely removed these copies in response to a claim that the company "selling" the e-books did not have the rights to them. Brad Stone, *Amazon Erases Orwell Books from Kindle*, N.Y. TIMES (July 17, 2009), https://www.nytimes.com/2009/07/18/technology/companies/18amazon.html [https://perma.cc/R8FH-82QV].

111. CALO, *supra* note 25, at 5 (observing that robotic systems combine "the promiscuity of data with physical embodiment").

112. To some, this is their most distinctive feature. DeNardis & Raymond, *supra* note 15, at 477 ("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."); *see also* Schneier, *supra* note 15 ("The internet is no longer a web that we connect to. Instead, it's a computerized, networked, and interconnected world that we live in. This is the future, and what we're calling the Internet of Things.").

possibility of physical harm.[113] Consider the relatively innocuous Roomba, an autonomous vacuum-cleaning robot. In addition to cleaning untold numbers of floors, one Roomba caused the Pooptastrophe;[114] another "attacked" its sleeping owner;[115] and a third destroyed itself on a hot plate and, due to the resulting smoke damage, left its owner homeless.[116] While there might be disagreement about where fault lies in each of these scenarios, the overarching point is that IoT devices' physicality alters and magnifies the harm potential of remote interference. The remote deletion of your music file or e-book might frustrate you; the remote disabling of your security alarm, car, or implantable medical device could kill you.

The possibilities for potential injuries are limited only by the item's damage potential. A disabled smart thermostat could allow a house to become so hot or cold that plumbing, pets, and potentially even people could be harmed.[117] Pacemakers, insulin pumps, drug-administration devices, and other wearable or implanted medical devices could affect someone's physical health,[118] while IoT vehicles

113. Jack Balkin, *The Path of Robotics Law*, 6 CALIF. L. REV. CIRCUIT 45, 49 (2015); Calo, *supra* note 34, at 534.

114. Jessie Newton, FACEBOOK (Aug. 9, 2016), https://www.facebook.com/jesse.newton.37/posts/776177951574 [https://perma.cc/PV4G-G9VJ] ("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.").

115. Justin McCurry, *South Korean Woman's Hair 'Eaten' By Robot Vacuum Cleaner as She Slept*, GUARDIAN (Feb. 8, 2015, 11:53 PM), https://www.theguardian.com/world/2015/feb/09/south-korean-womans-hair-eaten-by-robot-vacuum-cleaner-as-she-slept [https://perma.cc/Y6HR-2FNS] (detailing the event and noting that the vacuum may not have been appropriately programmed for cultures where it is common to sit or nap on the floor).

116. Macrina Cooper-White, *Robot Suicide? Rogue Roomba Switches Self On, Climbs onto Hotplate, Burns Up*, HUFFINGTON POST (Nov. 13, 2013, 1:26 PM), https://www.huffingtonpost.com/2013/11/13/robot-suicide-roomba-hotplate-burns-up_n_4268064.html [https://perma.cc/69MY-F9EB].

117. *See* Mick Bilton, *Nest Thermostat Glitch Leaves Users in the Cold*, N.Y. TIMES (Jan. 13, 2016), https://www.nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html [https://perma.cc/G487-CSSQ] ("For those who are elderly or ill, or who have babies, a freezing house can have dire health consequences. . . . [P]ipes could freeze and burst, causing major damage.").

118. *See, e.g.*, Basit Mahmood, *Lover Tried To Poison Diabetic Fiancé Using 'Remote Controlled Insulin Pump*,' METRO (Mar. 17, 2019, 1:08 PM), https://metro.co.uk/2019/03/17/lover-tried-poison-diabetic-fiance-using-remote-controlled-insulin-pump-8916952 [https://perma.cc/B9EV-X5Q] (describing a case of intentional insulin overdose via a remote controlled pump).

could injure or kill drivers,[119] passengers,[120] other drivers,[121] and pedestrians.[122]

This Article brackets cybersecurity-related harms to focus on harms resulting from corporate remote interference. To fully conceptualize the scope of potential harms posed by connected devices that affect our bodies and environment, however, it is worth discussing the potential physical threats posed by hacked devices.[123] 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 Buddhist prayer beads,[124] resulting in the neologism that "[t]he 'S' in 'IoT' stands for 'security.'"[125] Even reputable and experienced tech companies are producing insecure products. One team of researchers was able to remotely take control

119. *See, e.g.*, Nathan Bomey, *Tesla Model X Driver Killed in California Crash Wasn't Holding Steering Wheel, NTSB Says*, USA TODAY (June 7, 2018, 1:04 PM), https://www.usatoday.com/story/money/cars/2018/06/07/tesla-model-x-autopilot-crash-ntsb-report/681148002 [https://perma.cc/XB6B-YE69] (describing the fatal crash of a partially autonomous vehicle).

120. *See, e.g.*, Jake Lingeman, *Tesla Sued After Speed Limiter Removed, Passenger Killed in Fatal Crash*, AUTOWEEK NEWS (Jan. 11, 2019, 7:00 AM), https://autoweek.com/article/luxury/tesla-sued-after-speed-limiter-removed-passenger-dead-fatal-crash [https://perma.cc/J96S-EZZF] (describing a lawsuit over a passenger's death in a crash involving a partially autonomous vehicle).

121. *See, e.g.*, Tim Stelloh, *Tesla Was in Autopilot Mode Before Utah Crash, Driver Tells Police*, NBC NEWS (May 14, 2018, 6:06 PM), https://www.nbcnews.com/business/autos/tesla-was-autopilot-mode-utah-crash-driver-tells-police-n874136 [https://perma.cc/72GH-PSMF] (describing how a partially autonomous vehicle ran a red light and struck a truck).

122. *See, e.g.*, Daisuke Wakabayashi, *Self-Driving Uber Car Kills Pedestrian in Arizona, Where Robots Roam*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/uber-driverless-fatality.html [https://perma.cc/8QQJ-74NZ] (describing the death of a pedestrian after being struck by a partially autonomous vehicle).

123. *See supra* note 15.

124. Samuel Gibbs, *Hackers Can Hijack Wi-Fi Hello Barbie To Spy on Your Children*, GUARDIAN (Nov. 26, 2015, 6:16 AM), https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children [https://perma.cc/NT5J-5769]; Ko Tin-yau, *Buddhists Go High-Tech: Acer To Launch Smart Prayer Beads*, EJINSIGHT (Jan. 30, 2018, 5:06 PM), http://www.ejinsight.com/20180130-buddhists-go-high-tech-acer-to-launch-smart-prayer-beads [https://perma.cc/KYU2-CEU3]; *see* JAN-PETER KLEINHANS, STIFTUNG NEUE VERANTWORTUNG, INTERNET OF INSECURE THINGS: CAN SECURITY ASSESSMENT CURE MARKET FAILURES? 5 (2017) ("The current trend is to make everything 'smart' – toaster, fridge, thermostat, lighting.").

125. *Cf.* KLEINHANS, *supra* note 124, at 9–14 (describing how IoT devices are vulnerable to exploitation by hackers and criminals and suggesting ways to improve the security of IoT devices).

of a Jeep SUV while it was being driven;[126] another team identified flaws in Apple's HomeKit smart-home system that would have permitted hackers to unlock front doors.[127] The insecurity of the "Internet of Things Inside Our Body"[128] 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[129] and the FDA-mandated recall of more than four hundred thousand pacemakers due to a cybersecurity vulnerability.[130] Other hackers have demonstrated that it is possible to take control of smart lights and use them to induce epileptic seizures.[131] Further, the more electrical grids, transportation services, health and medical systems, and other critical infrastructure are incorporated into the IoT ecosystem, the more likely it is that disruption of those systems will threaten human safety and national security.[132] 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

126. Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, WIRED (July 21, 2015, 6:00 AM), http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway [https://perma.cc/6YCN-AMZT].

127. Samuel Gibbs, *Apple Fixes HomeKit Bug That Allowed Remote Unlocking of Users' Doors*, GUARDIAN (Dec. 8, 2017, 5:41 AM), https://www.theguardian.com/technology/2017/dec/08/apple-fixes-homekit-bug-remote-unlocking-doors-security-flaw-iphone-ipad-ios-112-smart-lock-home [https://perma.cc/546E-GYMG].

128. *See* Kerr, *supra* note 20, at 341–43 (listing the multiple medical uses and capabilities of radio-frequency implantable devices and warning of the corresponding need for stronger privacy regulations).

129. Dana Ford, *Cheney's Defibrillator Was Modified To Prevent Hacking*, CNN (Oct, 24, 2013, 9:51 AM), https://www.cnn.com/2013/10/20/us/dick-cheney-gupta-interview/index.html [https://perma.cc/UBF7-GUQC].

130. Swati Khandelwal, *FDA Recalls Nearly Half a Million Pacemakers over Hacking Fears*, HACKER NEWS (Sept. 1, 2017), https://thehackernews.com/2017/08/pacemakers-hacking.html [https://perma.cc/A9KC-FVJQ].

131. Eyal Ronen & Adi Shamir, *Extended Functionality Attacks on IoT Devices: The Case of Smart Lights* 3–5 (2016 IEEE European Symposium on Security and Privacy, Invited Paper, 2016).

132. *See* DeNardis & Raymond, *supra* note 15, at 486–87 (discussing the importance of power grids and transportation infrastructure to military effectiveness and Russia's targeting of these systems in Ukraine as a hybrid-warfare approach). The risks associated with an over-connected military have often been explored in science fiction. *See generally, e.g.*, P.W. SINGER & AUGUST COLE, GHOST FLEET: A NOVEL OF THE NEXT WORLD WAR (2016); BATTLESTAR GALACTICA (1978).

monitoring system at Ukraine's Chernobyl Nuclear Power Plant to go offline.[133]

While hackable cars,[134] home-security systems,[135] pacemakers,[136] and other IoT devices certainly create problems worth addressing,[137] the current focus on the physical risks of criminal hacks distracts from the physical risks of corporate remote interference. As detailed in the next Part, corporations can do anything hackers can do—but their actions are legitimized by contract.

II. BARRIERS TO CIVIL LIABILITY SUITS

Classically, contracts allow parties to negotiate their respective obligations, and informed party consent justifies superseding default rules. Meanwhile, tort liability for rights that cannot be contracted away acts as a backstop to protect potentially vulnerable parties.

In the IoT context, however, notwithstanding the escalating possibility of physical harm resulting from corporate remote interference,[138] contract and tort law operate in tandem to create a

133. Nicole Perlroth, Mark Scott & Sheera Frenkel, *Cyberattack Hits Ukraine Then Spreads Internationally*, N.Y. TIMES (June 27, 2017), https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html?mcubz=0&_r=0 [https://perma.cc/5ECP-CLRF].

134. Greenberg, *supra* note 126.

135. *See* Edenborough v. ADT, LLC, No. 16-CV-02233-JST, 2016 WL 6160174, at *1 (N.D. Cal. Oct. 24, 2016) (discussing a class action suit alleging that a home security system used unsecured and unencrypted protocols, rendering it vulnerable to hacking).

136. Khandelwal, *supra* note 130.

137. As IoT devices proliferate, so do stories of hacked IoT devices causing harm, ranging from hackers terrorizing children through baby monitors, to wide-scale privacy violations, to worldwide botnet attacks that have taken down large swaths of the internet. For examples of these incidents in their stated order, see Richard Adhikari, *Webcam Maker Takes FTC's Heat for Internet-of-Things Security Failure*, TECHNEWSWORLD (Sept. 5, 2013), https://www.technewsworld.com/story/78891.html [https://perma.cc/Y5U4-8GNB] (reporting how hackers posted live feeds from nearly seven hundred household cameras); *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 [https://perma.cc/U8WL-VP6T]; and 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 [https://perma.cc/YYS8-K9WA] (describing how Mirai-based "botnets" compromised IoT devices to launch the largest distributed denial-of-service ("DDoS") attack to date, taking "down a big chunk of the Internet for most of the Eastern seaboard").

138. Again, this Article brackets purely economic harms, privacy harms, and cybersecurity harms to focus on physical harms resulting from corporate remote interference.

series of hurdles for would-be plaintiffs. This Part details how our current civil liability system inappropriately shields IoT companies.[139]

This is not to say that civil liability mechanisms are incapable of evolving to address these situations. Common law principles are relatively tech neutral, allowing them to adjust to different circumstances. For example, the general duty of care—that an actor "has a duty to exercise reasonable care when the actor's conduct creates a risk of physical harm"[140]—applies equally to someone riding a bike, driving a car, or operating a tractor. However, absent a better understanding of how IoT-enabled harms operate and propagate, judges are likely to apply contracts, products liability, and negligence doctrinal standards narrowly, in ways that functionally minimize corporate liability. Further, because these devices allow for corporate action at a distance, technology's ability to redirect responsibility and disrupt the causal chain is heightened in the IoT context.

A. Contractual Obstacles

Most IoT terms of service notify users of the possibility of corporate remote interference and condition the purchase and use of a device on consumer acknowledgment and agreement to those terms.[141] Standing alone, contractual notice renders this form of electronic self-help lawful,[142] even in states that otherwise prohibit it.[143] When paired

139. *Cf.* Radin, *Regulation by Contract*, *supra* note 26, at 143–44 (discussing how private firms use contracts of adhesion, such as shrink-wrap contracts and click-wrap contracts, to sidestep consumer protection laws and tort law accountability mechanisms in the intellectual property context).

140. RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL AND EMOTIONAL HARM § 7(a) (AM. LAW INST. 2010).

141. *See* Whittaker, *supra* note 100 (identifying one smart speaker company that refused to provide necessary software updates to users who did not accept modifications to privacy terms).

142. *See, e.g.*, *In re* VTech Data Breach Litig., No. 15-CV-10889, 15-CV-10891, 15-CV-11620, 15-CV-11885, 2018 WL 1863953, at *4 (N.D. Ill. Apr. 18, 2018) (dismissing a breach of contract claim for discontinued services, as the company's Privacy Policy allowed defendants to terminate online services at any point).

143. The Uniform Computer Information Transactions Act ("UCITA") restricts "electronic self-help," the repossession of software. Only Virginia and Maryland have adopted the UCITA, but both states permit contracting parties to consent to such actions. MD. CODE ANN., COM. LAW § 22-816 (West 2017); VA. CODE ANN. § 59.1-508.16 (2017); *see also* Brian D. McDonald, *The Uniform Computer Information Transactions Act*, 16 BERK. TECH. L.J. 461, 474 (2001) (describing the nearly full and qualified adoptions of the UCITA by Virginia and Maryland, respectively). Connecticut also restricts electronic self-help, with an expansive definition that includes using electronic means to locate collateral, but it also permits contracting parties to agree that it can be employed. CONN. GEN. STAT. § 42a-9-609 (2016) (stating that repossession is only

with exculpatory clauses, notice can restrict or even eliminate corporate liability; when paired with disclaimers or express warranties, it can bar breach of warranty claims; standing alone, it can preclude common law tort suits.[144]

1. *Exculpatory and Other Liability-Limiting Clauses*. Unsurprisingly, IoT-device terms of service agreements attempt to minimize industry liability for the harms resulting from their remote interference[145] through liability disclaimers or caps on the costs of breaches.[146] Specific- and exclusive-remedy clauses allow companies to predetermine customer rights.[147] For example, Nest's terms of service note that, should someone not want the company's over-the-air updates, "[their] remedy is to stop using [the Services and] the Product[s]."[148] Meanwhile, monetary ceilings on direct damages[149] and

allowed "if the debtor separately agrees to a term of the security agreement authorizing electronic self-help that requires notice of exercise").

144. Granted, these statements are generalizations, as every state has different standards for evaluating these varied claims.

145. As others have detailed, the "law of the firm" often favors the company at the expense of the consumer. Radin, *Regulation by Contract*, *supra* note 26, at 147–48; *see* Melissa T. Lonegrass, *Finding Room for Fairness in Formalism—The Sliding Scale Approach to Unconscionability*, 44 LOY. U. CHI. L.J. 1, 4 (2012) (observing that "[s]tandard forms are ubiquitous, but hardly innocuous" and describing common terms and waivers that privilege industry).

146. *Cf.* U.C.C. §§ 2-316(4), 2-718, 2-719 (AM. LAW INST. & UNIF. LAW COMM'N 1951) (allowing contract modifications that limit damages and remedies).

147. *Cf.* U.C.C. § 2-719(1)(b) (allowing parties to agree to an exclusive remedy). *See, e.g.*, TESLA, MODEL S MODEL X MODEL 3 NEW VEHICLE LIMITED WARRANTY (2017–2018) [hereinafter *Tesla Warranty*], https://www.tesla.com/sites/default/files/downloads/Model_S_X_Warranty_NA_en.pdf [https://perma.cc/A77E-YEYJ] ("The performance of necessary repairs and parts replacement by Tesla is the exclusive remedy under this New Vehicle Limited Warranty or any implied warranties."); *see also Philips Hue Terms*, *supra* note 77 ("If you do not want such updates, your sole remedy is to cease using the Services altogether.").

148. *Nest License Agreement*, *supra* note 78.

149. *Cf.* U.C.C. § 2-719 (allowing limitation of damages). For example, Tesla's warranty states that it "shall not be liable for any direct damages in an amount that exceeds the fair market value of the vehicle at the time of the claim." *Tesla Warranty*, *supra* note 147, at 8. Alexa's terms of use state that "in no event will our licensors' or our service providers' aggregate liability with respect to any claim arising from or relating to this Agreement or your use of Alexa exceed fifty dollars ($50)." *Alexa Terms*, *supra* note 77. Nest limits liability to no more than two times the amount paid by the consumer, *Nest License Agreement*, *supra* note 78; and Philips Hue limits liability to the amount of fees paid in connection to the service, *Philips Hue Terms*, *supra* note 77.

exclusions of special, incidental, or consequential damages[150] also limit corporate liability.[151]

These terms purportedly reflect the informed agreement of the contracting parties; in reality, most of these "agreements" are contracts of adhesion where unsophisticated consumers have limited information about the risks of remote interference and no opportunity to bargain, effectively allowing companies to unilaterally price harms. Given that many IoT devices are used by individuals who are not in privity of contract with the IoT company, IoT companies are reasonably trying to "find ways to 'bake' or incorporate 'the equivalent of a click-wrap' agreement into the functionality of their device," to limit corporate liability with regard to *all* device users.[152] Ultimately, these contracts "launder injustice"[153] insofar as they legitimize otherwise unfair allocations of liability.

Granted, the ability to contractually limit liability is not unbounded.[154] While we are far from the days when courts would strike down any contractual limitation on liability for negligence,[155] most states circumscribe a limit's application. Exculpatory clauses that limit

150. *Cf.* U.C.C. § 2-715 (describing and defining incidental and consequential damages). For example, "Tesla . . . disclaims any and all indirect, incidental, special and consequential damages arising out of or relating to your vehicle." *Tesla Warranty*, *supra* note 147, at 7. Similarly, Nest excludes any "consequential, exemplary, special or incidental damages." *Nest License Agreement*, *supra* note 78.

151. Radin, *Regulation by Contract*, *supra* note 26, at 149 (discussing how exculpatory clauses purport to relieve firms of liability from negligence damages and litigation remedies generally).

152. E.g., Mauricio Paez & Mike La Marca, *The Internet of Things: Emerging Legal Issues for Businesses*, 43 NORTHERN KY. L. REV. 29, 61 (2016); *e.g. id.* ("If the product lacks a user interface where the end-user can check a box or otherwise agree to terms, the product should require the user's agreement through a website or mobile application prior to enabling functionality.").

153. Daniel Markovits, *Good Faith as Contract's Core Value*, *in* PHILOSOPHICAL FOUNDATIONS OF CONTRACT LAW 272, 291 (Gregory Klass, George Letsas & Prince Saprai eds., 2014) ("[C]ontract possesses the power to launder injustice, creating legitimate entitlements between parties where previously there were none and, moreover, inducing the parties to recognize these entitlements.").

154. *See, e.g.*, RESTATEMENT (SECOND) OF CONTRACTS § 195 (AM. LAW INST. 1981) (providing the contexts under which terms exempting parties from liability are unenforceable on grounds of public policy, including: (1) when the harm is caused intentionally or recklessly; (2) when the harm is caused negligently by (a) an employer to his employee, (b) by one owing a duty of public service, or (c) when the harm is done to someone of a protected class; and (3) when physical harm to a consumer would result from use of a product, unless that term is fairly bargained for and consistent with the policy underlying that liability).

155. *See* The Steamer *Syracuse*, 79 U.S. 167, 171 (1870) ("It is unnecessary to consider the evidence relating to the alleged contract of towage, because, [even] if . . . the canal-boat was being towed at her own risk, nevertheless, the steamer is liable, if, through the negligence of those in charge of her, the canal-boat has suffered loss.").

future liability for physical injury are invalid in three states.[156] Other states invalidate exculpatory clauses that are overly broad,[157] are presented in complex or unclear language,[158] attempt to waive liability for intentional acts[159] or gross negligence,[160] or are otherwise unconscionable[161] or contrary to public policy.[162] Further, under the U.C.C., clauses limiting liability for bodily harms caused by consumer

156. LA. CIV. CODE ANN. art. 2004 (1985); MONT. CODE ANN. § 28-2-702 (2017); Hiett v. Lake Barcroft Cmty. Ass'n, 418 S.E.2d 894, 897 (Va. 1992).

157. *See, e.g.*, Atkins v. Swimwest Family Fitness Ctr., 691 N.W.2d 334, 343 (Wis. 2005) (considering multiple factors and ultimately holding that the exculpatory waiver in a swimming facility agreement was too broad and did not provide notice or an opportunity to bargain).

158. *See* Swartzentruber v. Wee-K Corp., 690 N.E.2d 941, 944 (Ohio Ct. App. 1997) ("[E]xculpatory provisions in contracts are to be strictly construed so as not to relieve one from liability for his own negligence unless it is expressed in clear and unequivocal terms." (quotations omitted) (quoting Glaspell v. Ohio Edison Co., 505 N.E.2d 264, 265–67 (Ohio 1987))).

159. *See, e.g.*, Moore v. Waller, 930 A.2d 176, 179 (D.C. 2007) ("[C]ourts have not generally enforced exculpatory clauses to the extent that they limited a party's liability for gross negligence, recklessness or intentional torts." (quoting *Carleton v. Winter*, 901 A.2d 174, 181 (D.C. 2006))); Mankap Enters., Inc. v. Wells Fargo Alarm Servs., 427 So.2d 332, 333–34 (Fla. Dist. Ct. App. 1983) ("The law is settled that a party cannot contract against liability for his own fraud in order to exempt him from liability for an intentional tort, and any such exculpatory clauses are void as against public policy." (citations omitted)).

160. *See, e.g.*, Smallwood v. NCSOFT Corp., 730 F. Supp. 2d 1213, 1227 (D. Haw. 2010) (describing this as "the majority rule"); Henrioulle v. Marin Ventures, Inc., 573 P.2d 465, 468 (Cal. 1963) (delineating the *Tunkl* factors for when an exculpatory clause is invalid as contrary to public policy). This norm is sometimes enacted in state statutes. *See, e.g.*, CAL. CIV. CODE § 1668 (West 2013) ("All contracts which have for their object, directly or indirectly, to exempt any one from responsibility for his own fraud, or willful injury to the person or property of another, or violation of law, whether willful or negligent, are against the policy of the law.").

161. *See* Williams v. Walker-Thomas Furniture, 350 F.2d 445, 449–50 (D.C. Cir. 1965) (defining the scope of unconscionability and holding that, where the element of unconscionability is present at the time a contract is made, the contract may be unenforceable); Day v. CTA, Inc., 324 P.3d 1205, 1209 (Mont. 2014) ("A contract is unconscionable if it is a contract of adhesion and if the contractual terms unreasonably favor the drafter.").

162. *See, e.g.*, Kalisch-Jarcho, Inc. v. City of New York, 58 N.Y.2d 377, 384–85 (N.Y. 1983) ("[A]n exculpatory agreement, no matter how flat and unqualified its terms, will not exonerate a party from liability under all circumstances. Under announced public policy, it will not apply to exemption of willful or grossly negligent acts."); Dimick v. Hopkinson, 422 P.3d 512, 517 (Wyo. 2018) ("Wyoming courts enforce exculpatory clauses releasing parties from liability for injury or damages resulting from negligence if the clause is not contrary to public policy." (quoting Schutkowski v. Carey, 725 P.2d 1057, 1059 (Wyo. 1986))). California courts consider six factors to identify when an exculpatory clause should be held invalid as contrary to public policy. Tunkl v. Regents of the Univ. of Cal., 60 Cal. 2d 92 (Cal. 1963).

goods are prima facie unconscionable,[163] and—when litigated—courts rarely uphold such clauses.[164]

Given the variability of these rules and many consumers' lack of access to justice, however, companies often purport to waive all claims to the extent legally possible—and then some.[165] For instance, Tesla's warranty states that its "limitations and exclusions shall apply whether your claim is in contract, tort (including negligence and gross negligence), breach of warranty or condition, misrepresentation (whether negligent or otherwise) or otherwise at law or in equity."[166] Some IoT contracts attempt to waive liability even for "reasonably foreseeable" harm;[167] others induce reliance on a risk-avoidance service and then claim to waive liability when corporate remote interference results in a failure to provide that service.[168] Although an exculpatory clause's scope will be limited in situations where a company's remote interference constitutes an intentional act or gross negligence, in the forty-seven states that do not proactively invalidate exculpatory clauses, carefully crafted contractual terms can minimize corporate liability for injuries resulting from ordinary negligence.[169] For example, although retaliatory bricking of a garage door based on a bad Amazon review would likely be considered an intentional act that

163. U.C.C. § 2-719(3) (AM. LAW INST. & UNIF. LAW COMM'N 1951). This is a rebuttable presumption. *See* Mullan v. Quickie Aircraft Corp., 797 F.2d 845, 852–53 (10th Cir. 1986) (holding that the exculpatory provision at issue was not unconscionable because of the buyer's familiarity with the document and awareness of the terms, and thus the clause was valid and enforceable); Matthews v. Ford Motor Co., 479 F.2d 399, 402 (4th Cir. 1973) (noting that, in this case, the defendant failed to rebut the presumption of unconscionability).

164. Morrow v. New Moon Homes, Inc., 548 P.2d 279, 286 n.12 (Alaska 1976) (noting that courts "rarely uphold" waivers of liability for personal injuries).

165. Memo from Matthiesen, Wickert & Lehrer, S.C. on Exculpatory Agreements and Liability Waivers in All 50 States (Aug. 21, 2019), https://www.mwl-law.com/wp-content/uploads/2018/05/EXCULPATORY-AGREEMENTS-AND-LIABILITY-WAIVERS-CHART-00214377x9EBBF.pdf [https://perma.cc/Q8S5-PLEY].

166. *Tesla Warranty*, *supra* note 147, at 7–8.

167. *See, e.g.*, *id.* (stating that its warranty limitations and exclusions apply "even if Tesla is advised of the possibility of such damages or such damages are reasonably foreseeable").

168. Uconnect—a company that makes and services software for Fiat Chrysler—notes in its terms of service that it has the right to make software updates without notice and that, during updates, "you may be unable to use the Uconnect Services or place a call to 9-1-1 until the software update is complete." *Uconnect Terms*, *supra* note 77, ¶¶ 9.3, 17; *see also id.* ¶ 25 ("Sprint reserves the right to modify the Uconnect Services (including remote updates on the Device) . . . at any time without notice or liability to you in its sole discretion. . . . Sprint may deactivate the Uconnect Services at any time without notice or liability to you.").

169. Matthiesen, Wickert & Lehrer, *supra* note 165, at 6–7 (detailing standards for different states).

invalidates the contractual exculpatory clause, the automated bricking of that same door after nonpayment may retain the clause's protection.[170]

Nor will modern courts likely find exculpatory clauses void as unconscionable in cases involving IoT devices marketed for individual or household use. As has been frequently bemoaned, "the doctrine [of unconscionability] offers little hope in the consumer goods realm."[171] While the U.C.C. creates a strong presumption of unconscionability for IoT devices that cause bodily harm,[172] it does not create a similar one for property damage;[173] nor will it easily be applied when IoT devices cause bodily harm indirectly.[174] Further, courts are generally unwilling to find commercial contracts procedurally unconscionable,[175] particularly—as will be the case for most IoT items—where the consumer has options regarding which product to buy[176] or where the contract circumscribes corporate liability for a recreational or frivolous activity.[177] And even though IoT-device terms of service are often "take-it-or-leave-it" contracts, this is insufficient to establish

170. Gallagher, *supra* note 104.

171. Rory Van Loo, *Helping Buyers Beware: The Need for Supervision of Big Retail*, 163 U. PA. L. REV. 1311, 1364 (2015); *see also* Lonegrass, *supra* note 145, at 3 (observing that the unconscionability doctrine "has been an ineffectual tool for consumer protection").

172. U.C.C. § 2-719(3) (AM. LAW INST. & UNIF. LAW COMM'N 1951).

173. *Id.*; *see, e.g.*, Gladden v. Cadillac Motor Car Div., Gen. Motors Corp., 83 N.J. 320, 331–32 (1979) (distinguishing between personal injury loss and property loss).

174. *See infra* Part II.D.

175. In addition to the libertarian argument in favor of parties being able to bind themselves "as they see fit," Hall v. Sinclair Refining Co., 242 N.C. 707, 709 (1955), courts justify upholding exculpatory clauses in the business context on the ground that it promotes efficiency. As noted by one court, "[Exculpatory] clauses enable businesses to engage in commerce without incurring excessive financial risks that might otherwise make doing business prohibitively expensive." Locke v. Life Time Fitness, Inc., 20 F. Supp. 3d 669, 676 (N.D. Ill. 2014); *see also* Gladden v. Boykin, 402 S.C. 140, 144–45 ("Limitation of liability and exculpation clauses are . . . commercially reasonable in at least some cases, since they permit the provider to offer the service at a lower price, in turn making the service available to people who otherwise would be unable to afford it."); Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425, 438 (2008) ("[C]ourts are reluctant to apply the doctrine of unconscionability in the commercial context.").

176. Scott J. Burnham, *Are You Free to Contract Away Your Right to Bring a Negligence Claim?*, 89 CHI.-KENT L. REV. 379, 383 (2014). However, the existence of a market for IoT devices should not be a relevant factor in an unconscionability analysis—as discussed below, the market is unlikely to provide the information consumers would need to make an informed selection among products. *See infra* Part II.E.

177. Burnham, *supra* note 176, at 383.

procedural unconscionability.[178] Meanwhile, for a provision to be found substantively unconscionable, the terms must be "shocking to the conscience," "monstrously harsh," or "exceedingly calloused"[179]—and exculpatory clauses rarely meet this high bar.[180] In addition to these familiar limits, remote interference introduces an additional snarl: because the unconscionability doctrine applies to the sale of goods, courts may not apply it to sales of IoT devices that bundle a good with one or more services, especially where the injury results from the cessation of a service.[181]

While courts will sometimes void contractual provisions as contrary to public policy, they are often unwilling to do so on the grounds that efficiency and economic growth require predictability and stability in contract and property regimes.[182] For a public policy argument to succeed in the IoT context, the court must confront the larger question of whether these market values outweigh the aims achieved by requiring companies to shoulder liability for the physical harms caused by their remote interference.[183] But this determination requires a thorough understanding of how corporate remote

178. *See, e.g.*, Muhammad v. Cty. Bank of Rehoboth Beach, Del., 912 A.2d 88, 96–97 (N.J. 2006) ("The determination that a contract is one of adhesion, however, is the beginning, not the end, of the inquiry into whether a contract . . . should be deemed unenforceable . . . . A sharpened inquiry concerning unconscionability is necessary when a contract of adhesion is involved." (citations omitted)), *superseded in part by statute in* Litman v. Cellco P'ship, 655 F.3d 225 (3d Cir. 2011); *see also* Burnham, *supra* note 176, at 381 ("Most of the time, the exculpatory clause is going to be found in a contract of adhesion. But as the courts say *ad nauseam*, that is not enough to establish unconscionability, even procedural unconscionability."); Joshua N. Cohen, *Sound the Alarm: Limitations of Liability in Alarm Service Contracts*, 85 FORDHAM L. REV. 813, 818 (2016) ("Often, exculpatory clauses are found in standard-form contracts that are offered on a 'take it or leave it' basis, known as contracts of adhesion. However, the mere fact that an exculpatory clause appears in an adhesion contract is not enough to establish procedural unconscionability." (citations omitted)).

179. *See, e.g.*, Gandee v. LDL Freedom Enters., Inc., 293 P.3d 1197 (Wash. 2013).

180. *See, e.g.*, Sanislo v. Give Kids the World, Inc., 157 So.3d 256, 260 (Fla. 2015) (explaining that while "[p]ublic policy disfavors exculpatory contracts because they relieve one party of the obligation to use due care and shift the risk of injury to the party who is probably least equipped to take the necessary precautions to avoid injury and bear the risk of loss," the preference of courts is to respect the freedom to contract and honor contractual terms whenever possible; accordingly, "unambiguous exculpatory contracts are enforceable unless they contravene public policy" (citations omitted)); Lonegrass, *supra* note 145, at 4 (noting that this aspect of the doctrine "discourages decision makers from inquiring whether boilerplate [contract] terms produce unacceptably harsh results").

181. Elvy, *supra* note 14, at 118.

182. Matthiesen, Wickert & Lehrer, *supra* note 165, at 2.

183. This Article proposes various public policy arguments for limiting the scope of corporate exculpatory clauses below. *See infra* Part III.B.1.b.

interference enables and increases consumer harm, both at the individual and aggregate levels.[184]

2. *Warranty Claims*. When purchased items do not operate as expected, consumers can bring breach of warranty claims grounded in express or implied warranties. Assuming an IoT company does not explicitly state that it will not remotely alter or deactivate the IoT device—indeed, most terms of service have statements to the opposite, expressly reserving the right to engage in such activities[185]—a consumer's only possible warranty claim for harms arising from remote interference would be a violation of an implied warranty of merchantability.[186] This generally means that the goods are "fit for the ordinary purposes for which such goods are used," are of a fair quality, and "conform to the promise or affirmations of fact made on the container or label."[187] But breach of warranty claims for consumer harms resulting from remote interference will likely fail, either because the IoT device will be deemed incidental to the provision of a service, such that U.C.C. implied warranties will not attach,[188] or because they are barred by contractual provisions.[189]

Courts rarely find that devices that exist primarily to provide a service have an implied warranty of merchantability. Where a product bundles a good with a service, as is often the case for IoT devices, courts employ the predominance test to evaluate whether an implied warranty attaches; if the product's primary purpose "is the rendition of service, with goods incidentally involved," courts will generally find that there is no implied warranty of merchantability.[190] An Amazon

184. For a discussion of how intervening actors introduce seeming breaks in the causal chain, see *infra* Part II.D.

185. *See supra* note 101 and accompanying text.

186. There is also an implied warranty of fitness, which applies when a seller is assisting a buyer with a purchase. U.C.C. § 2-315 (AM. LAW INST. & UNIF. LAW COMM'N 1951). Absent significant revision, however, this warranty will not apply to postsale situations where remote interference results in harm, as it only governs the seller's actions at time of sale.

187. U.C.C. § 2-314.

188. Elvy, *supra* note 14, at 114–17. While courts have found two common law implied warranties in service contracts—namely, an implied warranty of good workmanship and of habitability—these warranties will generally not be relevant for most IoT devices purchased for individual or household use.

189. *Id.* at 119.

190. *See, e.g.*, Ogden Martin Sys. Indianapolis v. Whiting Corp., 179 F.3d 523, 530 (7th Cir. 1999); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 983 (S.D. Cal. 2014) (dismissing implied warranty claims regarding Sony's Playstation consoles

Echo, which "connects to Alexa to play music, make calls, set music alarms and timers, ask questions, [and] control smart home devices" might fail this test.[191]

IoT devices that are primarily goods, like a "smart" scale, will have an implied warranty of merchantability. But savvy companies can include various provisions in their terms of service contracts to preclude breach of warranty claims for harms resulting from remote interference. This implied warranty only represents a promise about the condition of the product at the time it is sold; it does not guarantee that a product will last or operate consistently for any specific length of time, and sellers can contractually modify the warranty's time period.[192] Furthermore, implied warranties do not address problems arising from failure to follow directions or improper maintenance; an IoT company could certainly argue that contractually prohibited tinkering or failure to install an update would constitute a failure to follow directions or engage in proper maintenance, voiding any express or implied warranty.[193] Finally, IoT companies can include disclaimers and express warranties that circumscribe implied consumer rights. Courts tend to uphold implied warranty disclaimers[194] and find that express warranties displace implied ones.[195]

3. *Trespass to Chattels and Conversion*. Common law courts have developed various torts to protect an individual's right to be free from others' interference with lawfully possessed property. Here again, however, the combination of contractual provisions and the tethered

on the grounds that network services predominated and that "network services are not subject to the UCC" because they do not satisfy the definition of "goods").

191. *Echo (2nd Generation) – Smart Speakers with Alexa and Dolby Processing*, AMAZON, https://www.amazon.com/all-new-amazon-echo-speaker-with-wifi-alexa-dark-charcoal/dp/B06X
CM9LJ4 [https://perma.cc/9NFN-M8HS].

192. Some states provide that implied warranties are in effect for a specific period of time after the sale of the item, but these provisions usually allow sellers to modify that length of time with superseding explicit warranties valid for shorter periods. *See, e.g.*, CAL. CIV. CODE § 1791.1(c) (2018).

193. *See, e.g.*, *Tesla Warranty*, *supra* note 147, at 7 (stating that warranties will be voided if the owner "do[es] not follow the specific instructions and recommendations," including "[i]nstalling the vehicle's software updates after notification that there is an update available").

194. Arlie R. Nogay, *Enforcing the Rights of Remote Sellers Under the UCC: Warranty Disclaimers, the Implied Warranty of Fitness for a Particular Purpose and the Notice Requirement in the Nonprivity Context*, 47 U. PITT. L. REV. 873, 898 (1986); Scott, *supra* note 175, at 438.

195. U.C.C. § 2-317(c) (AM. LAW INST. & UNIF. LAW COMM'N 1951) ("Express warranties displace inconsistent implied warranties other than an implied warranty of fitness for a particular purpose.").

nature of IoT devices shield IoT companies from claims for harms arising from their remote interference.

If a consumer owns a device, the personal property torts of conversion and trespass to chattels would seem to address remote interference.[196] Conversion is the "intentional exercise of dominion or control over a chattel which so seriously interferes with the right of another to control it that the actor may justly be required to pay the other the full value of the chattel."[197] Acts that fall short of conversion might qualify as trespass to chattels, the act of "intentionally (a) dispossessing another of the chattel, or (b) using or intermeddling with a chattel in the possession of another."[198] Liability attaches if the trespasser "dispossesses the other of the chattel," "the chattel is impaired as to its condition, quality, or value," "the possessor is deprived of the use of the chattel for a substantial time," or "bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest."[199] Notwithstanding the *Restatement*'s requirement that there must be "physical contact" with the property,[200] a number of courts have adopted trespass to chattels as a cause of action against digital activities, such as email spam and information-gathering software—also known as "crawlers" or "spiders."[201]

But contractual notice of remote interference will preclude these common law tort claims. Both trespass to chattels and conversion require proof that the defendant acted without the owner's consent.[202]

---

196. However, these items are increasingly licensed, rather than owned, by consumers, which creates an additional barrier to ownership-based tort claims. *See, e.g.*, FAIRFIELD, *supra* note 21; PERZANOWSKI & SCHULTZ, *supra* note 21; Mulligan, *Personal Property Servitudes*, *supra* note 13.

197. RESTATEMENT (SECOND) OF TORTS § 222 (AM. LAW INST. 1965).

198. *Id.* § 217.

199. *Id.* § 218.

200. *Id.* § 217 cmt. (e).

201. *See, e.g.*, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1070 (N.D. Cal. 2000) (granting injunctive relief on the ground that spiders likely engaged in trespass to chattels); CompuServ, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1027 (S.D. Ohio 1997) (stating that the inundation of spam email was actionable trespass to chattels); *see also* Intel Corp. v. Hamidi, 71 P.3d 296, 306–08 (Cal. 2003) (limiting recovery in similar cases to situations where the plaintiff could demonstrate either actual interference with the physical functionality of the computer system or the likelihood that such interference would occur).

202. RESTATEMENT (SECOND) OF TORTS § 256; W. PAGE KEETON, DAN B. DOBBS, ROBERT E. KEETON & DAVID G. OWEN., PROSSER AND KEETON ON THE LAW OF TORTS § 18 (5th ed. 1984). Modifying these common law torts to address remote interference would require more than extending an imperfect analogy; rather, it would require altering the consent standard, a

If the terms of service provide notice of the possibility of remote interference, defendants will argue that the consumer explicitly consented to such actions—and these arguments have proven largely successful in other contexts.[203]

Further, both torts also require a showing that the plaintiff owns or has the right to possess the personal property at issue.[204] However, at least in cases of remote interference permitted by contract, and particularly when employed as a response to a contractual breach, it is unclear whether the plaintiff has an exclusive right to the disputed property.

Other intentional common law torts also fail. Trespass to the person claims—such as battery and false imprisonment—require that the defendant intended an action, be it contact or confinement. But it is unlikely that corporate actors would act with the requisite intent. Even where a physical harm is a foreseeable result of corporate interference, IoT companies are unlikely to act with sufficient purpose or have substantial knowledge that a specific contact would ensue to support a battery claim, especially as statistical knowledge is insufficient to demonstrate intent.[205] Similarly, IoT companies are unlikely to act with the intent to confine someone, as required for a false imprisonment claim.[206] Meanwhile, although issues of trespass to land—the tort of wrongfully interfering with another's real property rights—often arise in the context of physical repossession, companies

fundamental element of these claims. For example, all cases applying trespass to chattel reasoning to digital activities emphasize the importance of the plaintiff's lack of consent.

203. *See, e.g.*, Opperman v. Path, Inc., 87 F. Supp. 3d 1018, 1053–54, 1062–63 (N.D. Cal. 2014) ("Courts in this district have interpreted 'without permission' to mean 'in a manner that circumvents technical or code based barriers in place to restrict or bar a user's access.'" (quoting Facebook, Inc. v. Power Ventures, Inc., 844 F. Supp. 2d 1025, 1036 (N.D. Cal. 2012))).

204. RESTATEMENT (SECOND) OF TORTS §§ 217, 222(A).

205. JOHN C.P. GOLDBERG, ANTHONY J. SEBOK BENJAMIN C. ZIPURSKY, TORT LAW: RESPONSIBILITIES AND REDRESS 637 (4th ed. 2016) ("A plaintiff suing for battery does not establish the defendant's intent merely by proving that the defendant *appreciated or should have appreciated* that his actions posed a *risk* of harmful or offensive contact . . . . Rather, the plaintiff must establish that the defendant *actually knew* that his actions *would cause* such contact."); *id.* at 638 ("[I]t is very implausible to infer a *purpose* to cause a harmful touching from mere statistical knowledge.").

206. RESTATEMENT (SECOND) OF TORTS §§ 13, 18, 21, 35; GOLDBERG ET AL., *supra* note 205, at 683 ("Accidental confinements, such as confinements arising out of misunderstandings, are ordinarily not actionable as false imprisonments.").

can engage in remote interference without coming onto another's land.[207]

Given these various contractual hurdles, would-be claimants will need to look to products liability and negligence, which classically have provided redress for physical harms regardless of contractual agreements. However, as described in the following two sections, rote applications of products liability and negligence standards may not sufficiently incentivize consumer safety.

B. Products Liability Problems

Modern products liability law considers how best to allocate liability for harms arising from consumer use of a product, based on what the seller can, does, or should know about the product being sold and the foreseeable uses, misuses, and extraneous harms that might arise.[208] Corporations cannot contract out of products liability claims, and these claims create a route of recourse for those not in privity with a company to bring suit, which will often be relevant in the IoT context. But while it is natural to look to products liability law to remedy harms caused by corporate remote interference, none of the three main products liability claims—that there is a manufacturing defect, design defect, or informational defect—map well onto these situations.

Certainly, existing products liability law can be applied to IoT devices.[209] As with any other product, "smart" devices can be poorly

---

207. RESTATEMENT (SECOND) OF TORTS § 329. Similarly, remote interference will not usually implicate nuisance, the tort of unreasonable interference with a person's right to the use and enjoyment of their land. *Id.* § 822. That being said, a creative court might draw on trespass and nuisance concepts to create a new common law tort to address harms arising from remote interference. *Cf.* Jack Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1165 (2018) (proposing "algorithmic nuisance," a new claim grounded on the idea that platforms should not be able to "externalize the costs of their operations onto strangers").

208. RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2(b) (AM. LAW INST. 1998); KEETON ET AL., *supra* note 202, § 98.

209. IoT devices do introduce some confusion into products liability law. While software has traditionally not been considered a product, an IoT device's integration of software with a physical object raises the issue of whether it is a component part subject to strict liability for defects. *See, e.g.*, Paez & La Marca, *supra* note 152, at 58–60; Scott, *supra* note 175. Also, it is unclear whether poor cybersecurity practices constitute a design defect or breach of implied warranty. *See* Butler, *supra* note 13 (arguing that companies could be held liable for harms caused by hacked IoT devices); Elvy, *supra* note 14, 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 U.C.C.]."); Paez & La Marca, *supra* note 152, at 56; *see also* Baker v. ADT Corp., 2015 U.S. Dist. LEXIS 180138, at *27–36 (C.D. Ill.

designed, improperly manufactured, or inadequately labeled.[210] When harm is caused by a design defect, manufacturing defect, or insufficient warning, it can be addressed under the appropriate standard.[211] Further, sellers' growing information about, access to, and control over their products could significantly expand their obligations, as sellers' increased knowledge could increase their liability for design or informational defects,[212] postsale failures to warn,[213] and even postsale failures to update.[214]

But none of these claims squarely address the possibility of a company interfering with how a device functions, either as a dispassionate policy or as a malicious act. This is hardly a manufacturing defect;[215] the possibility of remote interference is a feature, not a bug, of IoT devices. And informational-defect or failure-to-warn claims will likely fail, assuming that the terms of service notified the purchaser about the possibility of remote interference and its potential consequences.[216]

If anything, remote interference that results in harm might be considered a design defect. Design defects exist when a product is inherently dangerous or useless, because (1) it fails to meet consumer expectations regarding the product's safety, (2) it fails a risk-utility test, or (3) the risks associated with its use could have been corrected with a reasonable alternative design.

2015) (dismissing a claim of strict products liability regarding a hacked security system on the ground that it was precluded by the economic-loss doctrine).

210. For example, in *In re Toyota Motor Corp.*, 754 F. Supp. 2d 1145 (C.D. Cal. 2010), plaintiffs alleged classic products liability claims: first, that their cars had a software defect that caused them 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. *Id.* at 1192.

211. Manufacturing-defect cases tend to apply a strict liability standard; design- and warning-defect cases usually apply some variant of a negligence analysis. *See* Gifford, *supra* note 32, at 119–21.

212. Smith, *Proximity Driven Liability*, *supra* note 34, at 1802.

213. *Id.* at 1802–04 (discussing how rationales for limiting a postsale duty to warn are undermined by the increasing amount of information available to sellers about postsale product use).

214. *Id.* at 1805–08.

215. Manufacturing defects happen in the manufacturing process, often due to poor-quality materials or workmanship. *See generally* LEWIS BASS & THOMAS PARKER REDICK, PRODUCT LIABILITY: DESIGN AND MANUFACTURING DEFECTS § 4:8 (2d ed. Sept. 2018).

216. Informational defects and postsale failures to warn exist when a product has a nonobvious risk that could be lessened by an adequate warning. Most IoT contracts include notice of the possibility of remote interference. Indeed, in the context of licensed software, the law already "requires written notice of the possibility of electronic self-help." Cohen, *supra* note 12, at 1112.

For claims to succeed under the consumer-expectations test, a jury must find that the product did not function as safely as a reasonable consumer might expect.[217] Automobiles, coffee makers, and many other IoT devices do not obviously depend on the remote provision of services, and so a jury today might decide that a reasonable consumer could find certain kinds of remote interference unreasonably dangerous. However, this claim's strength depends in part on how the social norms and relevant law evolve. Even today, contractual notice of remote interference will undermine claims that the consumer did not know it was a possibility. In the longer term, it may become more commonplace for companies to affect items in our homes, which in turn may make the possibility of harmful remote interference less and less surprising—or more and more "expected."

The risk-utility test weighs a product's risk of causing harm against its expected usefulness. While this sounds objective and useful in the abstract, it is unpredictable in application when the value and damage potential of an item are both low or both high. For example, certain IoT devices, like smart fidget spinners, are neither useful nor dangerous. What would the test proscribe? Alternatively, connected automobiles, smart-home hubs, and medical devices can increase convenience or even be life-saving, but they also have a greater damage potential. Is the risk of harm worth the item's utility? Unsurprisingly, courts have tended to apply the test arbitrarily,[218] and would likely continue to do so when evaluating harms caused by corporate remote interference.

In an attempt to increase predictability, the *Restatement (Third)* endorsed the reasonable-alternative-design test.[219] To succeed, plaintiffs need to identify a design flaw and prove that a reasonable alternative design exists that would have reduced or eliminated the resulting harm, without increasing other kinds of harm.[220] Whether an alternative design is reasonable requires an assessment of a host of

217. This test, originally a misinterpretation of § 402A of the *Restatement (Second) of Torts* and rejected in the *Restatement (Third) of Torts: Products Liability*, has stubbornly persisted. Douglas A. Kysar, *The Expectations of Consumers*, 103 COLUM. L. REV. 1700, 1705–06 (2003).

218. Scott Wilkov & Elisa Arko, *No Alternative Design: An Often-Overlooked Defense to Product Liability Claims*, 2017 FOR THE DEFENSE 47, 48, https://www.tuckerellis.com/webfiles/files/DRI%20For%20The%20Defense_Wilcov%20and%20Arko_April%202017.pdf [https://perma.cc/6A3P-KDT9].

219. *Id.*; RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2 (AM. LAW INST. 1998).

220. RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 16 cmt. b. ("[T]he alternative to the product design must increase the overall safety of the product.").

factors, including its economic feasibility, its technological feasibility, and its effect on the product's longevity, maintenance, repair, and aesthetic.[221] Further, a plaintiff must show that the alternative design is an actual alternative, rather than an entirely different product, as "[g]enerally, courts are unwilling to hold manufacturers liable for a defective design when the only means of making the product safer is to alter the defining characteristic of the product."[222] For example, plaintiffs arguing that ionization smoke alarms did not provide sufficient warnings compared with smoke alarms that incorporated both ionization and photoelectric technology lost their suit; the court held that the plaintiffs' proposal was essentially a design for a different product.[223] Nor will a product be considered defective just because it was not designed as safely as possible if the proposed alternative design requires changing a fundamental characteristic.[224]

These requirements create multiple roadblocks for holding companies liable for harms resulting from remote interference. An IoT company could argue that proposed alternative designs would increase other kinds of harm, would be prohibitively expensive, would be technologically infeasible, or would essentially create a different product.[225] Further, the alternative-design standard is poorly suited to solutions which require the creation of new policies and software, as courts evaluate the design's appropriateness at the time of sale. For example, in response to the seemingly obvious claim that starter-interrupt devices should not be able to deactivate cars idling at active intersections, a starter-interrupt device designer might reasonably argue that equipping them with an ability to avoid such situations (1) would be economically infeasible, (2) would create a different product, and (3) would require the creation of new software to monitor the speed of the car at the time the device is engaged. Certainly, a court might still find in the plaintiff's favor—but it could just as easily identify precedent justifying a finding for the defendant.

Finally, all three of the design-defect tests face a similar problem: they assume a static product design, not something that can be unilaterally altered postsale. Although courts have recognized postsale

221. *Id.* § 2 cmt. f.

222. Wilkov & Arko, *supra* note 218, at 50–52 (discussing common challenges to design defect claims).

223. Hosford v. BRK Brands, Inc., 223 So. 3d 199, 206 (Ala. 2016).

224. *Id.* at 204.

225. Wilkov & Arko, *supra* note 218, at 50.

duties, they have been largely limited to a narrow duty to warn.[226] However, the *Restatement* does suggest that sellers and distributers may be liable for an unreasonable failure to provide appropriate postsale warnings when they learn of a new potential risk.[227] Accordingly, a plaintiff might argue that a company that remotely alters or curtails a device's capabilities in ways that foreseeably increase the likelihood of harm has a renewed duty to issue an updated warning.

This is, however, a rather low bar. Companies will find it easy to issue broad updated warnings, and even require users to acknowledge them to receive a needed system update, without practical effect or a significant net reduction in harm. As has been repeatedly demonstrated in the privacy-harms context, contractual provisions warning only of potential acts rarely provide effective notice.[228] Merely conditioning continued use of an item on acknowledgment of a clause stating that the company might remotely deactivate the device for any reason—including but not limited to nonpayment of subscription fees, refusal to install required updates in a timely manner, public disparagement of the product, and so on—would hardly minimize harms resulting from remote interference. Absent more stringent requirements,[229] such postsale warnings will effectively operate as a corporate liability shield.

---

226. *But see In re* Old Carco, No. 09–50002, 2017 WL 1628888, *5 (Bankr. S.D.N.Y. Apr. 28, 2017) (noting that a postsale software update that addressed one problem (a tendency of some Jeeps to shift into neutral without driver input) but created another (it disabled certain four-wheel drive capabilities) might create an independent claim, but ultimately finding this question beyond the scope of the case); Smith, *Proximity Driven Liability*, *supra* note 34 (arguing for increased postsale duties for IoT companies).

227. RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 10 (AM. LAW INST. 1998). While there was no uniform or consistent duty to warn at the time the *Restatement (Third)* was adopted, more than thirty states have since adopted various versions of this duty. *See* Tom Stilwell, *Warning: You May Possess Continuing Duties After the Sale of Your Product! (An Evaluation of the* Restatement (Third) of Torts: Products Liability*'s Treatment of Post-Sale Duties*), 26 REV. LITIG. 1035, 1037 (2007).

228. *See, e.g.*, Ignacio N. Cofone & Adriana Z. Robertson, *Consumer Privacy in a Behavioral World*, 69 HASTINGS L.J. 1471, 1506 (2018); Kirsten Martin, *Do Privacy Notices Matter? Comparing the Impact of Violating Formal Privacy Notices and Informal Privacy Norms on Consumer Trust Online*, 45 J. LEG. STUD. 191, 195 (2016); Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEG. STUD. 69, 72 (2016).

229. *See infra* Part III.B.2 (detailing potential expansions of the warning requirement).

C. Negligence Hurdles: Unclear Duties, Unclear Breaches

Would-be plaintiffs can also bring negligence claims, notwithstanding contractual terms purporting to limit them.[230] To succeed, the plaintiff would need to show that the IoT company breached a duty of care—that it had an obligation to do or not to do something, and it did not satisfy this obligation.[231] Depending on the case-specific facts and the analogies used, this standard may be difficult to meet in cases involving corporate remote interference.

The existence of a duty and its scope will necessarily depend on the scenario. The easiest case for finding a duty will be where an IoT device purports to reduce or mitigate the possibility of a physical harm, such as an IoT fire alarm or security system, and the device fails to render that service because of some act of remote interference.[232] It is less clear what duty an IoT company owes a consumer who breaches a contract—say, by attempting to jailbreak a device or failing to make a required payment.[233] It is also unclear what duty IoT companies owe consumers to ensure that their remote interference does not enable intervening sources of harms.[234]

In the absence of established duties, advocates and courts will cast about for helpful analogies, and the selection of one over another will have dramatic legal consequences.[235] Given their ability to legally

230. *See, e.g.*, Giles v. Gen. Motors Acceptance Corp., 494 F.3d 865, 874 (9th Cir. 2007) ("Whether or not the plaintiff is in a contractual relationship with the manufacturer, the plaintiff can sue the manufacturer in tort only for damages resulting from physical injury to persons or to property other than the product itself.").

231. For a negligence claim to succeed, a plaintiff must satisfy four elements: duty, breach, causation, and injury. This Section assumes an injury has already occurred and considers the question of whether a duty has been breached; the causation analysis is addressed below. *See infra* Part II.D.

232. RESTATEMENT (SECOND) OF TORTS § 323 (AM. LAW INST. 1965) ("One who undertakes . . . to render services to another . . . is subject to liability to the other for physical harm resulting from his failure to exercise reasonable care to perform his undertaking, if . . . (b) the harm is suffered because of the other's reliance upon the undertaking.").

233. "Jailbreaking" devices—altering the software or hardware that limits their use—at minimum voids warranties and at its most extreme can carry fines or even criminal charges. Digital Millennium Copyright Act, 17 U.S.C. § 1201 (2018) (criminalizing the creation or use of technologies that can disable certain architectural enforcement systems).

234. *See infra* Part II.D.1 (discussing the role intervenors play in the causal chain).

235. *Compare* Am. Broad. Cos., Inc. v. Aereo, Inc., 573 U.S. 431, 435–51 (2014) (reasoning that the Aereo streaming technology in question is best analogized to a cable system), *with id.* at 451–63 (Scalia, J., dissenting) (reasoning that the same technology is instead best analogized to a copy shop and library card). *See also* Rebecca Crootof, *Autonomous Weapon Systems and the Limits of Analogy*, 51 HARV. NAT'L SEC. J. 51 (2018) (teasing out how different analogies for autonomous weapon systems implicate entirely different legal regimes).

assume control of property or discontinue needed services, the three most obvious potential analogies for IoT companies are repossession agents, public utilities, or landlords. Accordingly, this Section considers the implications of relying on these three analogies to determine the duty IoT companies owe consumers, as well as how that duty might change should a consumer breach the contractual provisions.[236]

Repossession agents have remarkably few duties toward individuals from whom they are taking secured property. So, while it is tempting to analogize IoT companies to repossession agents in the wake of a contractual breach, doing so would support a finding that no duty was breached. Most states simply prohibit trespass or other actions that would constitute a breach of the peace.[237] Twelve states and Washington, D.C. have licensure requirements, which include additional restrictions.[238] For example, Florida bars repossession agents from carrying firearms and requires them to maintain an accurate listing of the repossessed inventory;[239] California bans the disclosure of personal information of individuals whose items have been repossessed.[240] Assuming that an IoT company's "digital repossession" does not breach the peace[241] and complies with other relevant state requirements, there is little legal incentive under the

236. As this Section concludes that these various analogies all raise problems, this Article argues for expanded corporate duties, grounded on the nature of the relationship between the IoT company and the device user. *See infra* Part III.B.2.

237. *See, e.g.*, U.C.C. § 9-609 cmt. 3 (AM. LAW INST. & UNIF. LAW COMM'N 2010) (outlining breach of the peace limitations to repossession); *supra* note 1 (citing state laws adopting this type of limitation, among others).

238. These include California, Florida, Hawaii, Illinois, Louisiana, Maine, Maryland, Michigan, Nevada, New Mexico, Oregon. and Pennsylvania. *State Requirements*, AMERICAN RECOVERY ASS'N, INC. (2019), https://repo.org/member-tools/state-requirements [https://perma.cc/JE4X-ABHB]. In other states, repossession agents must have a towing license, be bonded, or register with the state. *Id.*

239. FLA. DEPT. OF AGRIC. & CONSUMER SERVS., RECOVERY AGENT HANDBOOK 7, https://licensing.freshfromflorida.com/forms/P-00094_RecoveryAgentHandbook.pdf [https://perma.cc/4W7Y-265F]. Florida also requires repossession agents to be physically present for a repossession. *Id.* at 12. However, as this seems to presume that the primary, if only, alternative is for an unlicensed agent to carry out the repossession, *id.*, it is not clear that courts would impose this requirement when a company engages in electronic self-help.

240. CAL. BUS. & PROF. CODE § 7508.7 (2014).

241. Causing harm to defendants might constitute a "breach of the peace," if that phrase is construed liberally, and courts do have a history of reading it expansively. *See, e.g.*, *supra* note 89 (citing Connecticut and New York courts, which held that oral protest alone can constitute a breach of the peace).

repossession-agent analogy for the IoT company to take care to not cause foreseeable harms.[242]

Utility companies may also be a relevant legal analogy, particularly for IoT companies that provide an ongoing service necessary for a device's functionality.[243] Utilities have a "duty to exercise reasonable care to fulfill [their] obligation to provide continuing service,"[244] and, in recognition of the customer's dependence, they are required to provide reasonable notice of pending service terminations.[245] In evaluating the reasonableness of the notice, courts expect the utility to "take into account the likelihood of damage to the consumer"[246] and "act with the care that a reasonable person would exercise given the consequences of the shutoff."[247] Utility companies can terminate services in response to a customer's contractual violations, including nonpayment, but they cannot use the threat of discontinued service to coerce or punish customers.[248] Given users' dependence on utilities, companies cannot create and enforce arbitrary rules regarding whom they will serve.[249]

However, there are certain distinctions that limit the usefulness of the public-utility analogy. First, public utilities only have duties to those in privity: "[I]n the absence of a contract between the utility and the consumer expressly providing for the furnishing of a service for a

242. Depending on how direct the harm is, there may be nonlegal market incentives to avoid causing harm. For example, no company will remotely deactivate a pacemaker in reaction to a missed payment—aside from the ethical issues, the reputational costs would be prohibitive. However, given how technology can misdirect responsibility from remote decision-makers to those closer in time and space to the harmful incident, *see infra* Part II.D, there will be fewer market incentives to prevent the enabling of intervening sources of harm.

243. *Cf.* Nicholas Bagley, *Medicine as a Public Calling*, 114 MICH. L. REV. 57, 76–79 (2015) (arguing that, when certain industries are necessary to the public and those industries have leveraged that necessity to consumer disadvantage, governments tend to respond with public-utility-like regulation).

244. Roger D. Colton, *Prepayment Utility Meters, Affordable Home Energy, and the Low Income Utility Consumer*, 10 J. AFFORDABLE HOUSING & CMTY. DEV. L. 285, 297 (2001).

245. *See id.* at 295 ("[I]t may be argued that a utility's common law right to terminate service to enforce payment is conditional upon its duty to notify the customer of its intention to do so prior to exercising that right.").

246. *See id.* at 297 (quoting 15 STEPHEN R. PITCHER, AM. JUR. PROOF OF FACTS 2D § 125 (1978)).

247. *Id.* at 298.

248. Note, *The Duty of a Public Utility to Render Adequate Service: Its Scope and Enforcement*, 62 COLUM. L. REV. 312, 326 (1962) ("[D]iscontinuance can not be used to coerce a customer into paying a bill when there is a bona fide dispute concerning its validity.").

249. *See, e.g.*, Shepard v. Milwaukee Gas Light Co., 6 Wis. 539, 547–49 (1858) (voiding contractual terms allowing the gas company to "capriciously select" whom to serve).

specific purpose, the public utility owes no duty to a person injured as a result of an interruption of service or a failure to provide service."[250] If applied in the context of corporate remote interference, the utility analogy would not protect third-party users or bystanders. Second, precisely because they have the power to remotely terminate vital services, utilities are often public and heavily regulated industries,[251] and so there may be less of a need to impose additional liabilities on utilities than would be desirable for a private company with similar capabilities.

Should a court analogize an IoT company to a landlord, there is a greater chance that it would find a duty to minimize foreseeable harms under the IoT company's control—at least absent a contractual breach. Landlords have affirmative duties to protect the safety of their tenants. After *Kline v. 1500 Massachusetts Avenue Apartment Corp.*[252] established landlords' tort liability for a third party's criminal actions, almost all jurisdictions have found that landlords have a duty to keep common areas relatively safe, including both the physical premises and the overall environment.[253] Generally, landlords are liable for negligence when "there is a 'special relationship' between the landlord and tenant" and when "there are 'special circumstances' by which the landlord's act or omission expose[d] the tenant to an unreasonable risk

250. 53 CAL. JUR. 3D, *Public Utilities* § 149 (1979) (citing White v. S. Cal. Edison Co., 25 Cal. App. 4th 442, 435–36 (Cal. Ct. App. 1994)).

251. As one scholar has described the power that utility companies have:

> There are some firms whose control over basic necessities and infrastructure create a greater moral danger of unaccountable power than ordinary firms or businesses. . . . Public utility regulations were seen as vital for regulating those private actors operating in goods and services whose provision seemed to require some degree of market concentration and consolidation—and whose set of users and constituencies were too vast to be empowered and protected through more conventional methods of market competition, corporate governance, or ordinary economic regulation.

K. Sabeel Rahman, *The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept*, 39 CARDOZO L. REV. 1621, 1639 (2018).

252. Kline v. 1500 Mass. Ave. Apartment Corp., 439 F.2d 477, 486–88 (D.C. Cir. 1970) (allowing tenants to sue their landlord for injuries arising from a criminal assault and robbery in the common hallway).

253. *See* B. A. Glesner, *Landlords as Cops: Tort, Nuisance & Forfeiture Standards Imposing Liability on Landlords for Crime on the Premises*, 42 CASE W. RES. L. REV. 679, 682 (1992) (stating that tort standards "have evolved from narrow exceptions, to a general rule of immunity, to a broad duty of care"). This "duty to provide a reasonable amount of security in common areas extends to preventing foreseeable injuries within the leased premises as well." Catherine A. Hodgetts, *Torts*, *in The Maryland Survey: 2002-2003*, 63 MD. L. REV. 971, 971 (2004) (reviewing, among other recent decisions by the Court of Appeals of Maryland, *Hemmings v. Pelham Wood L.L.L.P.*, 375 Md. 522 (2003)).

of crime."[254] The foreseeability of the harm and the landlord's ability to control it are often determining factors in finding a duty.[255]

However, the landlord analogy may only create a duty of care for IoT companies in situations where there is no contractual breach. Should a tenant breach a lease—say, by failing to pay—landlords can evict them,[256] and landlords can often engage in self-help to do so as long as they provide the required notice and do not breach the peace.[257] It is unclear whether landlords have any other duties to minimize harm to tenants after nonpayment. For example, landlords do not have a duty to consider the implications of extreme weather[258] or to check for pets before changing the locks.[259] Applying the landlord analogy would allow IoT companies to engage in remote interference in response to contractual breaches with nearly no liability, although possibly subject to a notice requirement.

If courts took to analogies for guidance, the choice of analogy will determine the scope of the IoT company's duty. Assuming the harmed user did not breach the contract, both the utility and landlord analogies provide some basis for finding a duty of care to minimize foreseeable harms. The landlord analogy provides slightly more support for a finding that IoT companies owe a duty to everyone with whom they share a special relationship, rather than just to those with whom the companies are in privity. It also supports finding a duty to avoid

254. Glesner, *supra* note 253, at 702.

255. *See id.* at 686 (noting that, in some jurisdictions, "the landlord's liability is determined by balancing the foreseeability and reasonableness of the risk of injury against the ability of the landlord to reduce that risk"); Irma W. Merrill, *Landlord Liability for Crimes Committed by Third Parties Against Tenants on the Premises*, 38 VAND. L. REV. 431, 441 (1985) (reviewing precedential cases where courts have considered "areas that the landlord controls" and "foreseeability of the crime").

256. *See* Deborah Hodges Bell, *Providing Security of Tenure for Residential Tenants: Good Faith as a Limitation on the Landlord's Right to Terminate*, 19 GA. L. REV. 483, 538 (1985) (observing that "the most common reasons for eviction relate to the tenant's performance," including nonpayment or other violations of lease terms).

257. *E.g.*, Thomas M. Whelan, *Enforcement of Commercial Leases: Evictions and Dealing with a Tenant's Personal Property*, 3 TEX. WESLEYAN L. REV. 283, 290–91 (1997) (discussing Texas landlord–tenant statutory and contractual self-help remedies).

258. *See* Pam Fessler, *As Temperatures Fall, No Halt to Evictions Across Most of the Country*, NPR (Dec. 18, 2017, 5:00 AM), https://www.npr.org/2017/12/18/570796464/as-temperatures-fall-no-halt-to-evictions-across-most-of-the-country [https://perma.cc/PN4U-YD9X] ("A few places, like Maryland and Washington, D.C., postpone evictions when it's below freezing and over the holidays, although those places are the exception rather than the rule.").

259. Carl Campanile, *Proposed Law Hopes to Help Trapped Pets After Evictions*, N.Y. POST (Sept. 26, 2017, 4:24 PM), https://nypost.com/2017/09/26/proposed-law-hopes-to-help-trapped-pets-after-evictions [https://perma.cc/W8G7-4ZRW].

creating an environment where IoT device users are likely to be the victims of criminal acts.[260] If the consumer did breach the contract, the repossession-agent analogy will be tempting, but it suggests the IoT company owes device users nearly no duty of care. In contrast, both the utility company and landlord analogies imply the existence of a minimal duty of notice of the companies' intent to engage in responsive self-help, commensurate with the likelihood and degree of harm.

These analogies may well be appropriate for some situations where corporate remote interference causes harm, but the analogy that works in one scenario should not be blindly applied in another. Rather, the appropriate analogy for assessing IoT companies' duty toward device users and bystanders must be considered afresh with each new fact pattern—with an awareness that, in some circumstances, none of them may achieve the desired social goal.[261]

D. Seeming Breaks in the Causal Chain

Regardless of whether a suit is grounded in products liability, negligence claims, or both, a plaintiff will need to demonstrate that the IoT company's remote interference caused their harm. Corporate remote interference can cause harm in three ways: (1) directly, (2) via induced reliance which then results in harm, or (3) by enabling intervening sources of harm.

The first two categories have relatively straightforward causation analyses.[262] First, remote interference may be the direct cause of harm,

---

260. *See* Kline v. 1500 Mass. Ave. Apartment Corp., 439 F.2d 477, 482 (1970) ("In the case at bar we place the duty of taking protective measures guarding the entire premises and the areas peculiarly under the landlord's control against the perpetration of criminal acts upon the landlord, the party to the lease contract who has the effective capacity to perform these necessary acts."). Common carriers have been found to have a similar duty toward their passengers. *See* Hines v. Garrett, 108 S.E. 690, 694 (Va. 1921) ("A carrier, in the discharge of [its] very high duty . . . , is bound to know the character of the place at which it wrongfully discharges them; and if the defendant wrongfully require[s] the plaintiff to get off at a dangerous place without knowing it, it d[oes] so at its peril."); *see also* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CAL. L. REV. 1887, 1923 (2010) (noting that, where one entity creates "an unreasonable risk of criminal misconduct," it owes a duty of care toward those who will be foreseeably endangered (quoting Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1006–07 (N.H. 2003))).

261. For a discussion of other means of determining the appropriate scope of duty for corporate remote interference, see *infra* Part III.B.2 (articulating a standalone duty and various possible manifestations).

262. *See, e.g.*, Butler v. Pittway Corp., 770 F.2d 7, 11 (2d Cir. 1985) (finding that a malfunctioning smoke alarm "can create an unreasonable risk of harm" and support a products liability claim because "the inhabitants of a structure who rely on such an alarm may be lulled into an unjustified sense of safety and fail to be forewarned of the existence of a fire"); Scott &

as when an implantable medical device is remotely deactivated. Second, harm may result when a user relies on an IoT device for a critical alert or alarm, and due to remote interference, the device does not provide it. For example, in 2016, a man who passed out while driving due to low blood sugar crashed his car, suffering injuries and totaling the vehicle.[263] He filed a suit against Dexcom, alleging that its smart glucose monitoring device's alarm did not go off when his blood-sugar levels dropped.[264] IoT medical alerts, fire alarms, carbon monoxide sensors, and security systems are only useful to the extent they are functional—unexpected failures foreseeably cause harm.[265]

The third, and more complicated, situation arises where remote interference enables an intervening cause of harm. If your car is disabled while you are idling at a busy intersection, there is a higher likelihood that you will be hit by a car; if your front or garage door is remotely unlocked, there is a greater chance of burglary or assault. These situations raise questions about the proper scope of the proximate cause requirement,[266] especially as new technology often masks the influence and responsibility of remote decision-makers in enabling intervening actors. Accordingly, the rest of this Section examines the problem of intervening causes.

Fetzer Co. v. Montgomery Ward & Co., 493 N.E.2d 1022, 1029 (Ill. 1986) (holding, in a case where the failure of a fire alarm allowed a "small containable fire . . . [to] spread to engulf the entire building," that the contractor who installed the fire alarm could be found negligent and thus held liable to neighbors injured by the fire).

263. 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 [https://perma.cc/SC6Q-FD62].

264. *Id.*

265. RESTATEMENT (SECOND) OF TORTS § 324A cmt. e (AM. LAW. INST. 1965) ("Where the reliance of the other, or of the third person, has induced him to forgo other remedies or precautions against such a risk, the harm results from the negligence as fully as if the actor had created the risk.").

266. Proximate cause was originally developed to limit the scope of negligence. As Judge Cardozo wrote, "the orbit of the danger as disclosed to the eye of reasonable vigilance would be the orbit of the duty." Palsgraf v. Long Island R.R. Co., 248 N.Y. 339, 343 (1928). As products liability expands, courts are increasingly relying on proximate cause to limit the scope of liability. Where "the type of harm, manner of harm, or class of persons" harmed is unforeseeable, proximate cause shields manufacturers from liability. David A. Fischer, *Products Liability—Proximate Cause, Intervening Cause, and Duty*, 52 MO. L. REV. 547, 574 (1987). Under the risk-utility test, a "potentially dangerous product is not defective if it is reasonably safe"; under the consumer-expectations test, dangerous products "are not defective if the danger is known or obvious." *Id.* at 560. Generally, "[i]n cases of this kind, where a defective product produces an unforeseeable type of harm because of an intervening cause, proximate cause and intervening cause analyses are interchangeable." *Id.* at 562.

1. *Intervening Causes of Harm Versus Enabling Acts.* The doctrine of intervening causes applies in situations where an unforeseeable act occurs and breaks the chain of causation. In *Stahlecker v. Ford Motor Company*,[267] a woman's car failed in a remote area, and a man found, raped, and murdered her.[268] Her parents sued the car company, alleging 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."[269] Similarly, IoT companies could argue that intervening events break the chain of causation linking their possibly negligent actions to the consumers' injuries. A company may have bricked your car while you were in an intersection, but it is the other driver that hit you. They may have deactivated your door lock, but it was the burglar who assaulted you.[270]

The fact that there may be an intervening cause of harm, however, does not necessarily imply that the harm was unforeseeable—or that the entity that enabled it should not be held liable. In *Addis v. Steele*,[271] for example, the court held that an inn was liable for the injuries residents suffered in a fire set by an arsonist.[272] Although there was an intervening criminal cause of harm, the lack of an escape route created a situation where injury from a fire was foreseeable.[273] Similarly, landlords have a duty to take measures within their power to protect tenants from intervening criminal actors[274] and business owners have a

267. Stahlecker v. Ford Motor Co., 667 N.W.2d 244 (Neb. 2003).

268. *Id.* at 249–50.

269. *Id.* at 251 (quoting the district court opinion).

270. The affirmative defenses of contributory negligence, comparative negligence, and assumption of risk might partially or completely bar recovery where the individual's actions increased the likelihood of harm. Take the example of the car stranded in an intersection: an individual who left a car and was subsequently hit by another presumably knew of the hazardous nature of the situation and willingly exposed himself to it, which suggests the IoT company should not bear full responsibility for the injury.

271. Addis v. Steele, 38 648 N.E.2d 733 (Mass. App. Ct. 1995).

272. *Id.* at 438.

273. *Id.* (citing Fund v. Hotel Lenox of Boston, Inc., 635 N.E.2d 194 (Mass. 1994)).

274. *See, e.g.*, Kline v. 1500 Mass. Ave. Apartment Corp., 439 F.2d 477, 487 (D.C. Cir. 1970) ("[The landlord's] duty is to take those measures of protection which are within his power and capacity to take, and which can reasonably be expected to mitigate the risk of intruders assaulting and robbing tenants.").

duty to take reasonable measures to minimize the risk of foreseeable criminal acts.[275]

These are all examples of what torts scholar Robert Rabin has termed "enabling torts": situations where, in addition to an immediate perpetrator of harm, a plaintiff has a claim against "the individual, or more often, the enterprise, that set the stage for the suffering that unfolded. The Enabler."[276] Rabin argues that enabled torts do not depend on a relationship between the enabling defendant and the injured plaintiff; however, the existence of a relationship between IoT companies and users makes the case for liability "at least as strong if not stronger."[277]

Ultimately, if the intervening source of harm is sufficiently foreseeable, the causation requirement linking corporate remote interference to an individual's injury is satisfied; if not, the intervening source of harm breaks the chain. As discussed in the next subsection,

---

275. *See, e.g.*, Posecai v. Wal-Mart Stores, Inc., 752 So.2d 762, 766 (La. 1999) (stating that the court "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"); Hines v. Garrett, 108 S.E. 690, 695 (Va. 1921) (finding a train operator negligent for carrying a woman past her stop, as she was then raped while walking back through a bad neighborhood).

While many courts are wary of extending the *Posecai* reasoning, most reiterate its standard, and some have relied on it to find questions of fact regarding whether business owners might have reasonably foreseen harms from third parties. *See, e.g.*, Patton v. Strogen, 908 So.2d 1282, 1288–89 (La. Ct. App. 2005) (using *Posecai* as a baseline standard from which to determine liability); Williams v. State, 786 So.2d 927, 932 (La. Ct. App. 2001) (same).

276. Robert L. Rabin, *Enabling Torts*, 49 DEPAUL L. REV. 435, 437–38 (2000); *see also* John C.P. Goldberg & Benjamin C. Zipursky, *Intervening Wrongdoing in Tort: The* Restatement (Third)*'s Unfortunate Embrace of Negligent Enabling*, 44 WAKE FOREST L. REV. 1211, 1211–12 (2009) (noting that the "prevailing doctrine" in negligence law is to "recognize special rules that allow for, but also limit, remote-wrongdoer liability). "Enabling torts" might include negligent entrustment, "key in the ignition cases," premise-violence cases, hazards in the workplace cases, secondhand-smoke cases, and suits against handgun manufacturers and distributers. *See generally* Rabin, *supra* (surveying these forms of "enabling torts").

277. *Id.* at 442. *But see* Goldberg & Zipursky, *supra* note 276, at 1238–40 (arguing that liability attaches in Rabin's examples because there was a special relationship between the parties, even when one party is a stranger, creating an affirmative duty that was breached). Other "enabling torts" in the IoT context might include companies incurring liability when their weak cybersecurity practices permit third-party criminals to exploit known vulnerabilities, *see* Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1586 (2005) (suggesting elements for a prima facie case of negligent enablement of cybercrime), particularly if they permit hackers to interfere with IoT devices in ways that cause physical harm, *see* Butler, *supra* note 13, at 921–22 (arguing that the economic-loss rule should not bar recovery for such claims, as "[u]nlike defective business software or other products previously considered, the security vulnerabilities that plague IoT devices threaten damage to private property and create unique risks to innocent bystanders").

however, the foreseeability analysis may be affected by technology's tendency to obscure the role of remote decision-makers.

2. *Technology Deflects Responsibility*. Not only do IoT devices enable corporate remote interference, they also mask the role of IoT companies in enabling the resulting injuries. Technology can shift responsibility from those who make decisions at a distance to those more temporally and physically close to an accident, even when the distant decision-makers had more power to minimize its likelihood or impact.[278] This occurs in part because remote decisions are obscured by later actions[279] and in part because courts tend to find that early users of new technology assume the risks and should shoulder the resulting harms.[280] Sometimes this attribution is sensible, as when individuals involved in an accident are able to take steps to minimize a risk of harm; sometimes it is not, as when those immediate actors are presumed to have more power than they do.[281]

Given how technology can mask the role of remote decision-makers, intervening sources of harm are likely to be viewed as

278. *See* Madeleine Clare Elish, *Moral Crumple Zones: Cautionary Tales in Human Robot Interaction* 40 (Engaging Science, Technology, and Society, Working Paper, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757236 [https://perma.cc/VQS9-LP6B] (highlighting how "the human in a highly complex and automated system may become simply a component—accidentally or intentionally—that bears the brunt of the moral and legal responsibilities when the overall system malfunctions"); Molly K. Land & Jay D. Aronson, *The Promise and Peril of Human Rights Technology*, *in* NEW TECHNOLOGIES FOR HUMAN RIGHTS LAW AND PRACTICE, 1, 11–12 (Molly K. Land & Jay D. Aronson, eds., 2018) (discussing how, because technology obscures agency, it interferes with traditional human-rights enforcement mechanisms); Ryan Calo, Robots in American Law 36 (unpublished manuscript) (on file with the author) (Mar. 15, 2016) (observing that judges have a tendency to attribute liability to the person "in the loop" over a robotic system). This is particularly true for accidents resulting from design decisions, which indirectly regulate users' actions. *Cf.* LESSIG, *supra* note 45, at 133–35 (describing how regulatory "[i]ndirection misdirects responsibility," sometimes allowing a regulating entity to "get[] the benefit of what would clearly be an illegal and controversial regulation without even having to admit any regulation exists"). Nor is this a new development: early accidents involving cars and airplanes were often attributed to user error, rather than the fact that steering devices detached or engines failed. *See* Graham, *supra* note 32, at 1260–66 (discussing examples).

279. *E.g.*, Graham, *supra* note 32, at 1257 (hypothesizing that a jogger hit by an unheard hybrid vehicle would probably blame the driver, rather than the vehicle's lack of an alert noise); *id.* at 1260 (noting that, "in situations in which a third party might bring suit, responsibility for the harm may be shifted away from the technology itself and toward the user's decisions vis-à-vis the innovation").

280. *Id.* at 1260–61 ("In suits brought by users themselves, the law often regards early adopters as taking their chances with a technology. . . . [T]he definite tendency [of the law] was to assign fault to the user, rather than engage in a probing review of the technology.").

281. *Id.* (quoting an issue of the magazine *Scientific American* from 1900 to support the claim that many automobile accidents occurred when steering wheels detached from the tires).

independent and unforeseeable actors, rather than the enabled and expected side effects of remote interference. Consider the common narrative of autonomous-vehicle accidents. At the time of this writing, increasingly autonomous vehicles have been involved in a number of fender benders. Recently, a driverless shuttle bus was involved in a crash *less than an hour into its first deployment* when it failed to back up as the vehicle in front of it began reversing.[282] The following article is characteristic of how such incidents are described:

> A driverless shuttle bus being tested in Las 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, [the other car is] 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 it[s] 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."[283]

Rather than blame the designers who did not anticipate and address this common scenario or the company who deployed a shuttle incapable of interacting with human drivers, the narrative repeatedly blames the third-party operator of a delivery truck, who reasonably expected the other "driver" to move. Clearly, the delivery truck driver bears some responsibility for the accident. But even though the

---

282. James Titcomb, *Driverless Car Involved in Crash in First Hour of First Day*, DAILY TELEGRAPH (Nov. 9, 2017, 12:23 PM), http://www.telegraph.co.uk/technology/2017/11/09/driverless-car-involved-crash-first-hour-first-day [https://perma.cc/5XB2-6RPL].

283. *Id.* (emphasis added).

company and its designers could have made different business and design choices, their temporal remoteness and relative invisibility shift blame for the accident to the more immediately involved actor.

E. A Market for Unsafe Remote Interference

But won't the market solve this problem? Either consumers will purchase less safe but cheaper devices, demonstrating that the cost savings is worth the added risk, or they will forego unsafe ones, incentivizing companies to invest in developing and advertising safer products.

Unfortunately, the market for IoT devices has significant information asymmetries and failures that will prevent the invisible hand from perfecting it. First, there are the usual critiques regarding the reasonableness of assuming consumers are actually making informed purchasing decisions based on contractual terms.[284] Also, reputational harms only attach if the company name is tied to an accident, but as noted above, technology's ability to deflect responsibility from remote decision-makers can make it difficult to link an accident to a company. Further, one technology can sometimes shield another. For example, many are aware that the first autonomous vehicle to kill a pedestrian was an Uber car; far fewer know that it was a Volvo.[285] Additionally, rather than creating a market for safer products, the damage potential of some IoT devices might encourage industries to collectively downplay the risk of harm. Just as airlines

284. Often, consumers are not aware of or do not understand contractual provisions—in large part because sellers profit from consumers' confusion. *See, e.g.*, Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEG. STUD. 1, 2 (2014) ("[O]nly about one or two in one thousand shoppers access a product's EULA for at least one second, yielding an informed minority of 0.2% that is orders of magnitude smaller than the required informed minority size in realistic market settings . . . ."); Glenn Ellison & Sara Fisher Ellison, *Search, Obfuscation, and Price Elasticities on the Internet*, 77 ECONOMETRICA 427, 427–29 (2009) (finding empirical support for two ways in which online sellers' obfuscation increases their profits); Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1883–93 (2013) (arguing that consumers face structural and cognitive problems in gleaning information from contracts); Van Loo, *supra* note 171, at 1324–25 (reviewing claims that big retail shopping is marked by information asymmetries). Further, even if consumers are aware of the facts, such as the price of an item, they are often unable to accurately assess the associated risks. *See* Solove, *supra*, at 1887–88 (arguing that consumers have nearly no ability to accurately judge the consequences of sharing personal information).

285. *See, e.g.*, Wakabayashi, *supra* note 122 (noting that "the crash in Tempe will draw attention among the general public to self-driving cars . . . . and the companies advocating for it," as opposed to any particular brand).

have little incentive to market their respective safety scores to a populace with an irrational fear of crashes,[286] autonomous vehicle companies attempting to lure skeptical buyers have little incentive to highlight their comparatively low accident rates.

IoT companies' ability to evade the reputational costs that might otherwise attend accidents has two consequences, both of which encourage a market for lemons.[287] First, consumers cannot accurately judge which IoT devices and contracts are safer and therefore cannot make informed choices when selecting among products. Second, and consequentially, IoT companies that act with due care are unable to pass the costs of doing so onto consumers, which will discourage them from shouldering those costs in the absence of other legal incentives. Ultimately, the market disincentivizes corporate investment in designing and manufacturing safer IoT devices.

Granted, reputational costs will attach when an egregious act or spectacular accident can be tied to a particular IoT company. For example, Sonos is facing popular backlash and losing customers after announcing that customers who do not agree to policy changes that allow more intensive data gathering would not receive necessary software updates;[288] Tesla's stock crashed following an investigation into a fatal accident.[289]

But even a sensational story may have relatively little impact, as companies are increasingly attempting to lock consumers in proprietary ecosystems.[290] Company X's smart toaster may receive

286. Jack Linshi, *Why Airlines Don't Talk About Safety in Their Ads*, TIME (Jan. 20, 2015), https://time.com/3669161/airline-ads-safety [https://perma.cc/3UCQ-S8PB] ("Putting the 'S-Word' in slogans or commercials, airlines have found, doesn't reassure passengers—it just reminds them of the random chance of danger their next trip might bring, however slight it may be.").

287. Akerlof, *supra* note 31, at 488 (arguing that, when consumers cannot distinguish between high- and low-quality (or safe and unsafe) products, "good" products are crowded out by "bad" ones).

288. *See* Nick Whigham, *Sonos Customers React Angrily to New Privacy Policy*, NEWS.COM (Aug. 24, 2017, 8:45 AM), https://www.news.com.au/technology/home-entertainment/audio/sonos-customers-react-angrily-to-new-privacy-policy/news-story/3e088c4055685c1aed4ee5856bc353ce [https://perma.cc/ZYT7-B8ZG].

289. Lora Kolodny & Ari Levy, *Tesla Shares Drop After Report Says its Autopilot System Was Engaged During a Fatal Crash*, CNBC (May 17, 2019, 3:24 PM), http://www.cnbc.com/2019/05/17/tesla-shares-fall-on-report-autopilot-system-was-engaged-during-crash.html [https://perma.cc/98T7-YVPP].

290. *See* Patrik Fältström, *Market-Driven Challenges To Open Internet Standards* 7–8 (Global Comm'n on Internet Governance, Paper Series No. 33, 2016) (noting that many IoT companies

terrible reviews, but that might not be sufficient for someone enmeshed in Company X's network to switch to Company Y's smart toaster, given that the latter could not interact with the other items in their smart kitchen. Further, "in addition to traditional forms of lock-in, personal data introduces a form of monopoly power that deepens the connection between buyer and seller. Switching opportunities are not 'just a click away' when the competitor lacks the advantages gained from years of developing personalization and knowledge about the user."[291] These ecosystems create significant barriers to entry for market newcomers, minimizing competition that might foster the development of safer IoT devices.[292] Ultimately, in a situation defined by power and information asymmetries and high switching costs, we cannot rely on the market to produce safe IoT devices.

* * *

Regardless of one's theory of tort law, the current situation is problematic. Under a fairness theory, IoT companies are knowingly creating nonreciprocal and therefore "unfair" risks of harm.[293] IoT

---

are intentionally avoiding open designs that would permit interoperability with other companies' products). Amazon is just one of many IoT companies interested in creating a siloed ecosystem, as evidenced by the experience of one commentator:

> When you add Amazon Key to your door, something more sneaky also happens: Amazon takes over. . . . The Key-compatible locks are made by Yale and Kwikset, yet don't work with those brands' own apps. They also can't connect with a home-security system or smart-home gadgets that work with Apple and Google software. And, of course, the lock can't be accessed by businesses other than Amazon. No Walmart, no UPS, no local dog-walking company. . . . Amazon is barely hiding its goal: It wants to be the operating system for your home.

Geoffrey A. Fowler, *Amazon Wants a Key to Your house. I Did It. I Regretted It.*, WASH. POST (Dec. 7, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/12/07/amazon-wants-a-key-to-your-house-i-did-it-i-regretted-it/?utm_term=.e14e2981887e [https://perma.cc/8ULE-VS4H].

291. Chris Jay Hoofnagle, Aniket Kesari & Aaron Perzanowski, *The Tethered Economy*, 87 GEO. WASH. L. REV. 783, 841 (2019) (footnote omitted).

292. *Id.* at 840 (discussing how Google and Amazon strategically offer entry-level products at cheap prices to drive future consumer purchases and raise switching costs, thus creating barriers to entry for newer companies).

293. *See* George P. Fletcher, *Fairness and Utility in Tort Theory*, 85 HARV. L. REV. 537, 541–42 (1972) (arguing that unexcused nonreciprocal risks—where the defendant "generates a disproportionate, excessive risk of harm, relative to the victim's risk-creating activity"—unfairly shift losses); Gregory C. Keating, *Reasonableness and Rationality in Negligence Theory*, 48 STAN. L. REV. 311, 343–44 (1996) (articulating an approach that would require an enterprise to compensate those harmed by its profitable and risky activities, if those harmed do not benefit from those activities to the same extent as the enterprise, which could also justify imposing increased liability on IoT companies).

companies are also not required to make their users whole, despite the fact they bear at least partial moral responsibility for the resulting harms.[294] And, as the costs of accidents are not being appropriately allocated, the resulting harms will not be efficiently deterred.[295] How, then, should civil liability standards be changed to better achieve fairness, justice, and efficiency?

III. A CIVIL LIABILITY INFLECTION POINT

The proliferation of IoT devices has brought us to the cusp of a potential legal inflection point. Decisions made now about who should bear liability for harms resulting from remote interference will create a powerful feedback loop that will forge our future assumptions about IoT companies' obligations and consumer rights.

Just as technological development can spur legal evolution, legal defaults and tech-enabled capabilities influence social norms and expectations. Law permitted social media and e-commerce platforms to collect and monetize personal data, creating an environment where many believe personal privacy is endangered, if not already gone. Law permits e-book retailers to employ digital rights management technologies to limit how many people can share a copy, normalizing a restriction that would have been unimaginable with bound books.

---

294. Corrective-justice and civil-recourse theories also favor IoT companies bearing more liability. Under a corrective-justice theory, there are currently inadequate remedies for harms resulting from the breach of interpersonal duties. *See* JULES L. COLEMAN, RISKS AND WRONGS 320 (1992) ("Corrective justice imposes the duty to repair the wrongs one does." (emphasis omitted)). Meanwhile, under a civil recourse approach, IoT companies are inappropriately evading their responsibility for having wrongfully injured users, largely because those harmed by remote interference do not have a sufficient legal means of seeking redress. *See* John C.P. Goldberg & Benjamin C. Zipursky, *Tort Law and Responsibility*, *in* PHILOSOPHICAL FOUNDATIONS OF THE LAW OF TORTS 2 (John Oberdiek ed., 2014) ("Tort law is best understood as law that defines duties not to injure others, and that holds those who have breached such duties vulnerable to their victims' demands for responsive action.").

295. Under a Calabresian law-and-economics approach, liability should attach to the "cheapest cost avoider"—the party best suited to make the "cost-benefit analysis between accident costs and accident avoidance costs" and to act on that determination. GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 26–28 (1970). While users certainly have some limited discretion with regard to whether they breach contractual terms and how much they rely on an IoT device, this pales in comparison to the power IoT companies exercise. IoT companies commission and design devices and, by extension, control their damage potential. IoT companies also draft the terms of service, which are largely contracts of adhesion, outlining when they can engage in remote interference. IoT companies also have more information about the situation and its likely risks, as well as ultimate control as to when they choose to exert their power to remotely alter or deactivate an IoT device. Lastly, IoT companies can best spread the costs of accidents.

Today, law seems to permit IoT companies to engage in remote interference without having to bear an appropriate amount of liability for its harmful externalities.

Once social norms are established, they affect how legal questions are evaluated. If it is generally assumed that IoT companies have an obligation to avoid causing foreseeable harm, courts and other legal actors will be more likely to strike exculpatory clauses as unconscionable, find a design defect in cases regarding harms resulting from remote interference, or articulate a duty for the purpose of a negligence analysis. If not, they will not.

After reviewing prior evolutionary moments, this Part offers proposals for how our civil liability standards could evolve to better incentivize companies to protect consumers from foreseeable harms resulting from their remote interference.

A. Evolutionary Moments

The history of tort law is regularly punctuated with instances where new technologies alter social relations between entities, spurring legal evolution. The concept of ultrahazardous activities, the creation of no-fault workers' compensation and motor-vehicle insurance, and the rise of mass tort litigation can all be partially traced to underlying technological changes and accompanying social shifts. Two of the more momentous examples in American tort law are the development of modern "negligence" and the products liability revolution. In both of these situations, courts and legislatures responded to new, technologically enabled accident crises and changes in power dynamics by altering allocations of liability—in diametrically opposed ways—to better achieve social goals. These moments exemplify two possible ways forward for IoT corporate liability.

1. *The Industrial Revolution and Decreased Industry Liability*. Personal injury claims were rare in preindustrial America.[296] When someone brought a case, courts evaluated it under something akin to a strict liability standard.[297] To the extent preindustrial cases mention "negligence," the term usually entails a defendant's failure to fulfill a

296. Gifford, *supra* note 32, at 80–83.

297. HORWITZ, *supra* note 32, at 85.

duty toward a specific other, such as a shopkeeper's obligation to deliver a purchased item in good condition to the purchaser.[298]

The Industrial Revolution—and the advent of machines with "a marvelous capacity for smashing the human body"—changed everything.[299] Locomotives, automobiles, steamboats, and factory and mining machines created "an accident crisis like none the world had ever seen."[300] 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 familiar person, people were being mangled by machines whose owners they did not know—and whom they were far more willing to sue.[301]

As more and more personal injury suits were brought, courts began changing the standard under which they evaluated claims, from strict liability to the modern negligence analysis.[302] Whereas it had once been sufficient to show that the defendant caused an injury, plaintiffs now also needed to demonstrate that the defendant had not acted with reasonable care.

Scholars have posited different explanations for this shift. Edward White links the development of modern negligence to the explosion in "stranger" cases, arguing that courts had to develop a new standard to

298. *See, e.g.*, *id.* at 85–88 (discussing early nineteenth-century negligence cases, including those involving the public duty of sheriffs); WHITE, *supra* note 32, at 13, 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."). *But see* W. Jonathan Cardi & Michael D. Green, *Duty Wars*, 81 S. CAL. L. REV. 671, 700 (2008) (arguing that, prior to the Industrial Revolution, there was a "default duty of care").

299. FRIEDMAN, *supra* note 32, at 467; *see also* WITT, ACCIDENTAL REPUBLIC, *supra* note 32, at 7–8 (describing the evolution of Justice Holmes' analysis of tort law, from the individual injuries of *Brown v. Kendall*, 60 Mass. (6 Cush.) 292 (1850), to a more collective response to the injuries created by industrial progress).

300. *See* Witt, *Toward a New History*, *supra* note 32, at 694.

301. Gifford, *supra* note 32, at 89–90. Gifford also argues that a host of other social and legal shifts made bringing personal injury suits easier and more appealing. These included the emergence of deep-pocketed corporations, *id.* at 89, the creation and expansion of liability insurance, *id.* at 90–91, "the 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 81, 91–92; *see also* Witt, *Toward a New History*, *supra* note 32, at 753–54 (describing the history of the witness disqualification rule), and the appearance of a personal injury bar, Gifford, *supra* note 32, at 92–93.

302. Gifford, *supra* note 32, at 93 ("Legal scholars usually agree that the law governing personal injury claims changed from a strict liability standard in 1820 to a negligence regime by 1870.").

address the new relationship between injurer and injured.[303] Morton Horwitz and Lawrence Friedman claim that the law evolved in recognition of a need to protect fledging industries, namely factories, mines, and railroads.[304] John Fabian Witt suggests that the emergence of a fault-based liability system can be traced to the influence of "nineteenth-century political liberalism."[305] Donald Gifford attributes the rise of modern negligence liability directly to the new technology and the harms and social practices it enabled.[306] All agree, however, that this legal change resulted in a contraction of industry liability,[307] as it is far more difficult to prove that a defendant breached a duty of care than that its act caused an injury.

2. *Mass Manufacturing and an Expansion in Industry Liability*. In contrast, the rise of mass manufacturing and new transportation systems spurred the development of products liability law, which extended manufacturers' duty of care from those in privity to anyone who might foreseeably be harmed by their products. Scholars have described the resulting, primarily post-1960s shift as "among the most dramatic ever witnessed in the Anglo-American legal system"[308] and as "the most rapid and altogether spectacular overturn of an established rule in the entire history of the law of torts."[309]

---

303. WHITE, *supra* note 32, 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 . . . .").

304. FRIEDMAN, *supra* note 32, at 468; HORWITZ, *supra* note 32, at 99–100 (describing the legal change as providing "substantial subsidies for those who undertook schemes of economic development"); *see also* Gary T. Schwartz, *Tort Law and the Economy in Nineteenth-Century America: A Reinterpretation*, 90 YALE L.J. 1717, 1717–20 (1981) (describing this as the "prevailing view" and arguing that the shift to negligence was far less dramatic and intentional than Horwitz's description).

305. WITT, ACCIDENTAL REPUBLIC, *supra* note 32, at 45; *see also id.* at 45–49 (describing the difference between the strict liability and negligence standards in terms of "classical legal thought" concepts, such as separation between private and public spheres and the exercise of individual rights).

306. Gifford, *supra* note 32, at 76–77, 104–05 (concluding that the development of the negligence regime can be explained by "technology in and of itself" and resulting factors, including "the increased severity of injuries resulting from the proliferation of new machinery").

307. *See, e.g.*, HORWITZ, *supra* note 32, at 99–100 (describing the transformation of common law doctrines "to create immunities from legal liability"); Cardi & Green, *supra* note 298, at 699 (describing "duty's first doctrinal appearance . . . as a means of limiting liability").

308. George L. Priest, *The Invention of Enterprise Liability: A Critical History of the Intellectual Foundations of Modern Tort Law*, 14 J. LEGAL STUD. 461, 461 (1985).

309. William L. Prosser, *The Fall of the Citadel (Strict Liability to the Consumer)*, 50 MINN. L. REV. 791, 793–94 (1966) (footnote omitted).

Historically, consumer protections for product-caused harms were based on privity of contract: only those party to a contract of sale could bring suit for harms caused by an object.[310] As mass production and cross-country transportation increased the geographic, temporal, and contractual distance between the manufacturer of a product and the ultimate consumer, however, courts began to hold companies liable for the harms their products caused, regardless of whether there was a linking contract. In *MacPherson v. Buick Motor Co.*,[311] Judge Cardozo argued that manufacturers of products that could "place life and limb in peril when negligently made" owed a duty of care to direct consumers, their family members, and even to bystanders to anticipate and prevent likely harms caused by defective products.[312] In *Escola v. Coca Cola Bottling Co.*,[313] Judge Traynor noted in his famous concurrence: "As handicrafts have been replaced by mass production . . . the close relationship between the producer and consumer of a product has been altered. Manufacturing processes . . . are ordinarily either inaccessible to or beyond the ken of the general public."[314] And, in *Greenman v. Yuba Power Products*,[315] Judge Traynor cited his *Escola* concurrence in holding a manufacturer strictly liable for a product defect.[316] Products liability law was born.

The Industrial Revolution and the associated rise of "stranger cases" prompted courts to contract industry liability; the rise of mass production and newly distant seller–buyer relations spurred a reactionary expansion of industry liability.[317] The proliferating IoT

310. Winterbottom v. Wright (1842), 152 Eng. Rep. 402 (imposing a privity requirement to limit liability in early products liability law).

311. MacPherson v. Buick Motor Co., 111 N.E. 1050 (N.Y. 1916).

312. *Id.* at 1053; Jack M. Balkin, *The Three Laws of Robotics in the Age of Big Data*, 78 OHIO ST. L.J. 1217, 1232 (2017) (describing the scope of *MacPherson*'s holding).

313. Escola v. Coca Cola Bottling Co., 150 P.2d 436 (Cal. 1944).

314. *Id.* at 443 (Traynor, J., concurring).

315. Greenman v. Yuba Power Prods., Inc., 377 P.2d 897 (Cal. 1963).

316. *Id.* at 901.

317. Products liability law has since continued to evolve, mostly in ways that again contract industry liability. *See generally, e.g.*, James A. Henderson, Jr. & Aaron D. Twerski, *Closing the American Products Liability Frontier: The Rejection of Liability Without Defect*, 66 N.Y.U. L. REV. 1263 (1991) (discussing the evolution of products liability and asserting that liability without defect is undesirable); James A. Henderson, Jr. & Aaron D. Twerski, *Doctrinal Collapse in Products Liability: The Empty Shell of Failure To Warn*, 65 N.Y.U. L. REV. 265 (1990) (encouraging courts to develop stricter guidelines for product warning cases); James A. Henderson, Jr. & Theodore Eisenberg, *The Quiet Revolution in Products Liability: An Empirical Study of Legal Change*, 37 UCLA L. REV. 479 (1990) (pointing to changes in products liability decisions favoring defendants); Howard Latin, *"Good" Warnings, Bad Products, and Cognitive*

ecosystem and the new relationships it enables herald another potential liability inflection point.

B. Expanding Corporate Liability

We are at a crossroads. In one potential future, law will continue to shield corporations from liability for harms resulting from remote interference. In a world where IoT companies have few incentives to protect device users from the harms of corporate remote interference, consumers will come to accept that using IoT devices entails an assumption of risk, shifting their expectations even in the absence of contractual protections. In another future, where law evolves to incentivize companies to better protect consumers, societal understandings of consumer rights will evolve to create stronger default assumptions favoring consumer safety.

The remainder of this Part outlines different routes toward that second future. In some situations, it may be possible to apply existing tech-neutral doctrine more expansively. For example, implied warranties or design-defect standards could be interpreted to encompass postsale corporate actions. Alternatively, it may be clearer to explicitly articulate tech-specific restatements of existing standards. Doing so may make it easier to strengthen the unconscionability and public-policy doctrines, recognize broader relational duties, and extend proximate cause standards to address the particular issues raised by corporate remote interference.

Ultimately, given the considerable known unknowns about how various kinds of IoT devices will be integrated into our society, this Article does not purport to prescribe one single solution. Instead, it presents options that advocates, judges, and policymakers should consider when weighing precedential legal decisions during this critical but bounded regulatory opportunity.

1. *Limiting Corporate Exculpatory Clauses*. Contract law might evolve to better protect IoT-device users, either through strengthening the unconscionability doctrine or by employing public policy arguments to limit the scope of corporate exculpatory clauses.

Limitations, 41 UCLA L. REV. 1193 (1994) (considering the exculpatory effect of warnings that shift responsibility to consumers to protect themselves); Michael Rustad, *In Defense of Punitive Damages in Products Liability: Testing Tort Anecdotes with Empirical Data*, 78 IOWA L. REV. 1 (1992) (examining punitive damages in products liability and describing reform efforts).

a. *Strengthening Unconscionability Claims*. At least initially, courts may find that disclaimers of liability arising from remote interference—particularly for IoT devices that do not obviously depend on the remote provision of a service, like an automobile—are unexpected and therefore void as unconscionable.[318] Many today are startled to learn that a company can remotely boot someone's car, but that reaction is already swiftly fading as we become more accustomed to corporate remote interference. Consequently, grounding legal conclusions on the fact that remote interference is surprising is not a tenable long-term approach.[319] As we become accustomed to the fact that companies can remotely affect items in our homes, remote interference will become less and less shocking, but the consequences will remain equally harmful.

Strengthening the unconscionability doctrine would better limit the reach of exculpatory clauses in the context of corporate remote interference.[320] Many of the justifications for a limited unconscionability doctrine—that the market will solve the problem or that consumers knowingly assumed the risk—do not hold in the IoT context, as the market is unlikely to provide the information consumers would need to make informed choices about the relative risks of different products.[321] Instead, just as provisions that purport to waive liability for physical harms caused by consumer goods are presumed to

318. *See, e.g.*, Traxler v. PPG Indus., Inc., 158 F. Supp. 3d 607, 616 (N.D. Ohio 2016) ("Courts have found a term to be substantively suspect if it 'reallocates the risks of the bargain in a objectively unreasonable or unexpected manner.'" (quoting A & M Produce Co. v. FMC Corp., 135 Cal. App. 3d 473, 487 (Cal. App. Ct. 1982))); Acosta v. Fair Isaac Corp., 669 F. Supp. 2d 716, 721 (N.D. Tex. 2009) ("Contract terms which distribute risks in an unreasonable or unexpected way will be found to be substantively unconscionable."); Hartland Comput. Leasing Corp. v. Ins. Man, Inc., 770 S.W.2d 525, 527 (Mo. Ct. App. 1989) ("Only such provisions of the standardized form which . . . are unexpected and unconscionably unfair are held to be unenforceable.").

319. *See supra* Part II.B (discussing how corporate remote interference may become more commonplace, in the context of analyzing the applicability of products liability law).

320. There is a growing body of scholarship proposing reforms to strengthen the unconscionability doctrine. *See, e.g.*, Hazel Glenn Beh, *Curing the Infirmities of the Unconscionability Doctrine*, 66 HASTINGS L.J. 1011, 1034–39 (2015) (surveying recommendations for fine-tuning the doctrine, including recognizing unconscionability as a tort with punitive damages, expanding remedies to include attorney's fees, and shifting the burden of proof to the defendant); Russell Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. CHI. L. REV. 1203, 1278–90 (2003) (suggesting that unconscionability be strengthened with regard to nonsalient contract terms); Lonegrass, *supra* note 145, at 5 (noting that courts are increasingly employing a "sliding scale approach" to evaluating consumer contracts that "deemphasizes traditional, formalist markers of assent" and arguing for its expanded application).

321. *See supra* Part II.E.

be unconscionable,[322] provisions that purport to waive liability for foreseeable physical harms caused by remote interference should be as well, with a high bar for rebutting the presumption.

b. *A Public Policy Argument.* Stepping back, it is worth considering the more fundamental question of whether it is ever appropriate for IoT companies to contractually evade liability for the physical harms caused by their remote interference. For devices that create a risk of physical harm, contract law's current and much maligned legal fiction that opening a package or using a device constitutes agreement to opaque terms of service and corporate-liability limitations is no longer tenable.[323]

There are multiple arguments that exculpatory clauses contravene public policy. The right to be free from foreseeable product harms could be considered an inalienable entitlement, which cannot be contracted away.[324] From a law-and-economics perspective, honoring exculpatory clauses may inefficiently shift the duty of care away from the entity best situated to prevent, bear, or spread the costs of the injury.[325] There is also precedent for requiring companies to bear the costs of developing safer products and safer practices: the federal government requires compliance with various safety standards,[326] and

322. U.C.C. § 2-719(3) (AM. LAW INST. & UNIF. LAW COMM'N 1951).

323. Mark A. Lemley & Eugene Volokh, *Law, Virtual Reality, and Augmented Reality*, 166 U. PA. L. REV. 1051, 1135–36 (2018) ("There is a good argument that courts have stretched the definition of consent too far in the browsewrap cases generally. . . . Consent should mean informed consent with a reasonable alternative, not simply a legal acknowledgement of the existence of boilerplate somewhere."); *cf.* Tschider, *supra* note 14, at 110–11 (arguing that IoT devices "disrupt the historical informed consent model," as "[a] traditional model of prior notice followed by consent is not compatible with real-time improvements precipitated by the 'always-on' nature of pervasively connected devices").

324. *See* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1092 (1972) (discussing inalienable entitlements in property and liability rules). To the extent remote interference can be portrayed as an intentional tort or gross negligence, it will fit relatively comfortably into traditional prohibitions on contracting away liability. *See supra* text accompanying notes 159–69.

325. Applegate v. Cable Water Ski, L.C., 974 So. 2d 1112, 1114 (Fla. Dist. Ct. App. 2008) (explaining why exculpatory clauses are disfavored by public policy); *see also* Dresser Indus., Inc. v. Page Petroleum, Inc., 853 S.W.2d 505, 507–08 (Tex. 1993) (describing clauses that "relieve a party in advance of responsibility for its own negligence" as "an extraordinary shifting of risk"); RADIN, BOILERPLATE, *supra* note 26, at 138–40 (critiquing the efficiency argument for exculpatory clauses for harm caused by negligence); Burnham, *supra* note 176, at 390 (wondering, in light of the moral hazard raised by enforcement of exculpatory clauses, "if a firm has no liability, then will it take precaution against accidents?").

326. These include Federal Motor Vehicle Safety Standards ("FMVSS") and Occupational Safety and Health Act ("OSHA") safety standards. The authority for the National Highway

most states limit companies' ability to contract out of liability for physical harms.[327]

If they are not struck as void, exculpatory clauses should at least be strictly construed against IoT companies in situations where remote inference causes consumer harm. This may result in the clauses being drafted in extremely clear language that better puts the consumer "on notice of the range of dangers for which he or she assumes the risk of injury, enabling him or her to minimize the risk by exercising a greater degree of caution."[328] Finally, if judges strike or strictly construe exculpatory clauses, they should do so in a way that limits their application in other and future contracts.[329]

2. *Broadening Relational Duties*. The fact that IoT devices foster a personal and ongoing relationship between companies and users suggests that the companies have a heightened duty toward users.[330] Accordingly, this Article proposes recognizing that IoT companies have a duty to users and bystanders to refrain from engaging in remote interference that creates a foreseeable risk of physical harm or property damage. Put another way, IoT companies have a duty to only employ remote interference when it is reasonably safe to do so.[331] Arguably, this duty is merely a particularized version of a broader, extant duty of care, given that "[a]n actor ordinarily has a duty to

---

Traffic Safety Administration ("NHTSA") to promulgate the FMVSS is found in 49 U.S.C. § 301 (2018); *see also* Occupational Safety and Health Act of 1970, Pub. L. No. 91-596, 84 Stat. 1590 (codified as amended at 29 U.S.C. §§ 651–678 (2018)).

327. *See* Matthiesen, Wickert & Lehrer, *supra* note 165, at 6, 9 ("A majority of states hold that such agreements generally are void on the grounds that public policy precludes enforcement of a release of liability for harms caused by aggravated misconduct or gross negligence" and "[m]ost states will not enforce waivers intended to protect the provider against liability for gross negligence, reckless conduct, willful/wanton conduct, or intentional acts.").

328. Cox v. U.S. Fitness, LLC, 2 N.E.3d 1211, 1215 (Ill. App. Ct. 2013).

329. *See* Beh, *supra* note 320, at 1031 (noting that, rather than focusing on deterrence "to serve broader public policies beyond the case at issue," courts "tend to favor benign forms of severance of unconscionable terms").

330. *Cf.* Smith, *Proximity Driven Liability*, *supra* note 34, at 1797 ("[P]roximity will give rise to the kinds of special relationships that continue to matter in law."). For example, given that many companies now can exercise postsale control over property, IoT companies may have an attendant obligation to restrict the use of potentially dangerous property by malicious or negligent users. *Id.* at 1809.

331. *Cf.* ELLIOT F. KAYE & JONATHAN D. MIDGETT, U.S. CONSUMER PRODUCT SAFETY COMMISSION, A FRAMEWORK OF SAFETY FOR THE INTERNET OF THINGS: CONSIDERATIONS FOR CONSUMER PRODUCT SAFETY 2 (Jan. 31, 2019) ("Manufacturers and retailers of IoT devices and software should anticipate safety concerns as new capabilities are added to the IoT ecosystem or products are modified, updated or re-purposed throughout their useful lives . . . .").

exercise reasonable care when the actor's conduct creates a risk of physical harm."[332] Even so, there is utility in clearly articulating it to acknowledge the issues particular to the IoT context.

The scope of this duty will necessarily vary based on the nature of the relationship between the IoT company and device user, the likely gravity and frequency of harm, and the foreseeability of harm. Although this Article collectively refers to IoT-device designers, manufacturers, sellers, and service providers as "IoT companies," a court evaluating a claim of harm grounded in remote interference will need to disaggregate the various entities to determine the scope of their respective duties. Courts will also need to evaluate the damage potential of the IoT device on a case-specific basis, as remote interference with different IoT devices will occur at different rates and cause different degrees of harm. A deactivated Fitbit is an inconvenience; a deactivated pacemaker may be a death sentence. The damage potential of an IoT device will affect what degree of harm is foreseeable, and the expected use of an item will implicate different duties owed toward different people. IoT vehicles will be used in situations where bystanders and third parties may be harmed. IoT hairbrushes? Not so much. Ultimately, it may be sensible to employ a balancing test, as the court in *Posecai v. Wal-Mart Stores, Inc.*[333] did in a related context, suggesting that "[t]he greater the foreseeability and gravity of the harm, the greater the duty of care that will be imposed on the business."[334]

Additionally, the standard may vary depending on the social utility of the device and the corporate reason for the remote interference. If harm results from a blanket change in company policy designed to benefit the company, there should be a higher standard of care—and possibly even a rebuttable presumption of strict liability. However, a lower standard of care might be justified if the corporate remote interference is a genuine attempt to comply with new regulations or to act in the best interest of the device's users or the larger public.

Analyzing the standard of care for corporate remote interference in response to user breaches will be particularly complicated. On the one hand, breaches have built-in notice: a consumer might be assumed

332. RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 7(a) (AM. LAW INST. 2010).

333. Posecai v. Wal-Mart Stores, Inc., 752 So. 2d 762 (La. 1999).

334. *Id.* at 768.

to know that a missed payment on a subscription service will result in it being discontinued or that altering a device's hardware may incur risks or void warranties. On the other hand, because IoT companies often write and enforce their own contractual terms, purported consumer "breaches" deserve close examination. A consumer who fails to make a monthly payment on the Nest account has less justification for complaint than a consumer who is tinkering with its hardware in an attempt to limit its surveillance capabilities.[335]

This proposed duty is the mirror image of a corporate postsale duty to update a product to protect consumers from newly discovered risks. Even staunch critics of a postsale duty to update recognize it is legitimate when three requirements are met[336]: (1) "the danger the product poses [is] so extraordinary, pronounced, or special that a post-sale warning will not protect consumers";[337] (2) "the manufacturer [is] able to identify and locate product owners or users";[338] and (3) "the manufacturer [is] able to regain control of the product."[339] The same rationales would support a duty not to remotely interfere with an IoT device in a way that would foreseeably cause harm.[340] Certainly, postsale warnings alone would not prevent the harms of corporate remote interference,[341] unless they are explicit and nearly contemporaneous with the risk that spurred the warning.[342] And the IoT company can identify and locate product owners and users because it is exerting control over the product.

The remainder of this Section considers different potential manifestations of this duty, including as an implied warranty of

335. *See, e.g.*, Hill, *supra* note 48 (reporting on efforts to prevent the data of Nest users from being sent to Nest servers).

336. Smith, *Proximity Driven Liability*, *supra* note 34, at 1805–06 (describing the duty to update as "a rare duty that noted scholars have vigorously rejected and that courts have repeatedly refused to recognize, with the exceptions purportedly amounting in some cases to intellectually vacant aberrations" (quotations and footnotes omitted)).

337. Douglas R. Richmond, *Expanding Products Liability: Manufacturers' Post-Sale Duties To Warn, Retrofit and Recall*, 36 IDAHO L. REV. 7, 60 (1999).

338. *Id.*

339. *Id.*

340. Some of the strongest case law precedent for a duty to update has developed in the aviation context, where—as may be the case in the IoT context—there is both a great risk of harm and a "close and continuing relationship between [a company] and its customers." Smith, *Proximity Driven Liability*, *supra* note 34, at 1806–07.

341. *See supra* Part II.B.

342. *See infra* Part III.B.2.b.

reasonable interference, as an interference defect under products liability law, and as an IoT-specific informal fiduciary duty.

a. *An Implied Warranty of Reasonable Interference*. Courts might create a common law implied warranty of reasonable interference, prohibiting IoT companies from engaging in remote interference that results in foreseeable harm either as an element of a breach of contract claim or as part of a negligence claim. Implied warranties are a "contorts" solution to a "contorts" problem[343]: they are "a curious hybrid, born of the illicit intercourse of tort and contract—a contractual term promising quality but imposed by law rather than agreement."[344]

There are already a number of common law implied warranties. As discussed above, implied warranties of merchantability and fitness for a particular purpose accompany sales of goods.[345] Others attach to the provision of services. Most states have some version of an implied warranty of good workmanship, though they differ on whether this warranty sounds in contract law or negligence.[346] Some courts have found that architectural design–build contracts have an implied warranty "of the sufficiency of the plans and specifications for the contemplated purpose."[347] Residential leases are considered sales of both shelter and services and have implied warranties of habitability.[348]

---

343. Implied warranties, such as the implied warranty of good workmanship, are sometimes evaluated under contract law and sometimes under tort law. *See* Amica Mut. Ins. v. Abar Dev., LLC, No. CV095032593S, 2013 WL 1800453, at *3 (Conn. Super. Ct. Apr. 3, 2013) (stating that the claim was "based on a breach of a contract and not brought independently outside of that context"); Milau Assoc., Inc. v. N. Ave. Dev. Corp., 368 N.E.2d 1247, 1250 (N.Y. 1977) (discussing the contractual implied warranty of good workmanship as part of a negligence claim); Melody Home Mfg. Co. v. Barnes, 741 S.W.2d 349, 353 (Tex. 1987) (noting that warranties, often designated as elements of contract law, are not so easily categorized, and that "implied warranties are created by operation of law and are grounded more in tort than in contract").

344. Debra L. Goetz, Kathryn L. Moore, Douglas E. Perry & David S. Raab, *Article Two Warranties in Commercial Transactions: An Update*, 72 CORNELL L. REV. 1159, 1190 (1987).

345. *See supra* note 190 and accompanying text.

346. *See supra* note 343 and accompanying text.

347. Robert M. Hanlon, Note, *Implied Warranties in Service Contracts*, 39 NOTRE DAME L. REV. 680, 687 (1964); *see also* Kishwaukee Cmty. Health Servs. Ctr. v. Hosp. Bldg. & Equip. Co., No. 80 C 1850, 1988 U.S. Dist. LEXIS 2671, at *24 (N.D. Ill. Mar. 28, 1988) (stating, under Illinois law, even if "an architect does not warrant its services . . . an implied warranty can attach to the sale of a product by a design/builder").

348. *See, e.g.*, Park W. Mgmt. Corp. v. Mitchell, 391 N.E.2d 1288, 1293 (N.Y. 1979) (describing how a residential lease is a sale of "shelter and services" and carries three implied warranties: "first, that the premises are fit for human habitation; second, that the condition of the premises is in accord with the uses reasonably intended by the parties; and, third, that the tenants are not

While these common law implied warranties do not directly address harms arising from remote interference with IoT devices,[349] they provide a blueprint for an implied warranty of reasonable interference.

The creation of a new implied warranty is often justified on the grounds that the common law must evolve to keep up with changing relationships to "reflect the realities of present day society."[350] Implied warranties tend to arise where, as here, there is an uneven relationship between the contracting parties—where one occupies a position of dependence or vulnerability or the other has superior information or control and enjoys a position of (possibly unwarranted) trust.[351] Relevant considerations include whether one party has induced the reliance of the other on the former's skill or knowledge, is better situated to minimize the likelihood of harm, or is better able to distribute the loss of accidents.[352] These factors all weigh in favor of creating an implied warranty of reasonable interference, which would establish liability for harms experienced by owners, users, and bystanders.[353]

Breach of warranty claims for bundled good/services products often flounder at the predominance test, which distinguishes warranties that attach to goods from warranties that attach to

subjected to any conditions endangering or detrimental to their life, health or safety"); David A. Super, *The Rise and Fall of the Implied Warranty of Habitability*, 99 CALIF. L. REV. 389, 394 (2011) (noting that nearly all jurisdictions have adopted the implied warranty of habitability in rental agreements).

349. Elvy, *supra* note 14, at 114–17 (discussing why extant implied warranties generally do not apply to IoT devices and IoT companies).

350. Green v. Superior Court, 517 P.2d 1168, 1170 (1974); *see also id.* at 1169 (creating an implied warranty of habitability for residential leases based on the "realities of the modern urban landlord-tenant relationship").

351. Deborah A. DeMott, *Breach of Fiduciary Duty: On Justifiable Expectations of Loyalty and Their Consequences*, 48 ARIZ. L. REV. 925, 934–35 & n.46 (2006) (describing scholars' articulations of the characteristics of fiduciary duties); *id.* at 936–38 (describing various factors courts have considered in determining whether "a particular relationship warrant[s] the imposition of fiduciary duties").

352. Goetz et al., *supra* note 344, at 1190 n.185.

353. The U.C.C. extends express and implied warranties to bystanders and other third parties "who may reasonably be expected to use, consume or be affected by" a product. U.C.C. § 2-318 (AM. LAW INST. & UNIF. LAW COMM'N 1951). Two of the three U.C.C. categories of protected bystanders have no privity requirement, and while the third is limited to a buyer's family or guests, some courts have nonetheless applied it to employees and bystanders. Jennifer Camero, *Two Too Many: Third Party Beneficiaries of Warranties Under the Uniform Commercial Code*, 86 ST. JOHN'S L. REV. 1, 21–23 (2012).

services.[354] An implied warranty of reasonable interference should dispense with this increasingly artificial distinction and focus instead on whether the underlying harm was reasonably foreseeable and preventable.[355]

Ultimately, however, the creation of an implied warranty of reasonable interference may only be a temporary solution. Even if it is nonwaivable and not subject to disclaimers,[356] and even if the contractual standard is lower than the common law version, courts often defer to contract terms and find express warranties supersede implied ones. Accordingly, if an implied warranty is created, IoT companies will undoubtedly respond by including explicit and less onerous warranties in their terms of service.

b. *Interference Defects*. Because IoT devices are products, it is natural to look to products liability law to address their associated problems. But for products liability law to be applicable, courts may need to develop a new kind of claim. As discussed above, products liability law developed in the context of a changed relationship between companies and consumers. Design defects, manufacturing defects, and informational or marketing defects can be understood as identifying different kinds of relationships between consumers and entities in the products supply chain, where each actor has a different standard of liability for kinds of caused harm. None of these squarely addresses the new kind of relationship between IoT companies and

354. Ellen Taylor, *Applicability of Strict Liability Warranty Theories to Service Transactions*, 47 S.C. L. REV. 231, 252 (1996) (describing the predominant-purpose test as one which determines whether the U.C.C. applies to contracts for both goods and services by asking "whether [the contracts'] predominant factor, their thrust, their purpose, reasonably stated, is the rendition of service, with goods incidentally involved (e.g. contract with artist for painting) or is a transaction of sale with labor incidentally involved (e.g. installation of a water heater in a bathroom"); *see, e.g.*, Elvy, *supra* note 14, at 105–12 (discussing the predominant-purpose test in the IoT context).

355. In determining that U.C.C. implied warranties attached to utility services, one court argued that "implied warranties, as defined by the courts of this state, should apply to the sale of services as well as to the sale of goods. We see no reason upon which a logical distinction can be based . . . ." Buckeye Union Fire Ins. v. Detroit Edison Co., 196 N.W.2d 316, 317 (Mich. Ct. App. 1972); Taylor, *supra* note 354, at 264 ("To the extent that implied warranties are intended to protect consumers, there is no clear basis for treating purchasers of goods differently from purchasers of services.").

356. The implied warranty of good workmanship recognized in Texas, for example, is nonwaivable and cannot be disclaimed. Richard M. Alderman, *Warranty Disclaimers and the Texas Deceptive Trade Practices Act*, HOUS. LAW., Jan.–Feb. 1992, at 14. But see Centex Homes v. Buecher, 95 S.W.3d 266, 273 (Tex. 2002) ("The implied warranty of good workmanship serves as a 'gap-filler' or 'default warranty'; it applies unless and until the parties express a contrary intention.").

consumers, where the company has a postsale ability to remotely alter how a device functions based on its ongoing surveillance of the user.

Given this context, courts might delineate "interference defects" as a fourth kind of products liability claim. An interference defect would exist when remote interference renders a device inherently dangerous, either because it directly harms someone, deactivates a relied-upon critical service, or foreseeably enables an intervening source of harm.[357] Interference defects might be evaluated under a strict liability or negligence standard and have compensatory and specific-performance remedies.[358]

Additionally or alternatively, courts could explicitly recognize that remote interference necessitates more extensive warning requirements than are currently required. For example, Connecticut is unique in that it prohibits electronic self-help, unless a "debtor separately agrees to a term . . . authorizing electronic self-help that requires notice of exercise."[359] This requirement addresses the need for near-contemporaneous notification and creates an opportunity for engagement and negotiation between the parties.[360] Similarly, IoT

357. Under this definition, an "interference defect" would cover harms arising from the actions of both IoT companies and criminal hackers. A more limited definition, focused only on corporate remote interference, could also be employed.

358. Historically, courts have been reluctant to require specific performance of personal services, both because of the difficulty in evaluating how well a service is performed, *see* Alan Schwartz, *The Case for Specific Performance*, 89 YALE L.J. 271, 293 (1979) ("Courts, in enforcing the supervision defense, are concerned with their inability to supervise performance . . . ."), and because orders limiting personal freedoms are uncomfortably similar to creating an involuntary servitude, *see* Nathan B. Oman, *Specific Performance and the Thirteenth Amendment*, 93 MINN. L. REV. 2020, 2023 (2009) (rejecting the conventional wisdom that specific performance violates the Thirteenth Amendment's prohibition on involuntary servitude). These concerns are less applicable in the IoT 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. As with public utility services, these fungible services can be compelled. *Cf. The Duty of a Public Utility To Render Adequate Service: Its Scope and Enforcement*, *supra* note 248, at 329 (noting that mandamus actions can be used to compel restoration of utility services).

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 employees. Schwartz, *supra*, at 297 ("[R]equiring a sizable corporation that renders services to perform for a given promisee 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 less reasonable.

359. CONN. GEN. STAT. § 42a-9-609 (2012).

360. *Id.* ("Before resorting to electronic self-help . . . the secured party shall give notice . . . stating: (A) That the secured party intends to resort to electronic self-help . . . on or after fifteen

companies could be required to alert consumers when they intend to engage in remote interference that might result in harm, with the timing and strength of the warning designed with awareness of the damage potential of the act. If the remote interference has been triggered by a user's contractual breach, an alert could state the nature of the breach and provide a means of contacting the company so the user has an opportunity to dispute the claim and address mistakes.[361] This would alleviate some of the concerns about algorithmic enforcement limiting opportunities for interaction and otherwise providing insufficient due process.[362]

Acknowledging a new "interference defect" claim or a heightened duty to warn might be the best way to address most run-of-the-mill injuries caused by remote interference. To deter hidden or explicit abusive action, however, courts might want to consider a third option: raising the moral bar for IoT companies by finding that they have an informal fiduciary duty to device users.

c. *IoT Fiduciaries*. Tort law has long premised certain duties, particularly those regarding the sharing of personal information, on legally defined relationships. Doctors, therapists, accountants, and lawyers are all commonly recognized as fiduciaries—entities who have a "position of superiority or influence [over another], acquired by virtue of [a] special trust."[363] In addition to these "formal" fiduciary relationships, courts often find that "informal" fiduciary relationships exist where "a relationship of 'trust' exists and that one party dominates, is superior to, or is especially vulnerable to another

---

days . . . ; (B) The nature of the claimed breach . . . ; and (C) [A representative's contact information].").

361. *Cf.* Rory Van Loo, *The Corporation as Courthouse*, 33 YALE J. ON REG. 547, 560–62 (2016) (describing how customer-service departments address the vast majority of industry–consumer disputes and the importance of ensuring appropriate procedures to meet both businesses' and consumers' needs).

362. For a discussion of the underlying values of due process, see Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 20 (2014) ("[T]he underlying values of due process—transparency, accuracy, accountability, participation, and fairness—should animate the oversight of scoring systems . . . ." (footnote omitted)). *See generally* Citron, *supra* note 80 (arguing that administrative adoption of algorithmic decision-making threatens traditional due process rights).

363. Tornado Techs., Inc. v. Quality Control Inspection, Inc., 977 N.E.2d 122, 126 (Ohio Ct. App. 2012) (quoting Nichols v. Schwendeman, No. 07AP–433, 2007 WL 4305718, at *3 (Ohio Ct. App. Dec. 11, 2007)).

party."[364] Thanks to the flexible nature of fiduciary law,[365] scholars regularly build on the concept to suggest new duties in relationships characterized by power, trust, and vulnerability.[366]

To the extent there is a bedrock requirement for finding a fiduciary duty, it is that there must be a relationship between the parties characterized by "high levels of trust" and in which one party is "in a position of domination, inferiority, or vulnerability."[367] Further, "[t]he *degree* of control, complexity, and dominance or the broad range of the underlying relationship can also help direct courts in figuring out how strictly to enforce fiduciary duties and how to impose a proper remedy."[368]

When consumers are particularly vulnerable and the risk of harm is significantly high, courts could recognize an informal fiduciary relationship that justifies a heightened duty of care.[369] Individuals

---

364. Ethan J. Leib, *Friends as Fiduciaries*, 86 WASH. U. L. REV. 665, 672 (2009). In *Bazan v. Muñoz*, 444 S.W.3d 110, 118 (Tex. Ct. App. 2014), the court explained:

> [I]nformal fiduciary relationships may arise when one person trusts and relies upon another, whether the relationship is moral, social, domestic, or merely personal. Because not every relationship involving a high degree of trust and confidence rises to the stature of a formal fiduciary relationship, the law recognizes the existence of [informal fiduciary] relationships in those cases in which influence has been acquired and abused, in which confidence has been reposed and betrayed.

Id. at 118 (citation omitted).

365. *See* Harper v. Adametz, 113 A.2d 136, 139 (Conn. 1955) ("[E]quity has carefully refrained from defining a fiduciary relationship in precise detail and in such a manner as to exclude new situations.").

366. For examples of scholarly articles that call for expansion of fiduciary duties, see generally Evan J. Criddle, *Fiduciary Foundations of Administrative Law*, 54 UCLA L. REV. 117 (2006); 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 (2013); Leib, *supra* note 364; and Elizabeth S. Scott & Robert E. Scott, *Parents as Fiduciaries*, 81 VA. L. REV. 2401 (1995). *But see generally* Larry E. Ribstein, *Are Partners Fiduciaries?*, 2005 U. ILL. L. REV. 209 (calling for limitations on the expansion of fiduciary duties).

367. Leib, *supra* note 364, at 672; *see also* Hafemeister & Porter, *supra* note 366, at 545–46 (discussing the vulnerability of the beneficiary).

368. Leib, *supra* note 364, at 682–83 (emphasis in original).

369. *See* DeMott, *supra* note 351, at 926 (arguing that the law of fiduciary duties can best be understood as applying in circumstances where there is a justifiable expectation that one "actor's conduct will be loyal to the interests of another").

This would complement Jack Balkin and Jonathan Zittrain's proposed "information fiduciary" concept. IoT companies would certainly qualify as "information fiduciaries"—entities "who, because of their relationship with another, [have] taken on special duties with respect to the [customer data] they obtain in the course of the relationship." Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1209 (2016); Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain To Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346 [https://

relying on implantable medical devices that regulate necessary life functions; individuals relying on fire alarms, carbon monoxide monitors, and other critical alert systems; and individuals using cars and other items with the capacity to cause significant physical harm must all trust IoT companies to avoid an ill-timed remote interference. In these and similar situations, notice of the possibility of remote interference would not be sufficient to prevent harm; instead, recognizing these companies as IoT fiduciaries would encourage them to take more affirmative action to minimize foreseeable harms.[370]

Given that breaches of fiduciary duties can be addressed with both compensatory and punitive damages,[371] a fiduciary framing would be useful in addressing abusive self-help practices or other misuses of power. Certainly, the Garadget company owner—who bricked a customer's internet-connected garage door opener in response to a bad Amazon review[372]—violated even the weakest version of a duty of loyalty.[373] And a duty of loyalty might also prohibit using remote interference to limit a device's abilities with the aim of increasing sales or otherwise enriching the corporation,[374] holding devices hostage to extort preferable terms, or using data gathered to strategically time inconvenient or dangerous remote interferences.

3. *Extending Causation*. Regardless of how a duty not to engage in remote interference that creates a foreseeable risk of harm is

---

perma.cc/E98D-KYWN]; *see also* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 103 (2004) ("I posit that the law should hold that companies collecting and using our personal information stand in a fiduciary relationship with us.").

Under the information fiduciary model, IoT companies would have a duty to refrain from using data gathered by IoT devices to enrich themselves at the expense of device users. However, as these duties are limited to data-related harms, recognizing that IoT companies are information fiduciaries will not address the range of physical harms they may cause. Similarly, doctors are information fiduciaries—they have a duty not to use patient data to enrich themselves at their patients' expense—but a doctor's fiduciary role toward patients is hardly limited to protecting their information.

370. *See* Leib, *supra* note 364, at 674–75 ("Although the [fiduciary] duty resembles a basic requirement to avoid negligence, the duty is flexible and can require more substantial diligence than would be required of non-fiduciaries." (footnote omitted)).

371. DeMott, *supra* note 351, at 930.

372. *See supra* text accompanying notes 104–06.

373. While the duty of loyalty is a core fiduciary duty, "the strictness with which it will be enforced varies, depending on the type and scope of the fiduciary relationship at issue." Leib, *supra* note 364, at 674.

374. *See* Mullis, *supra* note 102 (reporting on how Apple pushed an update that slowed older iPhones, leading some to allege that the aim was to increase sales of newer versions).

articulated, courts must also apply a causation standard that acknowledges how companies' remote decisions can increase risks to consumer safety.

As noted above, identifying a causal link between corporate action and a resulting harm will be relatively straightforward where remote interference is the direct cause of harm or where an IoT company induced the user's reliance on a service or device and then, due to remote interference, failed to provide it. Intervening causes of harm and situations where the technology masks the remote decision maker's responsibility, however, test the current boundaries of the proximate cause limitation.

In light of the ongoing relationship between IoT companies and their device users, situations where remote interference enables harmful intervenors should be evaluated under an expansive proximate cause standard. Not only is the IoT company the entity best situated to have prevented the injury,[375] but intervenors will often be difficult to find or judgment proof, and the law's "deterrence rationale would be defeated if those enabling wrongdoing can escape judgment by shifting liability to individuals who cannot be caught and thus deterred."[376] Doing so would not unduly stretch the proximate cause analysis. At least where the defendant has a special relationship with the harmed individual that gives rise to an affirmative duty,[377] courts are increasingly comfortable expanding causation standards to encompass situations where a defendant "paved the way for the third party to injure another,"[378] even when that third-party intervenor is a criminal actor.[379]

375. *See, e.g.*, Rabin, *supra* note 276, at 444 (discussing how, in the context of apartment buildings, the enabler is in a better position than the victim to diminish the risk of foreseeable harm).

376. Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1836 (2010) (citing Rabin, *supra* note 276, at 444).

377. Goldberg & Zipursky, *supra* note 276, at 1238–40, 1243.

378. Citron, *supra* note 376, at 1836; *see also* Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1007 (N.H. 2003) (recognizing a "special circumstances" exception where "a duty is owed to those foreseeably endangered" if a party "create[s] an unreasonable [and foreseeable] risk of criminal misconduct"); RESTATEMENT (SECOND) OF TORTS § 302B cmt. e (AM. LAW INST. 1965) (discussing responses to criminal misconduct); Rabin, *supra* note 276, at 441–42 (observing that the erosion of the proximate cause limitation "can be regarded as a temporal shift in moral sensibilities from a more individualistic era to one in which tort law . . . increasingly reflects more expansive notions of responsibility for the conduct of others").

379. *See, e.g.*, Kline v. 1500 Massachusetts Avenue Apartment Corp., 439 F.2d 477, 483 (D.C. Cir. 1970) (evaluating causation and liability in the criminal context).

Expanding the proximate cause analysis does not entail doing away with it entirely. There will be many fact patterns with intervening causes that break the chain of causation, or at least weigh against the company bearing full liability.[380] And, just as proximate cause can be used to avoid underdeterrence, "judges ought to use proximate cause to avoid overdeterrence. They should also restrict liability in cases involving the kinds of losses that the public would not want to spread and involving the kinds of accidents that . . . liability is not likely to deter."[381] What is important, however, is that causation in these cases is evaluated with an awareness of how remote interference can enable certain intervenors and how technology can deflect responsibility from remote decision-makers.

C. Implementation

IoT companies' power over device users and bystanders highlights the need for regulatory intervention.[382] For simplicity's sake, this Article has implicitly assumed that courts would take the lead in expanding corporate liability. However, they are far from the only legal actors who can implement this Article's proposals.[383] This final Section teases out some of the respective institutional strengths and limitations of the judicial, legislative, and agency rulemaking processes and of lawmaking at the state and federal levels.

1. *Judicial, Legislative, and Agency Rulemaking*. In many ways, the common law is well suited to address harms resulting from remote

380. *See* Goldberg & Zipursky, *supra* note 276, at 1221–23 (providing examples of practical limits on enabled torts, such as the fact that car manufacturers have no duty to instruct dealers to refrain from selling to incompetent drivers, even though it is foreseeable that such drivers will purchase cars).

381. Fischer, *supra* note 266, at 582.

382. *Cf.* Rahman, *supra* note 108, at 240 (arguing that similar power imbalances in other contexts "justified regulatory interventions to redress issues like fraud, barriers to access, information asymmetries, and bargaining disadvantages").

383. Common law tort concepts are often relatively tech-neutral standards that have stood the test of time; given this, legislatures and agencies regularly draw on tort principles as a guide for more tailored rulemaking. For example, a draft bill was proposed in the Senate that responded to the Facebook Cambridge Analytica scandal and drew heavily on the tort law concept of fiduciary duties to articulate what duties information platforms owe their users. The bill died in the 115th Congress and has not been renewed. *See* Data Care Act of 2018, S. 3744, 115th Cong. § 3(a) (2d Sess. 2018), https://www.congress.gov/bill/115th-congress/senate-bill/3744/text [https://perma.cc/Z96H-SMA7] ("An online service provider shall fulfill the duties of care, loyalty, and confidentiality . . . .").

interference.[384] While delayed and reactive, common law legal evolution ensures that problems are addressed as they arise, avoiding limiting potentially beneficial innovation through early and overbroad rulemaking.[385] Individual plaintiffs bring tort suits in response to the harms that matter to them.[386] Courts are able to review situations on a case-by-case basis and calibrate liability to the device, its damage potential, the nature of the relationship between the IoT company and consumer, the foreseeability of harm, and the actual amount of harm caused. Meanwhile, the potential breadth of common law torts incentivizes industry to consider all of the harms a new technology might cause, rather than only those identified in an agency's mandate.[387] While an agency may have limited claims it can consider, common law judges must evaluate all complaints that come before them. And while an agency is subject to regulatory capture, a common law judge is relatively independent.

Ideally, over time, the common law will "work itself pure."[388] However, tort law will only evolve rigorously if these cases make it to court, and there are a host of legal and practical barriers that will prevent them from doing so. Should IoT companies engage in remote interference without notice, users may not even know their device has been modified. Technology's tendency to misdirect responsibility away from remote decision-makers likely affects which entities people blame for harms resulting from remote interference.[389] Injured individuals may also be deterred by high litigation costs or an assumption that

384. *See, e.g.*, Mary L. Lyndon, *Tort Law and Technology*, 12 YALE J. ON REG. 137, 162–63 (1995) (enumerating the benefits of tort's case-specific method for addressing harms caused by new technologies); Douglas A. Kysar, *The Public Life of Private Law: Tort Law as a Risk Regulation Mechanism*, 9 EUR. J. RISK REG. 48, 65 (2018) (arguing that courts are uniquely well suited to evaluating whether an action violates a plaintiff's common law entitlement to be free from wrongful injury).

385. Of course, common law responses to particular situations can sometimes create rules that are overbroad or inappropriate when applied in others.

386. Hoofnagle et al., *supra* note 291, at 171 ("Perhaps the most attractive feature of using private law is that harmed consumers will be in the best position to advocate for themselves, rather than relying on the government to acquire information about various harms and regulate companies accordingly.").

387. Lyndon, *supra* note 384, at 163.

388. Richard A. Epstein, *Cybertrespass*, 70 U. CHI. L. REV. 73, 73–74 (2003) ("[N]ew forms of technology create . . . new forms of resource use, [which] might not map well with the existing framework of property rights. A common law system . . . should be able to respond to these changes both by preserving what makes sense in the older system and by changing what does not.").

389. *See supra* Part II.D.

potentially void contractual terms are enforceable.[390] Given that many harms caused by remote interference may be relatively minor, class action suits may be the only means by which consumers could affordably bring the kinds of complaints that would allow the relevant common law to develop. But courts often enforce mandatory predispute arbitration clauses that eliminate the right to a jury trial and aggregate remedies, such as class action suits.[391] Even if some plaintiffs win suits or arbitrations challenging certain contract provisions, nondisclosure provisions may mean that other potential plaintiffs never learn that certain terms are unenforceable; furthermore, contract damages in the relatively few successful cases may not be sufficiently high to deter companies from continuing to employ these generally lucrative terms.[392] Finally, as tort law provides only ex post and imperfect remedies, an overreliance on a tort law solution may result in a societal failure to avoid foreseeable harms that will dramatically impact individual lives.[393]

Furthermore, while courts may be good at calibrating liability in individual cases, they may not be the best institutions to weigh the varied social concerns raised by IoT devices.[394] For example, increasing

390. RADIN, BOILERPLATE, *supra* note 26, at 145; *see also* Meirav Furth-Matzkin, *On the Unexpected Use of Unenforceable Contract Terms: Evidence from the Residential Rental Market*, 9 J. LEG. ANALYSIS 1, 8–10 (2017) (discussing how landlords regularly include deceptive and clearly invalid terms in their contracts, which significantly affects tenants' decisions to forgo valid legal rights and claims); Charles A. Sullivan, *The Puzzling Persistence of Unenforceable Contract Terms*, 70 OHIO ST. L.J. 1127, 1133 n.22 (2009) ("[I]nvalid [contractual] terms continue to be used by those who are well aware that they are unenforceable as written, presumably because . . . the other party to the contract . . . either does not realize the clause is unenforceable as written or is not willing to risk the resources needed to establish its invalidity.").

391. RADIN, BOILERPLATE, *supra* note 26, at 143. Arbiters also tend to be more deferential to contractual language, further limiting the reach and import of tort law. *See* Alan Scott Rau, *The Culture of American Arbitration and the Lessons of ADR*, 40 TEX. INT'L L.J. 449, 451–52 (2005) (focusing on the contractual nature of arbitration and the freedom of parties to make private choices about how to resolve their disputes); *see also* Joshua D.H. Karton, *The Arbitral Role in Contractual Interpretation*, 6 J. INT'L DISPUTE SETTLEMENT 1, 2–3 (2015) (discussing this in the international arbitration context). Further, 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. Radin, *Regulation by Contract*, *supra* note 26, at 143.

392. RADIN, BOILERPLATE, *supra* note 26, at 145.

393. *Cf.* Kysar, *supra* note 384, at 20 ("Legislative and regulatory approaches may work well on a prospective, industry-wide or economy-wide basis, but they often contain no compensatory provisions at all for those particular parties who have suffered or will continue to suffer.").

394. *Cf. id.* (noting that judges are often considered "normatively inappropriate decision makers for the sensitive societal tradeoffs involved in . . . safety decision making"); Hoofnagle et al., *supra* note 291, at 171 ("[P]rivate law is limited in the sense that it does little to prevent the macro, economy-wide effects of tethering, such as the competitive drain caused by lock-in.").

liability will incentivize IoT companies to take more safety precautions, but it will also justify additional corporate surveillance.[395] Alternatively, there may be situations where a connected device has information that the user is incapacitated or intends to commit an illegal act—say, a car might recognize that its driver is inebriated—and depending on what social values we privilege, we may prefer that the device does not operate.[396] Increasing corporate liability may chill innovation, but a light chill may be warranted if the alternative is significant risk to consumers' safety. A legislature or administrative agency is far better suited to hosting a public discussion and balancing competing social goals than a court considering the facts of a single (and possibly exceptional) case.

Legislatures and agencies also have institutional strengths for developing the law of corporate remote interference. Legislative action to protect consumers is particularly effective when harms are diffuse and small, imposed on a large number of people, and cannot be attributed to a single source.[397] This will often occur in the IoT context. Meanwhile, agencies can develop specialized knowledge and expertise, allowing them to address problems that arise with regard to a particular technology or its use.[398] If their mandate is sufficiently broad, agencies can address harmful conduct that would not be covered under existing tort law.[399] They can remedy some of the information asymmetries inherent to ex post tort litigation by requiring companies to disclose information, and more expansive definitions of harm allow agencies to take action to curb various kinds of corporate overreach and unfair,

395. *See* Eugene Volokh, *Tort Law v. Privacy*, 114 COLUM. L. REV. 879, 881–83 (2014).

396. *See* Smith, *Proximity Driven Liability*, *supra* note 34, at 1809 (suggesting that IoT companies may have an obligation to restrict the use of potentially dangerous property by malicious or negligent users, as "a company's ongoing control over a product could imply a commensurate responsibility to restrict, by contractual or technological means, access by those clearly incompetent to handle it").

397. Susan Rose-Ackerman, *Product Safety Regulation and the Law of Torts*, *in* PRODUCT LIABILITY AND INNOVATION: MANAGING RISK IN AN UNCERTAIN ENVIRONMENT 151, 153 (1994).

398. Woodrow Hartzog has detailed the regulatory tools available to the FTC in the robotics context, many of which also apply to issues raised by IoT devices. These include agencies' extensive notice and disclosure jurisprudence; new theories of design and secondary liability, under which companies may be liable for poor design choices or designs that allow others to indirectly harm consumers; and robust data-security jurisprudence. Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 MD. L. REV. 785, 818–23 (2015). *But see* Lyndon, *supra* note 384, at 142 n.20 (discussing agency limitations in recognizing and addressing technical problems).

399. *Cf.* Hartzog, *supra* note 398, at 814 ("[T]he FTC can regulate consumer harms that fall outside the scope of traditional torts and other regulatory efforts.").

deceptive, or abusive practices.[400] Further, unlike consumer plaintiffs, agencies are not bound by contractual fine print.[401]

Happily, there is no need to select one single medium of legal evolution among courts, legislatures, and agencies; the various rulemaking processes can coexist and supplement each other in developing laws for corporate remote interference.[402] In the absence of legislative or agency action, courts can act as a stopgap.[403] Meanwhile, as exemplified in the climate-litigation context, targeted tort suits can spur new legislation that systematically addresses an issue.[404] Conversely, should courts neglect to address the harms of remote interference, or do so in ways that do not incorporate broader policy concerns, that failure may encourage other institutional responses.[405] For example, legislatures regularly modify concerning tort precedents.[406] The different sources of regulation can also work together to address outlier situations: statutes can address the majority of cases and serve as a baseline framework for evaluating exceptional fact patterns in tort cases, and tort standards can act as a supplemental enforcement device for conduct that does not violate a statutory or agency standard.[407]

---

400. *Id.* at 820 ("[T]he FTC is more capable of addressing small and nuanced changes in design that affect consumers."); Hoofnagle et al., *supra* note 291, at 185, 186–92 (arguing that "[c]onsumer protection law is uniquely situated to vigorously pursue the maintenance of functional free markets while upholding the benefits of consumer rights" and suggesting targeted legal improvements, such as requiring sellers to disclose devices' anticipated lifetimes and enacting statutory right-to-repair laws).

401. Hartzog, *supra* note 398, at 817.

402. Rose-Ackerman, *supra* note 397, at 153–54; *see also* Lyndon, *supra* note 384, at 143 (noting that different sources of law "provide different procedural options or formats for addressing the social costs of technical change").

403. Rose-Ackerman, *supra* note 397, at 153.

404. Kysar, *supra* note 384, at 19.

405. *Cf.* WITT, ACCIDENTAL REPUBLIC, *supra* note 32, at 695–96 (detailing how workers' compensation systems displaced common law regulation of nineteenth-century industrial accidents); Kysar, *supra* note 33, at 49 ("[J]udges unabashedly and creatively forged a new body of products liability law to respond to the rise of a mass consumer marketplace[, which] . . . had the effect of protecting the common law from the kind of wholesale displacement that had occurred in the case of worker injury." (footnotes omitted)).

406. Examples include state statutes that determine when a minor must be held to the standard of an adult, statutes that set standards for informed consent, punitive-damage caps for malpractice, and standards of social-host liability. *See, e.g.*, GOLDBERG, SEBOK & ZIPURSKY, *supra* note 205, at 124 (discussing how, in response to *Rowland v. Christian*, 443 P.2d 561 (Cal. 1968), the California legislature enacted a bill qualifying the California courts' expansive understanding of landowners' potential duties towards trespassers).

407. Rose-Ackerman, *supra* note 397, at 153–54 (describing how the tort and regulatory systems can best complement each other).

2. *Federal and State Lawmaking*. The possibility of ex ante regulatory action raises the question of whether these issues are better addressed at the federal or state level.

There are some reasons to prefer federal regulation. National standards usually make industry compliance easier, as an industry does not need to tailor its practices to different rules in different states. Federal regulation avoids the challenge that state-by-state laws might place an undue burden on interstate commerce.[408] Federal agencies also may be better structured to regulate certain kinds of IoT devices, such as IoT medical devices or IoT vehicles, given that they are already aware of specific issues and governance structures associated with their less-connected cousins.

Conversely, many of the issues this Article discusses relate to consumer protection law, products liability law, and common law tort duties—subjects that have traditionally been developed at the state level. This might be an ideal space for states to serve as laboratories of experimentation in anticipation of federal regulatory action.[409] And, in light of the current federal political gridlock, states are more likely to operationalize this Article's proposals.

Granted, state law will be most influential when compliance requires a change at the hardware or physical-infrastructure level. When a state law only governs software or the provision or termination of a service, it will be relatively easy for companies to alter policies on a state-by-state basis. Indeed, the connected nature of IoT devices will allow companies to change how a particular device operates when it crosses state or national boundaries.[410]

That being said, individual state laws will not necessarily result in myriad contradictory standards; instead, state laws may create consistent nation-wide best practices.[411] For example, a California

408. *But see* Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L.J. 785, 787 (2001) ("[T]he dormant Commerce Clause, properly understood, leaves states with much more flexibility to regulate Internet transactions than is commonly thought.").

409. *See* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

410. For a concise fictional consideration of the dystopian possibilities, see Cory Doctorow, *Sole and Despotic Dominion*, REASON (Dec. 2018), https://reason.com/archives/2018/11/17/sole-and-despotic-dominion [https://perma.cc/728U-YZ86].

411. *See, e.g.*, DAVID VOGEL, TRADING UP: CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY 6 (1995) (discussing the "California Effect," which refers to "the critical role of powerful and wealthy 'green' political jurisdictions in promoting a 'race to the top' among their trading partners . . . help[ing] drive many American regulations upward"); Anu Bradford, *The Brussels Effect*, 107 N.W.U. L. REV. 1, 3 (2012) (discussing the European

requirement that starter-interrupt devices only trigger when the car is parked within five miles of where it spends 60 percent of its time would (1) demonstrate the feasibility of such a practice—which might be relevant when courts across the country consider whether there is a reasonable alternative design; (2) encourage companies forced to invest in creating the technological infrastructure to implement the practice nationally; and (3) influence both the market and tort law nationally by shifting consumer expectations regarding IoT companies' basic harm-prevention measures.

In short, both federal and state law approaches to regulating IoT devices could result in a unified national standard, with agency regulation offering the benefits of incorporating expertise and state regulation offering the benefits of experimentation. Again, these two approaches need not be mutually exclusive. Just as agency regulation of unfair business practices can exist alongside state consumer protection law, agency regulation of IoT devices can coexist with state statutory and common law.

CONCLUSION

Most technological advances are incremental, and most laws are sufficiently tech neutral to stretch to cover new developments. As a result, most technological innovations cause little to no legal disruption.[412] Parking restrictions apply equally to human-driven and self-parking cars; laws that ban bringing guns on airplanes cover both industrially manufactured and 3D-printed firearms. From time to time, however, a new technology will enable new kinds of conduct or generate new negative externalities, which in turn create uncertainty about the application of extant rules, expose or highlight existing contradictions, or even undermine the fundamental assumptions of an entire legal regime.[413]

Union's similar effect on global regulations); Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law* 6–10 (Univ. of Colorado Law Legal Studies Research Paper No. 19-25, Aug. 27, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3433922 [https://perma.cc/3VU7-WQ3W] (discussing the "Delaware Effect," "California Effect," and "Brussels Effect" in the context of privacy regulations).

412. Lyria Bennett Moses, *Why Have a Theory of Law and Technological Change?*, 8 MINN. J.L. SCI. & TECH. 589, 596 (2007) ("Despite occasional statements that some new technology changes everything, legal problems stemming from technological change are relatively rare and quite specific." (footnote omitted)).

413. *See generally* Rebecca Crootof, *Regulating New Weapons Technology*, *in* THE IMPACT OF EMERGING TECHNOLOGIES ON THE LAW OF ARMED CONFLICT 3, 6 (Eric Talbot Jensen &

The Internet of Things creates a new relationship and power dynamic between companies and consumers that is not anticipated by our current civil-liability regime. By collecting personalized data and maintaining an ongoing communications link, IoT devices allow companies to provide a host of convenient, entertaining, and even life-saving services. Simultaneously, IoT companies lock consumers into contractual governance regimes and use IoT-enabled surveillance and remote interference to enforce their rules, sometimes at the risk of consumer safety. Meanwhile, rather than incentivizing IoT companies to minimize foreseeable injuries, contract and tort law currently work in tandem to shield IoT companies from liability.

A techlaw perspective helps situate this moment in a larger story, highlighting the iterative relationship between law, society, and technology. New technologies may create social change and legal uncertainty, but law is a flexible tool that can evolve to address new, tech-facilitated conduct. In the wake of the Industrial Revolution and the associated increase in "stranger cases," courts limited company liability by creating the modern version of "negligence"; the rise of mass production and cross-country transportation networks changed seller–buyer relations and prompted the products liability revolution's reactionary expansion of industry liability.

IoT devices are yet another new technology that alters social and power relations between industry and individuals, creating a potential liability inflection point. Our choices now will determine whether law evolves to preserve or constrain industry's new, tech-enabled powers. A conservative application of existing contract and tort law will result in consumers continuing to bear the brunt of harms resulting from corporate remote interference, and social norms and consumer expectations will follow suit. Alternatively, expansive articulations and applications of current doctrines could retain the benefits and more fairly allocate the costs of this new technology going forward.

Ronald T.P. Alcala eds. 2019) (discussing "four ways in which a new technology can be legally disruptive" through the lens of new weapons technologies).