Richmond Journal of Law & Technology

Volume 26 | Issue 1 Article 4

2-21-2020

Click Here to Sue Everybody: Cutting the Gordian Knot of the Internet of Thing with Class Action Litigation

Dallin Robinson
Arizona State University Sanda Day O'Connor College of Law

Richmond Journal of Law & Technology Volume XXVI, Issue 1

CLICK HERE TO SUE EVERYBODY: CUTTING THE GORDIAN KNOT OF THE INTERNET OF THINGS WITH CLASS ACTION LITIGATION

Dallin Robinson*

Cite as: Dallin Robinson, *Click Here to Sue Everybody: Cutting the Gordian Knot of the Internet of Things with Class Action Litigation*, 26 RICH. J.L. & TECH., no. 1, 2020.

*This article is a humble response to public-interest technologist Bruce Schneier's *Click Here to Kill Everybody*, an articulate and engaging compendium which explores the implications of a hyperconnected world, analyzes the technical, political, and economic forces responsible for the IoT's cybersecurity crisis, and proposes thoughtful government regulation as the only acceptable solution. My deepest gratitude to him; to Professors Jones, Cohen, Carey, Aragon, Wurman, and Marchant; to Justin Larson and Jeff Landow; to the editors of JOLT; to my parents Greg and Nancy; and—especially—to my wife Maria. Without the insight, counsel, and support of these extraordinary individuals, this article would be far inferior and perhaps nonexistent. All errors are my own.

ABSTRACT

It is not hyperbole to state that the mass proliferation of the Internet of Things (IoT) will alter modern society to a degree surpassing even the Industrial Revolution. Data has surpassed oil as the world's most valuable resource, and the IoT generates a nigh-incomprehensible amount of it. As consumers, corporations, and governments increasingly embrace this marvelous technology, its possibilities and perils become ever more evident. Consider, for example, the 5G network. It will allow smart vehicles to communicate not only with each other but also with thousands of sensors installed along the roads. These connections will give drivers advance warning of traffic patterns, pedestrian crossings, and hazardous conditions, improving safety and reducing congestion. But most vehicles manufactured today—indeed, most smart devices in general—are not fit for this hyperconnected future. The misaligned incentives of the stakeholders involved in the IoT's development have led to a lack of oversight and thus a crisis of cybersecurity. Just a few months ago, for instance, a hacker broke into more than 27,000 vehicles through poorly configured GPS tracking devices. Besides scraping the drivers' personal information, the hacker threatened to remotely kill the vehicles' engines while they were in motion. Nearly all existing scholarship on the legal and policy implications of the IoT concludes with pleas to governing bodies for meaningful industry oversight. This article does not. Instead, it accepts the reality that policymakers, left to their own devices, will not adequately govern the IoT until its risks become unambiguously apparent; that is, until it is fatally hacked. To forestall this version of the future, this article proposes proactive class action litigation against all unacceptably dangerous IoT devices to realign the interests of the private sector with those of the public good.

Table of Contents

Table of Contents (Cont'd)

[1] It is 7:00 AM. You wake to the soft strains of Rossini's *The Thieving Magpie* as your bedroom curtains gradually open to the first rays of sunlight. The aroma of rich black coffee wafts through the air as you shuffle toward your bathroom, where the tile floor has already heated itself for your comfort. You splash some water on your face as your mirror recites your daily appointments and the weather forecast in a pleasantly professional voice. As you enter the kitchen, your refrigerator lets you know it has ordered your weekly shipment of groceries, which will arrive when you return home that evening. You pour your coffee and turn your attention to the TV. Its display flicks on to the morning headlines, which you briefly scan before arranging the eggs and bacon that have just finished cooking on a plate. You wash your breakfast down with the rest of your coffee and return to the bedroom to see what your closet has selected for you to wear to work. As you leave your apartment, your front door locks itself behind you and wishes you a cheery goodbye. Your car powers on and opens its door as you approach. You climb in, recline on its full-size passenger couch, and continue watching the news as the car sets off. You are whisked through tranquil suburbs to the nearest highway, which is teeming with vehicles yet just as silent as your neighborhood streets. You seamlessly merge into the morning commute in synchronicity with billions of individuals in thousands of cities around the globe, each of whom enjoys the same conveniences as you because the entire developed world is one titanic computer: the Internet of Things. The date is August 4, 2026.

I. OVERVIEW

[2] The Internet of Things (IoT) is deceptively straightforward at first glance. It is simply defined as the network of all Internet-capable devices, excluding Personal Computers (PCs) and smartphones.[1] However, the IoT

[1] *See* GARTNER, LEADING THE IOT: GARTNER INSIGHTS ON HOW TO LEAD IN A CONNECTED WORLD 2 (Mark Hung, ed., 2017), https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf [https://perma.cc/6S8Y-8T49].

also represents the future of our civilization.[2] Twenty years ago, a business columnist proclaimed that "[i]n the next century, planet [E]arth will don an electronic skin . . . . consist[ing] of millions of embedded electronic measuring devices[.]"[3] In just over a decade, the columnist's prediction became a reality.

[3] In the early 2010s, developments in hardware[4] and software[5] exponentially increased the efficiency and complexity of connected devices. The introduction of the raw processing power of cloud computing made it possible to comprehend the mammoth amounts of data that those

[2] *See id.* at 27 ("The IoT will do more for us . . . in the future than we have yet to imagine").

[3] Neil Gross, *The Earth Will Don an Electronic Skin*, BLOOMBERG BUS. (Aug. 29, 1999), https://www.bloomberg.com/news/articles/1999-08-29/14-the-earth-will-don-an-electronic-skin [https://perma.cc/HWY4-TTLJ].

[4] *See* Brandon Lewis, *2017 Embedded Processor Report: At the edge of Moore's Law and IoT*, EMBEDDED COMPUTING DESIGN (Jan. 31, 2017), https://www.embedded-computing.com/embedded-computing-design/2017-embedded-processor-report-at-the-edge-of-moores-law-and-iot [https://perma.cc/2L37-2GEE]; *see also* Taazaa, *The Technologies that Enable the Internet of Things*, https://taazaa.com/the-technologies-that-enable-the-internet-of-things/ [https://perma.cc/V34A-B43B].

[5] *See* Omer Shwartz et al., *Reverse Engineering IoT Devices: Effective Techniques and Methods*, 5 IEEE INTERNET OF THINGS J. 4965, 4965 (2018); *see also* Christian Daudt, *The Shift to Linux Operating Systems for IoT* (Mar. 8, 2018), IOTFORALL, https://www.iotforall.com/linux-operating-system-iot-devices [https://perma.cc/YDG6-RTNT] (stating that if a CPU is a computer's heart, the operating system (OS) is its brain. An OS allocates resources among all the computer's programs and provides an interface by which those programs can interact with each other); s*ee also* TAAZAA, *supra* note 4 (stating that increasing the sophistication of the CPUs at the heart of connected devices allowed them to run stripped-down versions of established OS's such as Windows and Linux; and stating that assuring compatibility with these established companies supplied the fledgling IoT industry with an army of developers and a wealth of resources).

devices generated.[6] These advancements led to the introduction of "smart" IoT devices into the marketplace. Built with perpetual Internet connectivity, these devices promise convenience and efficiency to end users[7] in exchange for the collection of countless data points, which are sold to third-party advertisers.[8] Emboldened by the success of Internet-connected consumer devices, intrepid technology companies expanded the IoT across all industries.[9] The rest, as they say, is history. In less than a decade, the IoT exploded to become a ubiquitous presence in the lives of more than five billion consumers.[10] Analysts predict that by 2025, there will be more than 64 billion IoT devices[11] processing over 90 zettabytes of

[6] *See* TAAZAA, *supra* note 4.

[7] *See* discussion *infra* Part II(A).

[8] *See, e.g.*, Alec Scott, *8 Ways the Internet of Things Will Change the Way We Live and Work*, GLOBE & MAIL, https://www.theglobeandmail.com/report-on-business/rob-magazine/the-future-is-smart/article24586994 [https://perma.cc/U78V-5JSA] (warning that consumer fitness trackers such as the FitBit and Apple Watch measure heart rate, sleep patterns, diet, and exercise; they could soon send the data they collect directly to health care providers and insurers); *see also* Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [https://perma.cc/C4DX-BZRR] (warning that the supposedly anonymous location tracking employed by many apps and sold to dozens of companies is precise and frequent enough to identify particular users).

[9] *See* discussion *infra* Part II(A).

[10] *See* David Reinsel et al., *The Digitalization of the World from Edge to Core*, IDC 5 (Nov. 2018), https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf [https://perma.cc/LP3Y-YQFF].

[11] *See* Peter Newman, *IoT Report: How Internet of Things Technology Growth is Reaching Mainstream Companies and Consumers*,, BUSINESS INSIDER (Jan. 28, 2019, 1:09 PM), https://www.businessinsider.com/internet-of-things-report [https://perma.cc/6DXR-SCZZ].

data.[12] That represents a potential value of $11.1 trillion—roughly 11 percent of the 2025 economy.[13] More than that: it represents "a single global Internet that affects the world in a direct, physical manner . . . an Internet that senses, thinks, and acts."[14]

[4] However, as any fan of science fiction knows, gleaming utopian civilizations are not always as they appear. Just so, there is a darker counternarrative to the IoT's inexorable progress. As a new industry, the IoT is expected to govern itself because policymakers are wary of stifling the growth of something which has implications and underpinnings that they do not fully understand.[15] But this "wait-and-see" sentiment is antithetical to the warnings of cybersecurity experts who staunchly believe the federal government is the only body capable of assuring the IoT's safety.[16] These experts began sounding dire warnings of the IoT's security

[12] *See* Thomas Barnett, Jr., *The Zettabyte Era Officially Begins (How Much is That?)*, CISCO SP360 (Sept. 9, 2019), https://blogs.cisco.com/sp/the-zettabyte-era-officially-begins-how-much-is-that [https://perma.cc/4DTZ-ZTUM] (illustrating that if each gigabyte were a brick, then one zettabyte would be the equivalent of 258 Great Walls of China); *see also* Reinsel et al., *supra* note 10.

[13] *See* McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype* 2 (June 2015), http://img.cecport.com/mediaCms/pdf/201507/15141040mcg6.pdf [https://perma.cc/RD9Y-SAXK].

[14] *See* BRUCE SCHNEIER, CLICK HERE TO KILL EVERYBODY: SECURITY AND SURVIVAL IN A HYPER-CONNECTED WORLD 7 (W. W. Norton & Co. 2018).

[15] *See, e.g.*, FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 47–49 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/C8RL-W3ZG] (labeling potential legislation as "premature" and leaving it to the industries to regulate themselves).

[16] *See, e.g.*, SCHNEIER, *supra* note 14, at 145 ("I can think of no industry in the past 100 years that has improved its safety and security without being compelled to do so by the government").

issues years before "smart" devices entered the public's consciousness.[17] The budding industry, of course, ignored these warnings. Desperate to make themselves heard as the IoT ballooned across consumers, corporations, and governments, these experts began comparing the IoT's insecurity to the personal computer security crisis of the mid-1990s,[18] to no avail.[19] The volume of attacks targeting IoT devices progressively grew as did the IoT itself.[20] Just a few months ago, for instance, a Chinese smart home management service leaked the hashed (i.e., scrambled) password, password reset codes, email addresses, and geolocation information of more than *two billion* customers when it accidentally left one of its servers connected to the Internet without a password.[21]

---

[17] *See, e.g.*, Gang Gan et al., *Internet of Things Security Analysis*, INT'L CONF. ON IEEE, 2011, at 1; *see also* Rodrigo Roman et al., *Securing the Internet of Things*, 44 IEEE COMPUTER 51, 51 (2011).

[18] *See e.g.*, Danny Palmer, *IoT Security: Why It will Get Worse Before It Gets Better* (Nov. 7, 2018) https://www.zdnet.com/article/iot-security-why-it-will-get-worse-before-it-gets-better/ [https://perma.cc/DZ7W-5D85] ("Speaking about IoT at a conference like this unfortunately makes me feel very old. It takes me back to the mid-1990s," said Steve Purser, Head, Core Operations Dep't., Eur. Union Agency for Network and Info. Sec., IoT Sec.); *see also* Bruce Schneier, *The Internet of Things Is Wildly Insecure—and Often Unpatchable* (Jan. 6, 2014), https://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/ [https://perma.cc/KWS5-U4UQ].

[19] *See, e.g.*, Engin Leloglu, *A Review of Security Concerns in Internet of Things*, 5 COMPUTER & COMM. 121, 122 (2017); *see also* Brian Krebs, *This is Why People Fear the 'Internet of Things'*, KREBS ON SECURITY, (Feb. 18, 2016), https://krebsonsecurity.com/2016/02/this-is-why-people-fear-the-internet-of-things/ [https://perma.cc/RY2Q-Y9MN].

[20] *See* SOPHOS, SOPHOSLABS 2019 THREAT REPORT 24 (2018).

[21] *See* Catalin Cimpanu, *Smart Home Maker Leaks Customer Data, Device Passwords*, ZDNet (Jul. 1, 2019), https://www.zdnet.com/article/smart-home-maker-leaks-customer-data-device-passwords [https://perma.cc/WP67-M6BQ].

[5] Thankfully, the current crisis of privacy provides a foil for what effective governance of the IoT should look like. A recent spike in high-profile data breaches has shattered the public's confidence that companies will adequately safeguard consumer data.[22] Revelations that many of these companies invited their breaches through grossly negligent security practices sparked outrage, forced a national conversation on privacy reform,[23] and led policymakers to draft bipartisan bills and consider antitrust actions against the worst offenders.[24]

[6] The Internet's crisis of privacy is nearing a resolution because the public's indignation at the industry's abuse of its privacy rights has finally grown too loud to ignore.[25] By contrast, the crisis of IoT safety is just beginning. Regulators have allowed major manufacturers of IoT devices and technologies to treat consumer safety with as little respect as privacy pariahs Facebook and Equifax have shown towards data security[26] and are unlikely to change course until human lives are lost.[27]

[7] Prominent members of the cybersecurity community, like Bruce Schneier, generally subscribe to the fatalities-as-necessary-for-

[22] *See, e.g.*, Julia Carpenter & Bourree Lam, *The Capital One Hack: Life in the Time of Breach Fatigue*, WALL STREET J. (Aug. 4, 2019), https://www.wsj.com/articles/the-capital-one-hack-life-in-the-time-of-breach-fatigue-11564824600 [https://perma.cc/DK8Y-Y2KT].

[23] *See infra* Part IV(C).

[24] *See id.*

[25] *See id.*

[26] *See infra* Part IV(A).

[27] *See* SCHNEIER, *supra* note 14, at 182.

policymaking theory.[28] While Schneier believes in a future where Silicon Valley tech experts and Washington bureaucrats work out their differences and share their expertise across a *Star Trek*-style conference table,[29] he admits that he cannot, as a practical matter, describe *how* this marriage of technology and politics will come about.[30] He accepts this as the "gaping hole" of his thesis on the IoT.[31] This article seeks to fill that hole by advocating for the use of private class action litigation premised on the Magnuson-Moss Warranty Act (MMWA) and fraudulent concealment claims to correct the "misaligned incentives" of the corporations and agencies responsible for the IoT's safety crisis.[32]

[8] In general, a successfully certified class action is a powerful bargaining chip in settlement negotiations.[33] Indeed, a 2008 empirical study of class actions found that "[e]very case in which a motion to certify

[28] *See id.*

[29] *See* Alfred Ng, *Computer Security Needs More Federal Regulation, Says U.S. Senator*, CNET (Dec. 6, 2017 5:00 AM), https://www.cnet.com/news/sen-maggie-hassan-security-needs-government-regulation/ [https://perma.cc/U8HX-UFPJ] (Senator Maggie Hassan (D–NH), one of the few members of Congress attuned to the dangers of the IoT, agrees with Schneier, declaring "[members of Congress] need to listen to tech companies to be sure about how we go about doing this so that they can continue to innovate, but it's our job to make them aware, as well as consumers, that we really do have threats we have to address."); *see also id.* at 221.

[30] *See* SCHNEIER, *supra* note 14, at 11.

[31] *Id.*

[32] *See id.* at 124, 126.

[33] *See, e.g.*, Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co., 559 U.S. 393, 445 (2010) (Ginsburg, J., dissenting).

was granted . . . resulted in a class settlement."[34] But successfully certifying a class is not for the faint of heart. A spate of recent legislation and Supreme Court decisions has forced plaintiffs into slow-moving federal court, intensified procedural requirements, and banished an ever-increasing number of putative classes to private arbitration.[35] Despite these difficulties, the plaintiffs in *Flynn v. FCA U.S. LLC*, a car-hacking class action filed in the Southern District of Illinois, recently secured certification of several classes against one of the world's largest automakers.[36] Both the Seventh Circuit and the United States Supreme Court have rejected the defendants' appeal of this decision[37] and so the parties will begin trial shortly after this article's publication.[38] The outcome of this case will stand as a landmark for the future of IoT litigation, as it is "the first case to proceed past summary judgment in which no actual data breach had occurred."[39]

---

[34] EMORY G. LEE III & THOMAS W. WILLGING, FED. JUDICIAL CTR., IMPACT OF THE CLASS ACTION FAIRNESS ACT ON THE FEDERAL COURTS: PRELIMINARY FINDINGS FROM PHASE TWO'S PRE-CAFA SAMPLE OF DIVERSITY CLASS ACTIONS 11 (2008).

[35] *See infra* Part VI(B).

[36] *See* Flynn v. FCA US LLC, 327 F.R.D. 206, 227 (S.D. Ill. 2018); *see also* Olivia Minnock, *Top 10 Biggest Car Manufacturers in the World*, MANUFACTURING GLOBAL (Nov. 9, 2017, 9:04 AM), https://www.manufacturingglobal.com/top10/top-10-biggest-car-manufacturers-world [https://perma.cc/QV8V-KUVZ].

[37] *See* Flynn v. FCA US LLC, 327 F.R.D. 206 (S.D. Ill. 2018), *cert. denied*, 139 S. Ct. 797 (2019).

[38] *See* Flynn v. FCA U.S. LLC, No. 15-cv-0855-MJR-DGW, 2017 WL 3592040, at *5 (S.D. Ill. Aug. 21, 2017).

[39] Philip N. Yannella, *Fiat-Chrysler Ruling May Pave the Way for Overpayment Class Actions Based on Security Flaws*, BALLARD SPAHR LLP: CYBERADVISER (July 13, 2018), https://www.cyberadviserblog.com/2018/07/fiat-chrysler-ruling-may-pave-the-way-for-overpayment-class-actions-based-on-security-flaws/ [https://perma.cc/U75Y-GA78].

[9] As a prophylactic response to Schneier's problem of feasibility, this article attempts to force a national conversation on IoT safety before human lives are lost. Part II examines the possibilities and perils of the industry.[40] Part III establishes that the privacy concerns of the Internet and the safety concerns of the IoT stem from a common source and share a common solution.[41] Part IV builds on Part III to anticipate the future of IoT governance by outlining the evolution of present-day privacy reform.[42] Part V sketches recent regulatory failures to argue that the reactive policymaking of the privacy era is an unacceptable solution to the emergent IoT crisis.[43] Part VI traces the history of the class action device as a tool for institutional reform.[44] It concludes by endorsing proactive class action litigation against the IoT to force its manufacturers to adhere to effective safety standards.[45] Finally, Part VII submits *Flynn v. FCA* as a realistic paradigm of Part VI's proposal and considers how *Flynn*'s theories of liability may be applied against all manufacturers of dangerous IoT devices who are guilty of inadequate cybersecurity practices.[46]

[10] If regulatory oversight and reformatory legislation are scalpels in a policymaker's toolkit, litigation is a sledgehammer: a less-than-optimal solution that is likely to leave unforeseen lasting effects and is admittedly inefficient in its application. But it is certainly better than no solution at all. Consumer class action litigation against the IoT, therefore, represents a first step towards the gathering of technology titans and septuagenarian

[40] *See infra* Part II.

[41] *See infra* Part III.

[42] *See infra* Part IV.

[43] *See infra* Part V.

[44] *See infra* Part VI.

[45] *See id.*

[46] *See infra* Part VII.

Senators around the proverbial conference table, where personal interests can be set aside in pursuit of a safer Internet and thus a better world.

II. THE UNPRECEDENTED POSSIBILITIES—AND PERILS—OF THE IoT

[11] The IoT will surely bring unprecedented convenience and efficiency to the society of the mid-21st century. But because of deep-rooted security flaws and market failures, this hyperconnected future will just as surely threaten the lives of its inhabitants in exotic and unprecedented ways.

A. A Future Anticipated by the Golden Age of Science Fiction

[12] The concept of converting the globe into a physical embodiment of the Internet itself seems pulled from the pages of pulp fiction. In fact, it will become reality in less than a decade.[47] The seemingly arbitrary date in this article's introduction is a reference to the date chosen by sci-fi author Ray Bradbury for the setting of his May 1950 short story *There Will Come Soft Rains*, which describes the comfort and convenience of an automated home left uninhabited in the wake of a nuclear holocaust.[48] At the time of this article's publication, hyperconnected homes were already

[47] *See* Olga Ezzheva, *Preparing for a 5G Future: How Telcos Will Monetize New Technology*, IOTFORALL (Oct. 18, 2018), https://www.iotforall.com/how-telcos-monetize-5g-technology/ [https://perma.cc/6UCW-288S] (noting that industry experts consider the 5G network to be the backbone of the smart cities of the future and project that the number of 5G subscriptions will number in the billions by the mid-2020s)*; see also* Sheryl Tian Tong Lee, *China Races Ahead of the U.S. in the Battle for 5G Supremacy*, BLOOMBERG (Aug. 1, 2019), https://www.bloomberg.com/news/articles/2019-08-01/china-bets-on-5g-socialism-in-push-to-lead-global-tech-race [https://perma.cc/H752-MJML] (explaining that the forthcoming 5G network is crucial to the timeline of IoT development; and the United States and China are furiously competing to be the first country to bring this essential technology to the masses).

[48] *See* Ray Bradbury, *There Will Come Soft Rains*, *in* THE MARTIAN CHRONICLES 205 (Doubleday & Company, Inc. 1950).

commonplace and trending towards the sophisticated automation imagined by Bradbury many decades ago.[49] The science fiction of yesteryear becomes the reality of tomorrow.[50]

[13] While the IoT of today is not as ubiquitous as it will be in the years to come, it is well on its way to becoming so. Indeed, the number of American adults who own at least one smart device is 62 percent and growing.[51] Every consumer market segment, from the usual suspects (like TVs,[52] security cameras,[53] and DVRs[54]) to the trendy newcomers (think toasters,[55] refrigerators,[56] and coffeemakers[57]), has begun manufacturing

[49] *See There's No Place Like [A Connected] Home*, MCKINSEY & COMPANY, https://www.mckinsey.com/spContent/connected_homes/index.html [https://perma.cc/23TQ-DA83].

[50] *See* Megan Willett, *24 Books that Forecast the Future*, BUS. INSIDER (July 30, 2014), https://www.businessinsider.com/sci-fi-books-that-predicted-the-future-2014-7 [https://perma.cc/Q3XY-QDQZ] (celebrating the giants of the genre, such as Jules Verne and H.G. Wells, for predicting (or influencing) the development of many future technologies decades in advance).

[51] *See The Dangers of the Internet of Things*, CYBERSECURITY DEGREES, http://cybersecuritydegrees.com/wp-content/uploads/2018/08/DangersIoT.png [https://perma.cc/Y6PP-5ZT3].

[52] *See, e.g.*, *Smart TVs*, SAMSUNG, https://www.samsung.com/us/explore/smart-tv/highlights/ [https://perma.cc/9QHL-TA35].

[53] *See, e.g.*, *IP Cameras*, LOREX, https://www.lorextechnology.com/ip-cameras/N-ewg3lh [https://perma.cc/9R7V-A6GG].

[54] *See, e.g.*, *BOLT VOX*, TIVO, https://www.tivo.com/products/bolt-detail [https://perma.cc/8CMY-R23C].

[55] *See, e.g.*, Brian Heater, *Smart Toasters Are Here*, TECHCRUNCH (Jan. 7, 2017), https://techcrunch.com/2017/01/07/toaster/ [https://perma.cc/3EHC-AXS4].

connected devices. The IoT even includes modern cars and modern homes—two industries with particularly ambitious visions of how Internet integration will affect the future of their products.[58] For example, once smart autonomous vehicles become commonplace, every car on the road will be able to communicate its position with its neighbors to make more efficient use of available space.[59] This will cut back on the 90 billion hours drivers sit idle in traffic jams every year, which generates 220 million metric tons of exhaust and wastes over $1 trillion in fuel costs and lost productivity.[60] As of June 2019, there were over 80 companies testing more than 1,400 autonomous vehicles in 37 states.[61]

[14] Consumer devices are just the beginning. The IoT has widespread implications for commercial industries as well. For example, retailers have

[56] *See, e.g.*, *Family Hub*, SAMSUNG, https://www.samsung.com/us/explore/family-hub-refrigerator/connected-hub/ [https://perma.cc/8KD4-MJFL].

[57] *See, e.g.*, *GranBaristo Avanti*, SAECO, https://www.philips.com/c-m-ho/saeco-espresso/granbaristo-avanti [https://perma.cc/GYN7-U8CZ].

[58] *See, e.g.*, *Home of the Future: Building a Connected Home with AWS IoT*, AMAZON WEB SERVS., https://d1.awsstatic.com/product-marketing/iot/AWS-IoT-Connected-Home-Infographic.pdf [https://perma.cc/DN6G-E2Z3]; *see also What's Driving the Connected Car*, MCKINSEY & CO. (Sept. 2014), https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car [https://perma.cc/G3ZP-J4NM].

[59] *See* Scott, *supra* note 8.

[60] *See id.*

[61] *See* Darrell Etherington, *Over 1,400 Self-Driving Vehicles Are Now in Testing by 80+ Companies Across the U.S.*, TECHCRUNCH (June 11, 2019), https://techcrunch.com/2019/06/11/over-1400-self-driving-vehicles-are-now-in-testing-by-80-companies-across-the-u-s/ [https://perma.cc/ENY8-GPRM].

begun to synthesize data from cameras, smart shelves, and mobile apps to "anticipate customer desires" and to increase operational efficiency.[62] Tech-savvy farmers use data gathered from sensors monitoring soil moisture, pesticide usage, and weather forecasts to oversee their farms' resources and quickly identify crop issues.[63] Similarly, modern manufacturing plants bristle with microsensors which regulate interior conditions, reduce maintenance costs, increase energy efficiency, and identify potential delays well in advance.[64]

[15] Writ large, the IoT is even changing the way we think about cities. Sidewalk Labs, a subsidiary of Alphabet, unveiled a CA$3.9 billion project in June 2019 to build a mixed-use neighborhood on Toronto's waterfront "from the Internet up."[65] With its futuristic conceptions of housing, energy consumption, mobility, social services, and shared public spaces, the proposed development is the most prominent example to date of Silicon Valley's plans to disrupt the urban planning industry.[66] It will include, among other things: a city-wide wireless network capable of

[62] *See, e.g.*, *Azure IoT*, MICROSOFT, https://azure.microsoft.com/en-us/overview/iot/?site=mscom_iot [https://perma.cc/SL48-HVKS].

[63] *See, e.g.*, *About OnFarm*, ONFARM, http://www.onfarm.com/about/ [https://perma.cc/X8P8-M3SQ].

[64] *See* Scott, *supra* note 8.

[65] Daniel L. Doctoroff, *Reimagining Cities from the Internet up*, SIDEWALK LABS (Nov. 30, 2016), https://www.sidewalklabs.com/blog/reimagining-cities-from-the-internet-up/ [https://perma.cc/EK2X-X9JF].

[66] *See generally Sidewalk Lab's Proposal, Master Innovation and Development Plan: Overview*, QUAYSIDE, (June 17, 2019), https://quaysideto.ca/sidewalk-labs-proposal-master-innovation-and-development-plan/ [https://perma.cc/553T-397S].

supporting the use of roughly 10 million devices at once;[67] sensors in each building which monitor structural integrity, vibration, odors, air quality, and noise levels;[68] smart logistics hubs within each mixed-use neighborhood which coordinate autonomous vehicles responsible for deliveries, waste disposal, and storage;[69] smart traffic lights which can prioritize a single packed transit vehicle over a line of empty taxis;[70] fleets of shared self-driving cars;[71] heated bike lanes which warm up just before a snowstorm hits;[72] and adaptive streets which can shift from wide boulevards during morning rush hour, to bike lanes in the afternoon, and to loading zones at night.[73]

[16] The IoT has transformed every aspect of modern society and will continue to do so with each passing day. Therein, as they say, lies the rub.

[67] *See The Urban Innovations*, SIDEWALK LABS 386, https://quaysideto.ca/wp-content/uploads/2019/07/MIDP-Volume-2-Printer-Friendly.pdf [https://perma.cc/PJZ4-W57X].

[68] *See id.* at 448–49.

[69] *See id.* at 68–83.

[70] *See id.* at 87.

[71] *See id.* at 54–56.

[72] *See id.* at 384.

[73] *See id.* at 94–95.

B. But at What Cost?

[17] The first law of cybersecurity is that every computer can be hacked.[74] The coming decades will see the computerization and connection of almost every tangible thing.[75] Given the IoT industry's chronic lack of cybersecurity, it is almost a certainty that as the IoT subsumes everything else, it will be hacked and people will die.[76]

1. Increasing Complexity Makes for Simpler Attacks

[18] If "all computers can be hacked" is the first law of cybersecurity, "offense always beats defense" is the second.[77] This truism, which dates to the infancy of the Internet,[78] is a consequence of complexity.[79] Greater

[74] *See* SCHNEIER, *supra* note 14, at 19 ("In 1989, Internet security expert Gene Spafford famously said: 'The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards—and even then I have my doubts.' Almost 30 years later, that's still true.").

[75] *See id.* at 6–7.

[76] *See* Bruce Schneier, *IoT Cybersecurity: What's Plan B?*, SCHNEIER ON SEC. (Oct. 18, 2017), https://www.schneier.com/blog/archives/2017/10/iot_cybersecuri.html [https://perma.cc/M99M-ZPFQ] ("The Internet is dangerous—and the IoT gives it not just eyes and ears, but also hands and feet. Security vulnerabilities, exploits, and attacks that once affected only bits and bytes now affect flesh and blood.").

[77] *See* SCHNEIER, supra note 14, at 26–28.

[78] *See* SCHNEIER, *supra* note 14, at 26; *see also* Roger R. Schell, *Computer Security: The Achilles' Heel of the Electronic Air Force?*, 30 AIR UNIV. REV., 16–33 (1979), *reprinted in* AIR & SPACE POWER J., Jan.–Feb. 2013, at 158, 174 (describing cybersecurity as "a rather unbalanced contest").

[79] *See* SCHNEIER, *supra* note 14, at 26–27; *see also* Bruce Schneier, *A Plea for Simplicity: You Can't Secure What You Can't Understand*, INFO. SECURITY, Nov. 19, 1999, *as reprinted in* SCHNEIER ON SECURITY,

complexity means a larger attack surface,[80] and the Internet is the most complex machine ever built.[81] In fact, the imbalance between attackers and defenders on the Internet is so skewed that every major company will always be vulnerable to cyberattacks to some degree regardless of the size of its cybersecurity budget.[82]

[19] The arrival of the IoT exponentially increased the Internet's complexity and, therefore, its insecurity.[83] The proliferation of virtual assistants, smart appliances, and the like drastically increased users' vulnerability to attacks because systems which are individually secure may become compromised through unforeseen interactions with each other.[84] A particularly illustrative example of this phenomenon occurred in 2017, when hackers acquired the high-roller database of an unnamed North American casino by exploiting an Internet-connected fish tank, of all things, to gain access to the casino's internal network.[85] The

https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html [https://perma.cc/LC6V-JBG2] ("The worst enemy of security is complexity. This has been true since the beginning of computers, and it's likely to be true for the foreseeable future.").

[80] *See* SCHNEIER, *supra* note 14, at 27.

[81] *See id*.

[82] *See id.* at 28 ("[A] sufficiently skilled, funded, and motivated attacker will always get in."); *cf.* Schell, *supra* note 78, at 174 (explaining how many private companies in the past gave up after failing to patch all necessary security holes, even after spending millions of dollars on the problem).

[83] *See id.* at 29.

[84] *See id.* at 28–29.

[85] *See id.at* 29; *see also* Jessica Miley, *A Casino's Database Was Hacked Through a Smart Fish Tank Thermometer*, INTERESTING ENGINEERING (Apr. 16, 2018), https://interestingengineering.com/a-casinos-database-was-hacked-through-a-smart-fish-tank-thermometer [https://perma.cc/MU5W-YP8G].

hyperconnected IoT of the near future will suffer many more attacks in this vein as creative hackers turn seemingly innocuous blind spots into catastrophic breaches.

[20] Every year, the U.S. Director of National Intelligence briefs both houses of Congress on the extant threats to national security.[86] Each of these addresses over the last five years has warned of the dangers of the relentlessly-expanding IoT with increasingly dire rhetoric.[87] But the IoT

[86] *See, e.g.*, Daniel R. Coats, *Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community*, OFF. OF THE DIRECTOR OF NAT'L INTELLIGENCE (Jan. 29, 2019, 7:59 AM), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf [https://perma.cc/5NFE-GTTU].

[87] *See* SCHNEIER, *supra* note 14, at 80–81, 89 (examining past statements made during Senate Worldwide Threat hearings which consistently move from discussing the increasing risks as a hypothetical to discussing them as a future certainty); *see also Worldwide Threats: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. (2018) (pre-published statement of Daniel R. Coats, Director of National Intelligence), https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf [https://perma.cc/A744-H7E5] ("The potential for surprise in the cyber realm *will* increase in the next year and beyond as billions more digital devices are connected—with relatively little built-in security—and both nation states and malign actors become more emboldened and better equipped . . .") (emphasis added); *see also Open Hearing on Worldwide Threats: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. (2017) (pre-published statement of Daniel R. Coats, Director of National Intelligence), https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf [https://perma.cc/K5PN-ZCK5] ("Cyber threats . . . pose an increasing risk to public health, safety and prosperity as cyber technologies are integrated with critical infrastructure in key sectors."); *see also Emerging United States Defense Challenges and Worldwide Threats: Hearing Before the S. Comm. on Armed Servs.*, 114th Cong. (2016) (pre-published statement of James R. Clapper, Director of National Intelligence), https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf [https://perma.cc/PX2L-UCN5] ("Future cyber operations *will almost certainly* include an increased emphasis on changing or manipulating data to compromise its integrity . . . .") (emphasis added); *see also Worldwide Threats: Hearing Before the S. Comm. on Armed Servs.*, 114th Cong. (2015) (pre-published statement of James R. Clapper, Director of National Intelligence), https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf [https://perma.cc/DED4-QQU9] ("In the future, however, we *might* also see more cyber operations that will change or

remains insecure for the same reasons the Internet itself has always been insecure: market forces and market failures.[88]

2. Microeconomics 101: Making Sense of the Internet of Things

[21] In the modern manufacturing sector, safety typically lags behind innovation for two reasons: corporate executives in pursuit of higher stock prices are incentivized to shun the higher research and development costs of cybersecurity for short-term profits;[89] unregulated markets force companies to cut corners to remain competitive, with potentially fatal results.[90]

a. The Market Rewards First Movers at the Expense of Consumer Safety

[22] A 2016 article about one of Samsung's early attempts at a smart refrigerator griped, "[T]he concept is novel, to be sure, but it's also a new extreme of making something connected for the mere sake of making it connected."[91] This misses the point of connected devices. The hardware

manipulate electronic information in order to compromise its integrity . . .") (emphasis added).

[88] *See* discussion *infra* Part III.

[89] *See* CHARLES WHEELAN, NAKED ECONOMICS: UNDRESSING THE DISMAL SCIENCE 40-41 (2010) (noting that Paul Volcker, former chair of the Federal Reserve, has called stock options "an instrument of the devil").

[90] *See infra* note 95, at 1.

[91] J.R. Raphael, *The 'Smart Everything' Trend Has Officially Turned Stupid*, COMPUTERWORLD, (Jan. 7, 2016), https://www.computerworld.com/article/3019713/smart-everything-trend.html [https://perma.cc/H676-V6J9]; *see* SCHNEIER, *supra* note 14, at 6.

and software advancements which decreased the marginal costs of adding computers to consumer devices[92] likewise decreased the marginal benefits necessary to justify their incorporation.[93] Thanks to the immense growth potential of digital technology, a company can leverage even a slight improvement in user experience or data collection into industry dominance.[94]

[23] The pressure exerted by competitive markets on manufacturers of IoT devices further steepens this technological adoption curve.[95] The first adopter of smart technology in any given industry commands a large market share and can charge a premium for its product.[96] Its competitors must quickly follow suit to avoid obsolescence.[97] In this race to market, the difference between billions of dollars and bankruptcy can be as narrow as a few days.[98] So, it quickly becomes prohibitively expensive for manufacturers to *omit* connectivity from their products. As Schneier puts

[92] *See* Taazaa, *supra* note 4 (referencing the "growing number of devices connected to the global; internet").

[93] *See* SCHNEIER, *supra* note 14, at 6.

[94] *See* BENJAMIN C. DEAN, *Strict Product Liability and the Internet of Things*, CTR. FOR DEMOCRACY & TECH. 3 (Apr. 16, 2018), https://cdt.org/files/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf [https://perma.cc/7VSV-ZFLA].

[95] *See* ADAM COPELAND & ADAM HALE SHAPIRO, PRICE SETTING IN AN INNOVATIVE MARKET 3 (Fed. Res. Bank of S.F., Working Paper No. 2013-04, 2013).

[96] *See id.*

[97] *See id.* at 3–4.

[98] *See* DEAN *supra* note 94, at 3.

it, it will soon "be cheaper to litter the city with sensors than to clean litter off the sidewalks."[99]

[24] The first-mover advantage invariably renders consumer safety an afterthought because installing additional security measures costs precious time,[100] and because the IoT is a classic lemons market.[101] That is, there is no way for consumers to make informed purchasing decisions because it is impossible to distinguish secure devices from fatally vulnerable ones.[102] Even if it were not illegal to access the source code of consumer products, the average person does not have the technical expertise to differentiate poorly written code from high-quality code,[103] nor is there a standardized IoT security certification program or labeling scheme.[104] Therefore, an insecure product advertised as secure will always crowd its genuinely

[99] *See* SCHNEIER *supra* note 14, at 6 (explaining that today, the average cost of an IoT sensor is fifty cents and falling).

[100] *See* DEAN, *supra* note 94, at 3.

[101] *See* SCHNEIER, *supra* note 14, at 134. *See generally* George A. Akerlof, *The Market for 'Lemons': Quality Uncertainty and the Market Mechanism*, 84 Q. J. ECON. 488 (1970) (explaining the "Market for Lemons").

[102] *See* SCHNEIER, *supra* note 14, at 134.

[103] *See* Letter from Joseph L. Hall et. al., Ctr. for Democracy & Tech., to Office of the Secretary, Consumer Prod. Safety Comm'n 3 (June 15, 2018) (on file with Ctr. For Democracy & Tech.).

[104] *See id*.

secure competitor out of the market[105] because the latter's higher production costs cannot be passed along to consumers.[106]

b. Corporate Executives Have Rejected Cybersecurity Because of Its High Opportunity Cost

[25] Every CEO knows that decreasing the chance of her company suffering a massive data breach is as simple as increasing its cybersecurity budget.[107] But it is less simple to measure the benefits of doing so. A CEO cannot point to a lack of cyberattacks as evidence that her investment was effective, and the all-or-nothing nature of cybersecurity means that a CEO's investment was all for nothing if a future breach should ever occur.[108] So, it would be rational for a CEO who is aware of the first and second laws of cybersecurity[109] to consider a large-scale breach inevitable and funnel the bulk of her company's cybersecurity budget towards the easily-quantifiable Return on Investment (ROI) of the first-mover advantage.[110]

---

[105] *See* SCHNEIER, *supra* note 14, at 134; *see also* Bruce Schneier, *How Security Companies Sucker Us with Lemons*, WIRED (Apr. 19, 2007), https://www.wired.com/2007/04/securitymatters-0419/ [https://perma.cc/R7UE-T4BG].

[106] *See* DEAN, *supra* note 94, at 3–4.

[107] See SCHNEIER, supra note 14, at 124.

[108] *See* Greg Ness, *The All or Nothing Cyber Security Paradox*, SECURITY BOULEVARD (May 22, 2018), https://securityboulevard.com/2018/05/the-all-or-nothing-cyber-security-paradox/ [https://perma.cc/XB9L-WHND].

[109] *See* SCHNEIER *supra* note 14, at 1, 26.

[110] *See* SCHNEIER, *supra* note 14, at 124; *see also infra* notes 328, 330.

[26] A recent report from the UK's Warwick School of Business suggests that major companies balk at firing their executives in the wake of a high-profile data breach to avoid compounding their reputational damage.[111] Instead, they tend to increase executive pay for several years afterwards to project solidarity and preserve organizational integrity.[112] This provides CEOs with a perverse incentive to *encourage* cyberattacks against their own companies,[113] and leads to products which trade security for convenience. Take the video conferencing unicorn[114] Zoom, for

[111] *See* DANIELE BIANCHI & ONUR TOSUN, CYBER ATTACKS AND STOCK MARKET ACTIVITY 25–27 (2019).

[112] *See generally id*. (explaining a study that examined 41 publicly traded blue-chip U.S. companies which suffered newsworthy data breaches between 2004 and 2016 and revealed breached companies tended to increase CEO salaries to protect structural concerns, while unaffected companies tended to decrease CEO compensation during the same period).

[113] *See* Schneier, *supra* note 14, at 124; *see also* Maria LaMagna, *After Breach, Equifax CEO Leaves with $18 Million Pension, and Possibly More*, MARKETWATCH (Sept. 26, 2017, 11:06 PM), https://www.marketwatch.com/story/equifax-ceo-leaves-with-18-million-pension-and-maybe-more-2017-09-26 [https://perma.cc/K8Z3-Y4L6] (noting that even if a CEO *does* receive a termination instead of a pay raise after a major breach, she's likely to make off with a generous severance package); *see also* Catalin Cimpanu, *Hack Cost Equifax Only $87.5 Million—For Now*, BLEEPING COMPUTER (Nov. 11, 2017, 3:00 AM), https://www.bleepingcomputer.com/news/business/hack-cost-equifax-only-87-5-million-for-now/ [https://perma.cc/J9K9-H9TW] (explaining, for example, although Richard Smith, Equifax's former CEO, took an early retirement after his company's disastrous 2017 data breach (*see infra* Part IV(A)), he absconded with an $18 million pension on top of a $90 million bonus, even though the breach was estimated to have cost his former company over $600 million); *see also* John McCrank & Jim Finkle, *Equifax Breach Could Be Most Costly in Corporate History*, REUTERS (Mar. 2, 2018, 10:05 AM), https://www.reuters.com/article/us-equifax-cyber/equifax-expects-net-200-million-in-breach-related-costs-in-2018-idUSKCN1GE257 [https://perma.cc/9FKW-GCNG].

[114] As used here, the term "unicorn" highlights the rarity of Zoom's situation within their industry.

example, which enjoyed one of the most successful Initial Public Offerings (IPOs) of 2019 thanks to a frictionless user experience which allows users to join a call with just a single click.[115] It turned out, however, that Zoom's major selling point was also its major weakness: by omitting the customary authentication steps, Zoom made it trivial for attackers to hijack the webcams of unsuspecting users who clicked on fake links.[116] Yet the company declined to patch this vulnerability, even after it became public knowledge, for the sake of retaining its competitive advantage.[117]

[27] IoT devices are unsecured and unsafe because although IoT manufacturers are perfectly aware of their products' security vulnerabilities, forces beyond their control frustrate their attempts to self-police.[118] These market failures, and their solutions, have their roots in the history of the Internet itself.[119]

---

[115] *See* Priscilla Barolo, *Zoom Receives Morgan Stanley CTO Innovation Award at the 19th TechWeek & CTO Innovation Summit*, ZOOM BLOG (June 5, 2019), https://blog.zoom.us/wordpress/2019/06/05/zoom-receives-morgan-stanley-cto-innovation-award-at-19th-techweek-cto-innovation-summit/ [https://perma.cc/CK2C-P5ZX].

[116] *See* Lily Hay Newman, *A Zoom Flaw Gives Hackers Easy Access to Your Webcam*, WIRED (Jul. 9, 2019), https://www.wired.com/story/zoom-bug-webcam-hackers/ [https://perma.cc/P2BW-SX3X].

[117] *See id*.

[118] *See* Ng, *supra* note 29 (Senator Maggie Hassan: "[I]f you just leave it up to the market to eliminate unsecured devices or raise standards, that's not going to be a short-term or long-term solution.").

[119] *See infra* Part III.

III. ONLY GOVERNMENT INTERVENTION CAN REPAIR THE CRACKS IN THE INTERNET'S FOUNDATION

[28] Both the privacy concerns of today's Internet in general and the safety concerns of the IoT in particular stem from the fact that the architects of the original Internet had no idea what their creation would become.[120] In 1969, a few scientists created ARPANET, the main predecessor to the modern Internet, simply to help a few dozen researchers among three universities exchange messages and files with one another.[121] ARPANET's creators designed it to be a "fast, open, and frictionless" network where every user knew the identity of every other, and security was limited to simply excluding "untrustworthy people."[122] While the Internet quickly evolved beyond its humble beginnings, its security measures did not.[123] To the Internet's overseers, an attack on the network from within was inconceivable,[124] and so the responsibility of guarding against external threats fell on the shoulders of the end users.[125] This end-user security philosophy persisted even as computers became affordable enough for average consumers to connect to the newly created World

[120] *See* SCHNEIER, *supra* note 14, at 23; *see also* Craig Timberg, *A Flaw in the Design*, WASH. POST (May 30, 2015), https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/?utm_term=.f454a924c96d [https://perma.cc/QPQ6-S8J2].

[121] *See* SCHNEIER, *supra* note 14, at 23; *see also* Timberg, *supra* note 120.

[122] *See* SCHNEIER, *supra* note 14, at 23.

[123] *Id.* at 23–24.

[124] *See id.* at 22.

[125] *See id.* at 23; *see also* INTERNET ENGINEERING TASK FORCE, ARCHITECTURAL PRINCIPLES OF THE INTERNET (Brian E. Carpenter, ed., 1996), ("Confidentiality and authentication are the responsibility of end users and must be implemented in the protocols used by the end users . . . .").

Wide Web[126] and as the Internet quickly grew too large for the government to manage.[127]

[29] In the 1990s, budgetary concerns prompted the National Science Foundation to relinquish control of the World Wide Web's infrastructure to a burgeoning industry of Internet service providers (ISPs).[128] Under the ISPs' stewardship, the Internet spread across the globe at an astounding rate.[129] This tectonic shift towards a global economy based on information technology was one of the defining moments of the Information Age.[130]

---

[126] *See* BUREAU OF LABOR STATISTICS, COMPUTER OWNERSHIP UP SHARPLY IN THE 1990S (Mar. 1999), https://www.bls.gov/opub/btn/archive/computer-ownership-up-sharply-in-the-1990s.pdf [https://perma.cc/GP8B-22YT].

[127] *See* Zac Rogers, *Irregular Regulation: Has the Internet Become Too Big to Regulate?*, PSNEWS: TECH TALK (Aug. 19, 2019), https://psnews.com.au/2019/08/19/irregular-regulation-has-the-internet-become-too-big-to-regulate/ [https://perma.cc/EWU8-A4NP]; *see also* Peter H. Lewis, U.S. Begins Privatizing Internet's Operations, N.Y. TIMES (Oct. 24, 1994), https://www.nytimes.com/1994/10/24/business/us-begins-privatizing-internet-s-operations.html [https://perma.cc/WE9D-9PW2].

[128] *See id.* (noting that today, the private sector owns and operates over 90 percent of the Internet's infrastructure, as well as roughly 85 percent of U.S. critical infrastructure (defined as "national security, energy and power, banking and finance, health and safety, communications, and transportation")); *see also* SCHNEIER, *supra* note 14, at 117, 126; *see also* Ash Carter, *The Department of Defense Cyber Strategy*, U.S. DEP'T OF DEFENSE (Apr. 17, 2015), https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf [https://perma.cc/GTN5-TFAL].

[129] *See* Manuel Castells, *The Impact of the Internet on Society: A Global Perspective*, BBVA OPEN MIND, CH@NGE: 19 KEY ESSAYS ON HOW THE INTERNET IS CHANGING OUR LIVES (2014), https://www.bbvaopenmind.com/en/articles/the-impact-of-the-internet-on-society-a-global-perspective [https://perma.cc/5H8E-3ZB8].

[130] *See generally* MANUEL CASTELLS, THE RISE OF THE NETWORK SOCIETY (2d ed. 2011) (highlighting the economic and social dynamics of the information age and how the network society has fully risen on a global scale).

As the number of Internet users skyrocketed, oversight bodies finally realized the need for end-to-end network security,[131] but too late to implement any meaningful changes.

[30] A simple economic principle, the influence of positive network externalities on competitive markets,[132] explains why all global network security proposals have failed. Essentially, collective action paralysis was inevitable because each improvement is worthless if not universally adopted.[133] The lack of coordination among ISPs permanently prevented them from improving their individual portions of the Internet: each waited in vain for its competitors to shoulder the heavy costs of early adoption before acting.[134] As a result, many of the basic building blocks of today's

[131] *See* SCHNEIER, *supra* note 14, at 23.

[132] *See* S. J. Leibowitz & Stephen E. Margolis, *Network Externality: An Uncommon Tragedy*, 8 J. ECON. PERSP. 133, 133 (1994) (summarizing crudely: positive network externalities are the benefits conferred on third parties by a given transaction); *see also* Michael. L. Katz & Carl Shapiro, *Network Externalities, Competition, and Compatibility*, 75 AM. ECON. REV. 424, 436–37 (1985) (explaining that during the 1980s, two economists found that a single member of a competitive market will not adopt a technology of its own volition if it will bear the full cost of doing so and if the benefits of adoption require most firms following suit); *see also* Tyler Moore and Ross Anderson, *The Economics of Information Security*, 314 SCIENCE 610 (2006) (noting that this results in an S-shaped adoption curve, "in which slow early adoption gives way to rapid deployment once the number of users reaches some critical mass." Unsurprisingly, Katz and Shapiro's findings show positive network externalities encourage a "free-rider" mentality).

[133] *See* SCHNEIER, supra note 14, at 23–24.

[134] However, it would have been difficult for these corporations to coordinate to improve the security of the Internet as a whole. § 1 of the Sherman Act prohibits unreasonable combination in restraint of trade. *See* United States v. Assoc. Press, 52 F.Supp. 362, 368 (S.D.N.Y. 1943) (Hand, J.), *citing* Standard Oil Co. v. U.S., 221 U.S. 1 (1910). In a nutshell, coordinated group conduct is unreasonable if it unjustifiably tends to harm the

Internet retain their original security flaws[135] because the proposals intended to repair them were instead relegated to academic purgatory.[136]

competitive process. *See* PHILIP AREEDA & HERBERT HOVENKAMP, ANTITRUST LAW: AN ANALYSIS OF ANTITRUST PRINCIPLES AND THEIR APPLICATION ¶ 1402 (Wolters Kluwer, 4th ed. 2013); s*ee, e.g.*, Fashion Originators' Guild of Am., Inc. v. Fed. Trade Comm'n., 312 U.S. 457, 468 (1941) (holding that an association of dress and textile manufacturers violated federal antitrust laws by linking sales to an agreement not to deal with "design pirates," even though several states had found design piracy to be tortious misconduct). Thus, an ISP trade association which refused to deal with any of its members which did not implement end-to-end security would likely have opened itself up to civil liability from the boycotted companies. *See generally* AREEDA & HOVENKAMP, at ¶ 1477.

[135] *See* SCHNEIER, *supra* note 14, at 22–23 ("There's no security in the Domain Name Service that translates Internet addresses from human-readable names to computer-readable numeric addresses, or the Network Time Protocol that keeps everything in synch. [And] [t]here's no security in the original HTML protocols that underlie the World Wide Web . . .").

[136] *See* SCHNEIER, *supra* note 14, at 23–24 (explaining that the Border Gateway Protocol (BGP) is "how the Internet physically routes traffic through the various cables and other connections between service providers, countries, and continents."); *see also* Stephen Kent, Charles Lynn & Karen Seo, *Secure Border Gateway Protocol (S-BGP)*, 18 IEEE J. ON SELECTED AREAS IN COMM. 582, 584–87 (2000) (noting that because the BGP was designed to trust all its users, "[i]t is highly vulnerable to a variety of malicious attacks, due to the lack of a secure means of verifying the authenticity and legitimacy of BGP control traffic." The S-BGP, or Secure Border Gateway Protocol, proposed security improvements which would prevent unauthorized access of the BGP, ensure the authenticity of point-to-point communication, and validate diversions of Internet traffic. But even though 18 years have passed since that article's publication, none of its proposals have yet been implemented.); *see also* Craig Timberg, *Quick Fix For an Early Internet Problem Lives on a Quarter-Century Later*, WASH. POST (May 31, 2015), https://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/?utm_term=.f3a80c3d846c [https://perma.cc/4WQ4-63EF] ("With infinite numbers of possible paths—some slow and meandering, others quick and direct—BGP gives routers the information they need to pick one, even though there is no overall map of the Internet and no authority charged with directing its traffic.").

[31] With the Internet's insecurities placed in context, the case for government intervention becomes straightforward. The laissez-faire policies of the 1990s[137] created the collective action problems responsible for the cybersecurity vulnerabilities of the Internet of today. Those problems will continue indefinitely until government stakeholders encourage the private sector to act (ideally, through subsidies on upgrade costs coupled with traditional command-and-control regulation[138]). But no such incentives are forthcoming.[139]

---

[137] *See, e.g.*, EV Ehrlich, *A Brief History of Internet Regulation* at 4–5 (Mar. 2014), PROGRESSIVE POL'Y INST., https://www.progressivepolicy.org/wp-content/uploads/2014/03/2014.03-Ehrlich_A-Brief-History-of-Internet-Regulation.pdf [https://perma.cc/UC8T-BU3N] ("The Clinton Administration . . . believed strongly that relying on private investment and markets would be the best route to promoting innovation . . . [This perspective was made manifest in] the Telecommunications Act of 1996 . . . [a] watershed event that marked the end of the telephone age and the beginning of the Internet age . . . .").

[138] Carrots and sticks. Economists' preferred solution to market inefficiencies caused by positive externalities is known as a Pigouvian subsidy. It is, in essence, a subsidy set to the same level as the external benefit, or the value that a consumer "misses out on" and is instead enjoyed by bystanders. *See* Atilla A. Uğur, *Internalizing Externality in the Case of Joint and Separate Productions: Property Rights Regulation as the Public Economy Solution*, 2 INT'L J. BUS. & SOCIAL SCI. 47, 48 (2011). This subsidy shifts the demand curve up until the value to the consumer is equivalent to the value to society as a whole. *See id.* Proper application of Pigouvian subsidies "internalize" positive externalities and bring a market back into efficient equilibrium. *See id.* at 56; *see also* N. Gregory Mankiw et al., *Optimal Taxation in Theory and Practice*, 23 J. ECON. PERSP. 147, 164 (2009). For an example of this theory in action, see generally Benjamin M. Althouse et al., *A Public Choice Framework for Controlling Transmissible and Evolving Diseases*, 107 PROC. NAT'L ACAD. SCI. U.S., 1696–1701 (2010), which provides framework for controlling the spread of measles by subsidizing vaccinations to account for the positive externality of herd immunity.

[139] For many reasons, both political and apolitical. *See infra* Part V(B); *see generally* Klint Finley, *The WIRED Guide to Net Neutrality*, WIRED (May 9, 2018, 7:00 AM), https://www.wired.com/story/guide-net-neutrality/ [https://perma.cc/64ZS-PQEX] (discussing net neutrality and treating internet information equally); *see also 37 Ways Donald Trump Has Remade the Rules for Business*, WALL ST. J. (Jan. 17, 2018 7:00

IV. FROM LAWLESSNESS TO LEGISLATION: THE FITFUL PROGRESS OF PRIVACY REFORM

[32] Today's age of big data and data breaches has created a sustained debate over online privacy,[140] perhaps best defined as "the ability to control data we cannot stop generating, giving rise to inferences we can't predict."[141] The commercial Internet was built on corporations collecting consumer data (generally without informed consent)[142] in exchange for

AM), https://www.wsj.com/articles/how-donald-trump-has-remade-the-rules-for-business-1516190400 [https://perma.cc/UT3B-5GLE] (outlining how the Trump administration has deregulated business in numerous fields). While the FTC has pursued a few manufacturers of flagrantly insecure IoT devices, the enforcement actions of a single agency cannot hope to correct the course of an entire industry. *See* MEGAN GRAY, UNDERSTANDING AND IMPROVING PRIVACY "AUDITS" UNDER FTC ORDERS 3 (2018); *see also* TIM POLK, ENHANCING RESILIENCE OF THE INTERNET AND COMMUNICATION ECOSYSTEM: A NIST WORKSHOP PROCEEDINGS 7 (2017) ("Contributions from all sectors [infrastructure, manufacturing, consumers, academia, and government] will be required to significantly increase the resilience of the [Internet] ecosystem . . . .").

[140] Hence the term "breach fatigue." *See generally* Jennifer Abel, *Don't Let "Breach Fatigue" Leave You Vulnerable to Hackers and Malware*, CONSUMERAFFAIRS (Jan. 5, 2015), https://www.consumeraffairs.com/news/dont-let-breach-fatigue-leave-you-vulnerable-to-hackers-and-malware-010515.html [https://perma.cc/H97S-Q5T3] (discussing hackers and security breach vulnerability).

[141] Andrew Burt, *Privacy and Cybersecurity Are Converging. Here's Why that Matters for People and for Companies*, HARV. BUS. REV., (Jan. 3, 2019), https://hbr.org/2019/01/privacy-and-cybersecurity-are-converging-heres-why-that-matters-for-people-and-for-companies [https://perma.cc/QB7S-BRHA].

[142] *See, e.g.*, Sam Schechner & Marc Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, WALL ST. J. (Feb. 22, 2019 11:07 AM), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636 [https://perma.cc/526P-E6YQ] (revealing that popular smartphone apps send "intensely personal information" such as heart rate, favorited home listings, and ovulation times to Facebook "just seconds after users enter it . . . even if no Facebook account is used to log in and [even] if the end user isn't a Facebook member."); *see also* Teresa Carr, *Your Prescriptions Are Not a Secret*, CONSUMER REPORTS, (Mar. 18, 2016), https://www.consumerreports.org/health-privacy/prescriptions-not-secret/

free and convenient services. Known as "surveillance capitalism,"[143] this business model is a modern illustration of the old marketing aphorism, "if you're not paying for the product, you are the product."[144] But the way tech companies collect and use consumer data has come under fire in recent years. As data breaches occur with increasing frequency, privacy policies are amended to become increasingly opaque.[145] Thankfully, high-profile hacks have prompted an unprecedented bipartisan push for federal privacy reform.[146] The factors responsible for drawing the public's attention to the crisis of privacy merit discussion as they reveal how far removed the country is from an analogous push for IoT safety.

A. Corporate Carelessness Permitted Large-Scale Data Breaches

[33] Treasure troves of personal, financial, and healthcare information command hefty sums on the black market.[147] Hackers acquire this

[https://perma.cc/4YJT-ZAAS] (warning that pharmacies sell prescription records to analytics companies for marketing purposes).

[143] SCHNEIER, *supra* note 14, at 57 (referencing Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH., Apr. 2015, at 75–89).

[144] *See, e.g.*, Richard Serra & Carlota Fay Schoolman, *Television Delivers People*, YOUTUBE (1973), https://www.youtube.com/watch?v=Vfnm5XHsHkc [https://perma.cc/YHX6-4HCU] ("Television delivers people to an advertiser . . . who is the customer . . . . [y]ou are the end product.").

[145] *See* Kevin Litman-Navarro, Opinion, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, N.Y. TIMES (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html [https://perma.cc/64V2-7GAV] (noting that the readability score of Facebook's privacy policy exceeded that of Stephen Hawking's *A Brief History of Time*).

[146] *See infra* Part IV(C).

[147] *See* Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-

sensitive data by pillaging the servers of vulnerable institutions, such as retailers, banks, credit bureaus, hospitals, health insurers, and law firms.[148] The victims of the identity thefts and Medicare frauds resulting from these breaches have their bank accounts drained, their credit scores tarnished, and their peace of mind destroyed.[149]

[34] With so much at stake, it is imperative that the companies which safeguard sensitive consumer data do so with the utmost care, or at the very least, in accordance with basic security practices. Yet, many of the largest data breaches to date occurred not because hackers leveraged never-before-seen vulnerabilities to bypass state-of-the-art defenses,[150] but because their victims failed to adhere to even the most basic of cybersecurity principles.[151] So, rather than painstakingly cracking the codes of digital safes, cybercriminals are casually walking into vaults of data left unguarded and unlocked.

[35] In 2013 and 2014, Target, Neiman Marcus, and Home Depot each suffered large-scale breaches in the same manner: through the physical installation of malware on individual point-of-sale terminals.[152] These attacks exposed the personal information of 180 million customers and 97 million credit cards.[153] In August 2013, Yahoo suffered the largest data

experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ [https://perma.cc/VN2N-583V].

[148] *See* Lily Hay Newman, *The WIRED Guide to Data Breaches*, WIRED (Dec. 7, 2018 9:00 AM), https://www.wired.com/story/wired-guide-to-data-breaches/ [https://perma.cc/T94Y-7H4K] (hereinafter Newman Data Breaches).

[149] *See id*.

[150] These are known as "zero-day exploits" in cybersecurity parlance. *See id*.

[151] *See id*.

[152] *See id*.

[153] *See id*.

breach of all time, exposing the personal information of 3 *billion* accounts to Russian-sponsored hackers thanks to a single Yahoo employee clicking on a phony link in a spear-phishing email.[154] In November 2018, Marriott announced that it had lost the personal data of up to 500 million customers; crucially, the attackers infiltrated the database in 2014 and gradually siphoned away data *for four years* before the system's loss prevention measures noticed anything was amiss.[155] Additionally, in July 2019, Capital One, which uses Amazon's cloud service to store its data, lost the personal information of around 106 million customers (including around 140,000 Social Security numbers) when a former Amazon Web Services employee broke through the bank's firewall and siphoned away its data.[156]

[36] The worst breach of all, both in the significance of the stolen data and in the corporate malfeasance permitting its loss, was the 2017 hack of the credit reporting agency Equifax, which exposed the names, birth dates, addresses, credit cards, and Social Security numbers of almost 150 million individuals.[157] Equifax encouraged this colossal infringement with a history of "laughably bad" security measures,[158] a "lack of accountability"

---

[154] *See* Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSO ONLINE, https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html [https://perma.cc/M5QQ-8X6C] (falling for a spear-phishing email is only slightly more excusable than wiring money to a Nigerian prince).

[155] *See* Newman Data Breaches, *surpa* note 147. *See also* Lily Hay Newman, *How to Protect Yourself from the Great Marriott Hack*, WIRED (Nov. 30, 2018, 11:59 AM), https://www.wired.com/story/marriott-hack-protect-yourself/ [https://perma.cc/XES7-533Z].

[156] *See* Nicole Hong et al., *Capital One Reports Breach Affecting 100 Million Customers, Applicants*, WALL ST. J., https://www.wsj.com/articles/capital-one-reports-data-breach-11564443355 [https://perma.cc/2EW3-NN9Q].

[157] *See* Newman, *supra* note 147.

[158] *See* SCHNEIER, *supra* note 14, at 106.

within its management,[159] and a "complex[] and antiquated" IT system.[160] The House of Representatives called the breach "entirely preventable;"[161] the Senate attributed it to "long-standing" shortcomings and a "neglect of cybersecurity."[162]

[37] Even so, the worst that can be said about Equifax was that it was complacent in its handling of consumer data. The world's largest technology companies (Big Tech), on the other hand, have been complicit in the abuse of their users' privacy rights.

[159] *See* COMM. ON OVERSIGHT AND GOV'T REFORM, 115TH CONG., THE EQUIFAX DATA BREACH 4 (2018).

[160] *See id.*

[161] *See id.* at 2.

[162] STAFF OF S. PERMANENT SUBCOMM. ON INVESTIGATIONS OF THE S. COMM. ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS, 116th CONG., REP. ON HOW EQUIFAX NEGLECTED CYBERSECURITY AND SUFFERED A DEVASTATING DATA BREACH 6 (2019). *See generally In re* Equifax Inc. Sec. Litig., 357 F. Supp. 3d 1189, 1223–24 (N.D. Ga. 2019) (holding that Equifax's repeated pronouncements of the strength of its cybersecurity before its disclosure of the breach went beyond "inactionable puffery" because reasonable investors would assign weight to the specificity and volume of those misrepresentations while making their investment decisions); Kevin LaCroix, *Equifax Data Breach-Related Securities Suit Dismissal Motion Denied in Part, Granted in Part*, The D&O Diary (Jan. 30, 2019) https://www.dandodiary.com/2019/01/articles/securities-litigation/equifax-data-breach-related-securities-suit-dismissal-motion-denied-part-granted-part/ [https://perma.cc/S83S-WWF5] (finding that, thanks for its unparalleled disregard for data security, Equifax earned the dubious distinction of being the first defendant in a data breach-related securities fraud class action to lose its motion to dismiss).

B. Big Tech's Privacy Violations Finally Reach a Tipping Point

[38] In April 2019, Bloomberg reported that Amazon, which has sold more than 100 million Alexa-equipped devices,[163] trains its digital assistant by using thousands of its employees to listen to and transcribe Alexa recordings without its customers' knowledge.[164] Also, Google, which boasts over one billion unique users per day,[165] was fined €50 million by a French regulatory body earlier this year for targeting users with personalized ads without first obtaining their consent.[166] But neither of these major technology companies' privacy violations captured the public consciousness in the way Facebook's Cambridge Analytica scandal did. Like the Equifax data breach, Cambridge Analytica marked a fundamental and irreversible shift in consumer perception of the corporations in which we have entrusted our data.

[39] To say that Cambridge Analytica hacked Facebook is inaccurate, as it impliedly absolves Facebook of responsibility. In fact, Cambridge Analytica exploited an undisclosed feature in Facebook's app development interface that allowed third-party developers to collect data

---

[163] *See* Adam Westlake, *Amazon Confirms Alexa Device Sales Numbers, and It's a Lot*, SLASH GEAR (Jan. 5, 2019), https://www.slashgear.com/amazon-confirms-alexa-device-sales-numbers-and-its-a-lot-05560097/ [https://perma.cc/6ZQM-9HWU].

[164] *See* Matt Day et al., *Amazon Workers Are Listening to What You Tell Alexa*, BLOOMBERG (Apr. 10, 2019), https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio [https://perma.cc/6TSF-6DJZ].

[165] *See* Danny Sullivan, *Google Now Handles At Least 2 Trillion Searches Per Year*, SEARCH ENGINE LAND (May 24, 2016), https://searchengineland.com/google-now-handles-2-999-trillion-searches-per-year-250247 [https://perma.cc/Y4HG-TWEV].

[166] *See* Klint Finley, *EU Privacy Law Snares Its First Tech Giant: Google*, WIRED (Jan. 22, 2019), https://www.wired.com/story/eu-privacy-law-snares-first-tech-giant-google/ [https://perma.cc/QY3P-93F8].

from the *friends* of their apps' users as well as the users themselves.[167] Between 2013 and 2015, 270,000 people took a Facebook quiz developed by Aleksandr Kogan, a psychology researcher at Cambridge University.[168] Kogan scraped the personal data of these 270,000 plus that of around 87 million of their unsuspecting Facebook friends and sold the lot to Cambridge Analytica,[169] whose vice president, Steve Bannon, was also the chief executive of Donald Trump's 2016 presidential campaign.[170] The Trump campaign used the data to identify a small slice of "persuadable" voters in each electoral district and target those voters with ads precisely tailored to appeal to their individual personalities.[171]

[40] Facebook's senior executives, including Mark Zuckerberg, likely learned of Cambridge Analytica's data harvest in the summer of 2016[172]

---

[167] *See* Kurt Wagner, *Here's How Facebook Allowed Cambridge Analytica to Get Data for 50 Million Users*, VOX: RECODE (Mar. 17, 2018), https://www.vox.com/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data [https://perma.cc/24W8-TMXJ].

[168] *See* Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html [https://perma.cc/9Q9T-6D65].

[169] *See id.*; *see also* Wagner, *supra* note 167.

[170] *See* Jane Meyer, *New Evidence Emerges of Steve Bannon and Cambridge Analytica's Role in Brexit*, THE NEW YORKER (Nov. 17, 2018), https://www.newyorker.com/news/news-desk/new-evidence-emerges-of-steve-bannon-and-cambridge-analyticas-role-in-brexit [https://perma.cc/G3SL-S6XM].

[171] Mike Butcher, '*The Great Hack': Netflix Doc Unpacks Cambridge Analytica, Trump, Brexit and Democracy's Death*, TECHCRUNCH (July 23, 2019), https://techcrunch.com/2019/07/23/the-great-hack-netflix-doc-unpacks-cambridge-analytica-trump-brexit-and-democracys-death/ [https://perma.cc/GD5X-SU4U] (quoting Cambridge Analytica).

[172] *See* Carole Cadwalladr, *Facebook Faces Fresh Questions Over When It Knew of Data Harvesting*, THE GUARDIAN (Mar. 16, 2019), https://www.theguardian.com/technology/

but managed to hide it from the public until the spring of 2018, when one of Cambridge Analytica's former employees blew the whistle and provided the press with a smoking gun: a trove of documents establishing that Facebook permitted Cambridge Analytica to use military-grade psychological warfare tactics on the American electorate.[173] This bombshell prompted the Federal Trade Commission (FTC), the Securities Exchange Commission (SEC), the Department of Justice (DOJ), the FBI, and 38 U.S. state attorneys general, as well as the governments of the UK and the EU, to each open investigations into Facebook over the following months.[174] In February 2019, the UK Parliament concluded its investigation with the extraordinary proclamation that Facebook's leadership were "digital gangsters"[175] whose deceptive practices had genuinely made it impossible to have a free and fair election under existing law.[176]

2019/mar/16/facebook-fresh-questions-data-harvesting-cambridge-analytica [https://perma.cc/67EL-552G].

[173] *See* Carole Cadwalladr, *'I Made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower*, THE GUARDIAN (Mar. 18, 2018, 5:44 EDT), https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump [https://perma.cc/NJT7-6WF8]; *see also* Carole Cadwalladr, *The Great British Brexit Robbery: How Our Democracy Was Hijacked*, THE GUARDIAN (May 7, 2017, 4:00 EDT), https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy [https://perma.cc/VDU8-CRD7].

[174] *See* Carole Cadwalladr, *Cambridge Analytica a Year On: 'A Lesson in Institutional Failure'*, THE GUARDIAN (Mar. 17, 2019 4:00 EDT), https://www.theguardian.com/uk-news/2019/mar/17/cambridge-analytica-year-on-lesson-in-institutional-failure-christopher-wylie [https://perma.cc/B9EW-TXQV].

[175] *See* David Pegg, *Facebook Labelled 'Digital Gangsters' by Report on Fake News*, THE GUARDIAN (Feb. 17, 2019, 19:01 EST), https://www.theguardian.com/technology/2019/feb/18/facebook-fake-news-investigation-report-regulation-privacy-law-dcms [https://perma.cc/D3GB-MS68].

[176] THE GREAT HACK (Netflix 2019) (statement of Carole Cadwalladr at 1:36:00).

C. These Scandals Drew the Ire of the Public and Forced Policymakers to Act

[41] If any good came out of these massive data breaches, human rights abuses, and botched corporate cover-ups, it was that they were shocking enough to stimulate meaningful action among federal stakeholders.[177] Drawing on groundbreaking legislation such as the EU's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA),[178] Congressional leaders in both parties have submitted a series

[177] Cameron Kerry, *Will This New Congress be the One to Pass Data Privacy Legislation?*, LAWFARE (Jan. 11, 2019, 8:00 AM), https://www.lawfareblog.com/will-new-congress-be-one-pass-data-privacy-legislation [https://perma.cc/R8VC-PADE].

[178] Commission Regulation 2016/679, 2016 O.J. (L 119) 1; CAL. CIV. CODE § 1798.100 (West 2018). Commission Regulation 2016/679, art. 13–21, 2016 O.J. (L 119) 1, 48–54 (the GDPR grants the following privacy rights to EU residents and to all individuals whose data is collected by EU businesses and organizations: 1) the right to be informed of what their data will be used for, how long it will be stored, and with whom it will be shared; 2) the right to access their data; 3) the right to rectification of inaccurate data; 4) the right to erasure of unnecessary or non-consensually collected data; 5) the right to restrict the use of data when its accuracy or processing is in dispute; 6) the right to portability (i.e., the right to securely move, copy, or transfer their data from one service to another); and 7) the right to object to the processing of their data for public interest or direct marketing purposes). CAL. CIV. CODE §§ 1798.100–1798.120; CAL. CIV. CODE § 1798.150 (besides adopting the GDPR's rights of information, access, erasure, restriction, and portability, the CCPA creates a duty for businesses to take reasonable steps to secure the data they collect and grants consumers a private right of action against businesses which disregard that duty and then suffer a data breach). *See* Rita Heimes & Sam Pfeifle, *New California Privacy Law to Affect More Than Half a Million U.S. Companies*, INT'L ASS'N OF PRIVACY PROFESSIONALS (July 2, 2018), https://iapp.org/news/a/new-california-privacy-law-to-affect-more-than-half-a-million-us-companies/ [https://perma.cc/QQ5R-JUJE] (the CCPA's passage was a watershed moment in American privacy reform because when it goes into effect in 2020, it will force every major U.S. company to adopt a separate set of standards for California residents). *See, e.g.*, *IAB Urges Congress to Pass Federal Privacy Legislation to Protect Consumers & Avoid Patchwork of State Laws*, INTERACTIVE ADVERTISING BUREAU (Feb. 26, 2019), https://www.iab.com/news/iab-urges-congress-to-pass-federal-privacy-legislation-to-protect-consumers-avoid-patchwork-of-state-laws/ [https://perma.cc/T2NL-YPZ9] (the

of extraordinary bills establishing high-level corporate disclosure requirements much like those of the Sarbanes-Oxley Act and creating duties of "care, loyalty, and confidentiality" for the handling of consumer data.[179] Even Intel, an industry leader in both central processing unit (CPU) manufacturing[180] and autonomous vehicle development,[181] submitted a reasonably pro-consumer bill which would give teeth to existing voluntary privacy standards[182] by subjecting violators to criminal and civil penalties with eye-popping punitive measures.[183]

[42] Some regulators, though, remain skeptical that these proposed measures will go far enough and are searching for alternative ways to hold Big Tech accountable.[184] This skepticism has kindled renewed interest in

prospect of a regulatory "patchwork" of conflicting state standards has motivated many major corporations to campaign for preemptive federal privacy legislation).

[179] *See* Kerry, *supra* note 177.

[180] *See AMD vs Intel Market Share*, CPU BENCHMARKS (updated Feb. 8, 2019), https://www.cpubenchmark.net/market_share.html [https://perma.cc/Q7C7-M4WB].

[181] *See Intel Completes Tender Offer for Mobileye*, INTEL NEWSROOM (Aug. 8, 2017), https://newsroom.intel.com/news-releases/intel-mobileye-acquisition/ [https://perma.cc/V7FG-6WLY].

[182] *See* Innovative and Ethical Data Use Act of 2018, S., 116th Cong. § 3 (as drafted by Intel, Jan. 28, 2019), https://usprivacybill.intel.com/wp-content/uploads/IntelPrivacyBill-01-28-19.pdf [https://perma.cc/Y42Y-9KEC].

[183] Specifically, knowing falsification of the required privacy certification would be subject to a maximum fine of one million dollars or a maximum prison sentence of 10 years, and a violation of any of the codified privacy principles would be subject to damages of $16,500 per individual whose privacy rights were infringed on, with a damages cap of one billion dollars per act or omission. *See id.* at § 6.

[184] David Streitfeld, *To Take Down Big Tech, They First Need to Reinvent the Law*, N.Y. TIMES (June 20, 2019), https://www.nytimes.com/2019/06/20/technology/tech-giants-antitrust-law.html [https://perma.cc/T4SC-PA65].

the viability of antitrust actions against companies such as Facebook, Google, Apple, and Amazon, each of which is alleged to have used its dominant position in its respective market to illegitimately stifle competition, to the detriment of consumer welfare.[185]

[43] The antitrust movement has grown stronger as the impotence of traditional enforcement strategies has become increasingly obvious. For example, the FTC's investigation into Facebook following the shockwaves of the Cambridge Analytica scandal ended with disappointing results for consumer privacy advocates.[186] The settlement "only" required Facebook to pay a mere $5 billion in fines, a rounding error for a company valued at around half a trillion, and accept increased privacy oversight.[187] It omitted

[185] *See* James V. Grimaldi & Brent Kendall, *The Government vs. Big Tech: Arguments Each Side Could Make*, WALL ST. J. (Sept. 9, 2019), https://www.wsj.com/articles/the-government-vs-big-tech-arguments-each-side-could-make-11568031427 [https://perma.cc/6U74-RMKQ]; *see also Apple, Inc. v. Pepper*, 139 S. Ct. 1514, 203 L. Ed. 2d 802 (2019) (allowing a monopolization suit against the company to proceed); Brent Kendall et al., *FTC Antitrust Probe of Facebook Scrutinizes Its Acquisitions*, WALL ST. J. (Aug. 1, 2019), https://www.wsj.com/articles/ftc-antitrust-probe-of-facebook-scrutinizes-its-acquisitions-11564683965?mod=hp_lead_pos2 [https://perma.cc/AJK8-KRF2]; Tripp Mickle, *Apple Dominates App Store Search Results, Thwarting Competitors*, WALL ST. J., (July 23, 2019), https://www.wsj.com/articles/apple-dominates-app-store-search-results-thwarting-competitors-11563897221?shareToken=st745875a69c3b4a5191cc0a2d657fe55b [https://perma.cc/Y2AA-MWED]; Julia Angwin & Surya Mattu, *Amazon Says It Puts Customers First. But Its Pricing Algorithm Doesn't*, PROPUBLICA (Sept. 20, 2016), https://www.propublica.org/article/amazon-says-it-puts-customers-first-but-its-pricing-algorithm-doesnt [https://perma.cc/V5GT-S7C7] ("[T]he company appears to be using its market power and proprietary algorithm to advantage itself at the expense of sellers and many customers."); Natasha Lomas, *Google Fined $2.7BN for EU Antitrust Violations Over Shopping Searches*, TECHCRUNCH (June 27, 2017), https://techcrunch.com/2017/06/27/google-fined-e2-42bn-for-eu-antitrust-violations-over-shopping-searches/ [https://perma.cc/L4PH-88YQ].

[186] *See* Mike Isaac and Natasha Singer, *Facebook Agrees to Extensive New Oversight as Part of $5 Billion Settlement*, N.Y. TIMES (Jul. 24, 2019), https://www.nytimes.com/2019/07/24/technology/ftc-facebook-privacy-data.html [https://perma.cc/P2Y6-WZZS].

[187] *See id.*

all consumer remedies and failed to require Facebook to admit wrongdoing or to hold Zuckerberg personally accountable.[188] Even the head of the FTC's investigatory commission acknowledged the settlement agreement's shortcomings, admitting that his agency's lack of direct oversight authority and the nonexistence of a federal data privacy law severely limited the FTC's capacity to regulate Facebook's privacy violations.[189]

[44] Even so, it would be unfair to characterize the FTC as toothless. A few hours after it disclosed its privacy settlement with Facebook, it confirmed that it was also investigating the company for antitrust violations[190] in tandem with the DOJ, which had just opened independent antitrust investigations into Facebook, Google, Apple, and Amazon.[191] Later that week, the New York Times reported that Chris Hughes, co-founder of Facebook, had begun working with investigators to build a case against his old company.[192] Another layer of scrutiny was added about a

[188] *See* Tony Romm, *Facebook Will Have to Pay a Record-Breaking Fine for Violating Users' Privacy. But the FTC Wanted More.*, WASH. POST (Jul. 22, 2019), https://www.washingtonpost.com/technology/2019/07/22/facebook-vs-feds-inside-story-multi-billion-dollar-tech-giants-privacy-war-with-washington/?dlbk [https://perma.cc/F8YA-AHG4].

[189] *See* Cecilia Kang, *The Man Deciding Facebook's Fate*, N.Y. TIMES (Mar. 8, 2019), https://www.nytimes.com/2019/03/08/technology/ftc-facebook-joseph-simons.html [https://perma.cc/3E4X-8Q3R].

[190] *See* Mike Isaac & Natasha Singer, *Facebook Antitrust Inquiry Shows Big Tech's Freewheeling Era Is Past*, N.Y. TIMES (Jul. 24, 2019), https://www.nytimes.com/2019/07/24/technology/facebook-ftc-antitrust-investigation.html [https://perma.cc/S2T4-DYFT].

[191] *See* Brent Kendall, *Justice Department to Open Broad, New Antitrust Review of Big Tech Companies*, WALL ST. J. (Jul. 23, 2019, 5:34 PM), https://www.wsj.com/articles/justice-department-to-open-broad-new-antitrust-review-of-big-tech-companies-11563914235 [https://perma.cc/DY9C-CMT2].

[192] *See* Steve Lohr, *Chris Hughes Worked to Create Facebook. Now, He Is Working to Break It Up.*, N.Y. TIMES (Jul. 25, 2019), https://www.nytimes.com/2019/07/25/

month later, when a group of state attorneys general announced that they would be joining forces with the DOJ to conduct their own investigations of Google, Facebook, Amazon, and Apple.[193] These revelations rattled Big Tech, confirming that government stakeholders had begun to take a far broader position on the regulatory potential of antitrust law than they did in decades past.

[45] Because breaking up Big Tech is one of the few issues that both parties agree on[194] and has even been endorsed by several prominent Democratic presidential candidates,[195] the subjects of these antitrust investigations may soon be forced to adopt pro-consumer privacy policies as part of their campaigns against dissolution. But while society needs IoT safety reform just as sorely as it needed Internet privacy reform, it cannot tolerate the years of corporate carelessness and government indifference which preceded that privacy reform. The cost of a data breach can be measured in dollars, but the cost of a hack on a power grid, automobile, or airplane will be measured in human lives.

technology/chris-hughes-facebook-breakup.html [https://perma.cc/GM3P-A8YU].

[193] *See* John D. McKinnon & Brent Kendall, *Attorneys General to Move Forward with Antitrust Probe of Big Tech*, WALL ST. J. (Aug 19, 2019), https://www.wsj.com/articles/attorneys-general-to-move-forward-with-antitrust-probe-of-big-tech-11566247753 [https://perma.cc/RNA6-7XUR].

[194] *See* Nellie Bowles, *Fighting Big Tech Makes for Some Uncomfortable Bedfellows*, N.Y. TIMES (July 14, 2019), https://www.nytimes.com/2019/07/14/technology/big-tech-strange-bedfellows.html [https://perma.cc/WL72-X23K].

[195] *See* Mike Dorning, *It's Not Just Warren. The Next Democratic President Is Coming for Your Monopoly*, BLOOMBERG (Jul. 3, 2019), https://www.bloomberg.com/news/articles/2019-07-03/the-next-democratic-president-is-coming-for-your-monopoly [https://perma.cc/TJ2X-A5YM].

V. CONSUMER SENTIMENT PRECLUDES THE FEDERAL GOVERNMENT FROM REFORMING IOT SAFETY AS IT IS REFORMING PRIVACY [196]

[46] More than a dozen different cybersecurity guidelines for IoT design exist, each of which could serve as a template for federal policymaking.[197] But, like current privacy standards, these cybersecurity guidelines are paper tigers and are therefore largely ignored by the industry they purport to regulate.[198] Because technology companies are among the nation's largest lobbyists,[199] Congress is unlikely to give teeth

[196] The current landscape of state IoT cybersecurity legislation leaves much to be desired. California rushed to pass the nation's first IoT cybersecurity law in 2018, which provides that all connected devices offered for sale in the state beginning in 2020 must be designed with "reasonable security feature or features." CAL. CIV. CODE § 1798.91.04(a). This ostensibly strove to adopt "security by design," a favored IoT development philosophy because most consumer IoT devices are built for quantity not quality and thus can be patched only with difficulty or not at all. *See* Taazaa, *supra* note 4; *see also* SCHNEIER, *supra* note 14, at 34–40. At face value, this provision seems like a first step towards a federal IoT cybersecurity law. *Cf.* Calif. Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.120, 1798.150 (2018). But the cybersecurity community vehemently criticized the California law as regressive, superficial, and vague. *See, e.g.*, Robert Graham, *California's Bad IoT Law*, ERRATA SEC. (Sept. 10, 2018), https://blog.erratasec.com/2018/09/californias-bad-iot-law.html#.XY-mN0ZKiUk [https://perma.cc/3ZR4-XFQZ]. Nor did the law establish a private right of action, which further handicaps its actual effectiveness. § 1798.91.06(e). Future state IoT cybersecurity legislation should follow the CCPA's lead and confine itself to widely recognized principles, else it risks doing more harm than good.

[197] *See* SCHNEIER, *supra* note 14, at 109.

[198] *See id.*

[199] *See* SCHNEIER *supra* note 14, at 154; *see also* Rani Molla, *Google, Amazon, and Facebook All Spent Record Amounts Last Year Lobbying the U.S. Government*, RECODE (Jan. 23, 2019), https://www.vox.com/2019/1/23/18194328/google-amazon-facebook-lobby-record [https://perma.cc/5ZD5-AES3].

to these standards without being compelled to do so by an Equifax- or Cambridge Analytica-level scandal.[200]

A. All Meaningful Legislation, Lacking Impetus, is Dead on Arrival

[47] Over the last several years, Senators Ed Markey (D–MA) and Richard Blumenthal (D–CT), ranking members of the Commerce, Science, and Transportation Committee, have spearheaded a campaign to establish cybersecurity standards for the increasingly connected automobile and aviation industries.[201] One of their bills would require automakers, through National Highway Transportation Safety Administration (NHTSA) regulations, to (1) safeguard against fatal hacking attacks by taking "reasonable measures" to isolate critical systems from non-critical systems, evaluate vulnerabilities, and "immediately detect, report, and stop" attempts to take over control of the vehicle; and (2) "inform consumers" of the vehicle's cybersecurity protections by affixing an "easy-to-understand graphic" to the window of each new car for sale.[202] Another bill would require air carriers and manufacturers to take "reasonable measures" to protect against hacking attacks by isolating

[200] *See generally* Martin Lipton et al., *It's Time to Adopt the New Paradigm*, HARV. L. SCH. F. ON CORP. GOVERNANCE AND FIN. REG. (Feb. 11, 2019), https://corpgov.law.harvard.edu/2019/02/11/its-time-to-adopt-the-new-paradigm/ [https://perma.cc/EY6Y-856Q] ("It must be recognized that employee and public discontent lead to populism, and populism may well lead to state corporatism.").

[201] *See Senator Markey and Blumenthal Reintroduce Legislation to Improve Cybersecurity of Vehicles and Airplanes*, MARKEY.SENATE.GOV (Mar. 22, 2017), https://www.markey.senate.gov/news/press-releases/senator-markey-and-blumenthal-reintroduce-legislation-to-improve-cybersecurity-of-vehicles-and-airplanes [https://perma.cc/XU5A-D39P].

[202] *See* David Bender, *Senators Reintroduce Cybersecurity Legislation for Cars and Planes*, COVINGTON (Mar. 22, 2017), https://www.insideprivacy.com/data-security/cybersecurity/senators-reintroduce-cybersecurity-legislation-for-cars-and-planes/ [https://perma.cc/NL3Q-5YLP].

critical systems from non-critical systems and updating cybersecurity standards based on the results of periodic vulnerability tests.[203] Neither bill has reached the Senate floor.

[48] In August 2017, Senators Mark Warner (D–VA), Maggie Hassan (D–NH), Ron Wyden (D–OR), and Cory Gardner (R–CO) introduced a bill which would have required all government-purchased IoT devices to be free from known vulnerabilities and be capable of timely updates.[204] But like the bills proposed by Senators Markey and Blumenthal, it never made it out of committee.[205] In fact, the only piece of federal IoT-specific legislation to pass either chamber of Congress to date is a cursory measure which would simply require the U.S. Department of Commerce to survey the current state of the industry.[206] This bill, titled the SMART IoT Act, is merely intended to encourage cross-agency collaboration and to provide stakeholders with "the first compendium of essentially who is doing what in the IoT space,"[207]—a far cry from the unambiguous cybersecurity standards for which experts have so extensively advocated.[208] That prominent business interests such as the Retail Industry Leaders

[203] *See id.*

[204] S. 1691, 115th Cong. (2017).

[205] *See id.*; *see also* S. 680, 115th Cong. (2017); S. 679, 115th Cong. (2017).

[206] H.R. 6032, 115th Cong. § 2 (2018).

[207] *Internet of Things Legis.: Hearing Before the Subcomm. on Digital Com. and Consumer Protection of the Comm. on Energy and Com*., 115th Cong. at 6 (2018) (statement of Rep. Walden, Chairman, H. Comm. on Energy and Com.).

[208] *See, e.g.*, SCHNEIER, *supra* note 14, at 145–50 (advocating for the creation of a new government agency or other measures to combat ambiguity in regulation electronic platforms).

Association[209] support the half-measures of the SMART IoT Act[210] signifies that consumer advocates should not.

[49] Like the Internet privacy legislation submitted during the Obama administration, all pending legislation seeking to improve the safety and security of IoT devices is doomed to fail because the public has not yet appreciated the significance of the issue. Without public awareness, corporations are free to lobby against reform without pushback.[211]

B. Government Agencies are Hindered by Procedural Thickets and Misaligned Incentives

[50] Section 553 of the Administrative Procedure Act of 1946 outlines a simple process for agencies to follow when enacting new regulations.[212] First, the agency puts the public on notice of its proposed rules or the issues it intends to resolve.[213] Next, the agency gives "interested persons"

[209] Corinne Ruff, *Which Retailers Spend the Most on Lobbying?*, RETAIL DIVE (July 11, 2018), https://www.retaildive.com/news/which-retailers-spend-the-most-on-lobbying/527085/ [https://perma.cc/5NM6-JMAW].

[210] *See* Kathleen McGuigan & Autumn Moore, Comment Letter on U.S. Consumer Product Safety Comm'n Hearing on the Internet of Things and Consumer Product Hazards (June 15, 2018) (written on behalf of the Retail Indus. Leaders Ass'n), https://www.regulations.gov/document?D=CPSC-2018-0007-0056 [https://perma.cc/T6LK-7NA6].

[211] *See, e.g.*, Chamber of Commerce of the United States of America, Comment on U.S. Consumer Product Safety Comm'n Hearing on the Internet of Things and Consumer Product Hazards (June 15, 2018), https://www.regulations.gov/document?D=CPSC-2018-0007-0046 [https://perma.cc/G7R7-ADRN] (exhorting the Consumer Product Safety Commission (CPSC) to "foster innovation [of the IoT] with a light-touch approach," and to "eschew regulatory action," admonishing the CPSC to *"allow the market, not agency-imposed certification requirements, to drive adoption of best security practices."*) (emphasis added).

[212] 5 U.S.C. § 553(b) (1946).

[213] *See id.* § 553(b)(3).

the opportunity to contribute written comments containing data, views, or arguments on the proposed rules.[214] Finally, after the agency has issued its final rules, it must provide a statement of "basis and purpose" on the intent of the rules and in response to significant comments it received from the public.[215] This process is interchangeably known as "notice-and-comment rulemaking" or "informal rulemaking"[216] and was historically the preferred method of regulatory rule promulgation.[217] But over the latter half of the twentieth century, this straightforward process ossified[218] into a tangled mess of complications and controversies, causing many agencies to forgo it entirely.[219] This ossification led scholars to lament the contemporary impracticality of a procedural tool once considered a

[214] 5 U.S.C. § 553(c) (2012).

[215] *See id.* § 553(c); Perez v. Mortg. Bankers Ass'n, 135 S. Ct. 1199**,** 1203 (2015).

[216] "Formal rulemaking," which takes place on the record in a courtroom setting, where interested persons get to testify and cross-examine adverse witnesses, has been all but abandoned in modern agency proceedings. *See generally* Kent Barnett, *How the Supreme Court Derailed Formal Rulemaking*, 85 GEO. WASH. L. REV. ARGUENDO 1, 3 (2017). The Court in *United States v. Florida East Coast Ry. Co.*, 410 U.S. 224, 240–41 (1973), presumed formal rulemaking inferior to informal rulemaking, therefore, this article focuses solely on the latter.

[217] *See* Thomas O. McGarity, *Some Thoughts on "Deossifying" the Rulemaking Process*, 41 DUKE L.J. 1385, 1385 (1992) ("As the "rulemaking era" dawned in the early 1970s, the courts, commentators, and most federal agencies agreed that informal rulemaking under § 553 of the Administrative Procedure Act (APA) offered an ideal vehicle for making regulatory policy."). Also, "[i]nformal rulemaking was originally designed to avoid the procedural quagmires that had ensnared formal rulemaking and adjudication. Agencies that elected to make broad policy through informal rulemaking would not be subject to time-consuming discovery, unnecessary rules of evidence, and wasteful cross-examination." *Id.* at 1398.

[218] The term "ossified" was coined by E. Donald Elliott, former General Counsel of the Environmental Protection Agency. *See id.* at 1385–86.

[219] *See id.* at 1436.

paragon of policymaking and forced agencies to develop new policies through reactive adjudication or not at all.[220]

[51] An ossified bureaucracy is bad enough. An ossified bureaucracy crippled by self-interest is far worse. The public-choice school of economics argues that the administrative state suffers from two fundamental shortcomings comparable to the private sector's market failures: rent-seeking and regulatory capture.[221] "Rents," as used here, refers to "the above-normal profits of a privileged firm," thus "rent-seeking" connotes corporate seeking of political favoritism, generally at the expense of the common good.[222] Regulatory capture is rent-seeking writ large: when a special interest group's lobbying efforts are so successful as to realign the interests of the agency regulating it with the interests of the special interest group itself, that agency is "captured."[223] A captured agency provides regulatory privileges, tax breaks, kickbacks, and general economic protectionism to the corporations it was commissioned to keep in check.[224]

[52] IoT manufacturers have thus far achieved remarkable success in their rent-seeking.[225] Through record lobbying expenditures,[226] they

[220] *See id.* at 1386.

[221] *See* Adam Thierer & Brent Skorup, *A History of Cronyism and Capture in the Information Technology Sector*, 18 J. TECH. L. & POL'Y 131, 135–37 (2013).

[222] *Id.* at 136.

[223] *See id.* at 137–38; SCHNEIER, *supra* note 14, at 155.

[224] *See* Thierer & Skorup, *supra* note 221, at 142.

[225] *See* SCHNEIER, *supra* note 14, at 154–55.

[226] *Id.* at 154 ("[T]hey're now spending twice what the banking industry does, and many times more than oil companies, defense contractors, and everyone else.").

delayed FTC oversight for years[227] and ensured that all agency-promulgated privacy standards would be nigh impossible to enforce.[228] Conflicts of interest prevent both the market and the federal government from independently improving the safety and security of the IoT.[229] Hence the need for class action litigation.

IV. IS IT STILL PRACTICABLE TO EFFECT CHANGE FROM INSIDE THE COURTROOM?

[53] These days, the class action is notorious for settlements leading to exorbitant payouts for class counsel but minimal relief for absent class members.[230] But it was not always so. Class action litigation was an

---

[227] *See* FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 48-49 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/C8RL-W3ZG].

[228] *See* SCHNEIER, *supra* note 14, at 109; *cf.* Innovative and Ethical Data Use Act of 2018, S.___, 116th Cong. 9–14 (as drafted by Intel, Jan. 28, 2019), https://usprivacybill.intel.com/wp-content/uploads/IntelPrivacyBill-01-28-19.pdf [https://perma.cc/Y42Y-9KEC].

[229] *See* SCHNEIER, *supra* note 14, at 101.

[230] Any proposed class settlement can be approved only upon a court's finding it "fair, reasonable, and adequate." Fed. R. Civ. P. 23(e)(2). Settlements typically bind absent class members from later bringing their own suits and thus a court which conducts only a cursory review of a submitted settlement agreement is likely to be reversed for abuse of discretion. To avoid this, a court must generally consider the relative strength of the plaintiff's case, the complexity, expense, and extent of further litigation, the likelihood of collusion in reaching the settlement, and whether unnamed class members approve of the settlement terms. *See, e.g.*, Kleen Prods. LLC v. Int'l Paper Co., No. 1:10-cv-5711, 2017 WL 5247928 at *2 (N.D. Ill. 2017) (reciting the Seventh Circuit's test for settlement approval). But these procedural safeguards often fail because they align the interests of the class counsel and the defendants against overworked district court judges, who are ill-equipped to challenge not-obviously-unfair-settlements. *See* Ted Frank, *The Problem of Self-Dealing by Class Counsel*, POINT OF LAW (Apr. 17, 2012), http://www.pointoflaw.com/feature/archives/2012/04/the-problem-of-self-dealing-by-

essential driver of institutional change in the latter half of the twentieth century. This article's submission of the class action device as a catalyst for reform of IoT safety standards is a call for the doctrine to return to its original *raison d'être*.

A. The Glory Days: Class Actions Conceived to Bypass the Bureaucracy

[54] The modern class action dates to the Advisory Committee's wholesale revision of Rule 23 of the Federal Rules of Civil Procedure in the early 1960s.[231] A product of the civil rights movement and President Lyndon B. Johnson's Great Society,[232] the refashioned rule was immediately pressed into service by both private firms and public interest

class-counsel.php [https://perma.cc/JT63-XU9E]; *See also In re* Subway Footlong Sandwich Mktg. and Sales Practices Litig., 869 F.3d 551, 557 (7th Cir. 2017) (characterizing a settlement approved by the district court, which would have paid the plaintiffs' attorneys $525,000 and left the class with nothing, as "utterly worthless"); *In re* Walgreen Co. S'holder Litig., 832 F.3d 718, 726 (7th Cir. 2016) (Posner, J.) (overturning a "strike suit" settlement which would have awarded the plaintiffs' attorneys $370,000 while class members would receive only "worthless" shareholder disclosures); *In re* Dry Max Pampers Litig., 724 F.3d 713 (6th Cir. 2013) (scrapping a settlement granting $2.73 million to class counsel but only "illusory" relief to unnamed class members); *In re* Bluetooth Headset Prods. Liab. Litig., 654 F.3d 935, 949 (9th Cir. 2011) (chastising the district court for rubber-stamping a settlement which would provide no relief to absent class members but $800,000 in attorney's fees and for approving the settlement despite its questionable "clear sailing agreement" and "kicker" provisions—compelling indicia of collusion).

[231] *See* David Marcus, *The History of the Modern Class Action, Part I: Sturm und Drang*, 1953–1980, 90 WASH. U. L. REV. 587, 603–09 (2013).

[232] Minutes of the Advisory Committee on Civil Rules, April 28 and 29, 1994 (statement of John P. Frank), in WORKING PAPERS OF THE ADVISORY COMMITTEE ON CIVIL RULES ON PROPOSED AMENDMENTS TO CIVIL RULE 23: VOLUME ONE, 202 (1997), https://www.uscourts.gov/sites/default/files/workingpapers-vol1.pdf [https://perma.cc/5J4C-Y2UB].

groups as pragmatic compensation for bureaucratic inadequacies.[233] For these powerful plaintiffs' advocates, the class action device represented a means to positive social and economic reform which, when prudently deployed, achieved regulatory efficacy while retaining the judiciary's institutional integrity.[234] During those heady early years, consumers' champions Joseph Tydings and Ralph Nader spoke glowingly of the newly expanded role of the federal courts "as a substitute for a captured and inefficient federal bureaucracy" and of the consumer class action as an "exquisite congruence of sanction and relief."[235]

[55] While the Advisory Committee was revising Rule 23, enterprising members of Congress were taking matters into their own hands. Divided party control of the legislative and executive branches and a deepening ideological rift between the parties were causing perennial clashes between Congress and the president over control of the enforcement mechanisms of the federal government.[236] Pressed for a solution and reluctant to add further complexity to the already cumbersome administrative state, progressive legislators paradoxically seized permanent control of the enforcement process by relinquishing it to the

[233] *See supra* Part V(b) (discussing ossification and the economic theory of regulation); *see also* Marcus, *supra* note 231, at 592–93. The other commonly cited purposes of class actions, furthering the goals of judicial efficiency and vindicating the rights of "negative value" plaintiffs, were subordinated to the primary role of the class action as institutional deterrent. *Id.*, n. 20 (*citing* Beverly C. Moore, Jr., *Does It Go Far Enough?*, 63 A.B.A. J. 837, 842 (1977)).

[234] *See* Marcus, *supra* note 231, at 591, 593.

[235] *See id.* at 610 (citing *Class Action Jurisdiction Act: Hearings Before the Subcomm. on Improvements in Judicial Machinery of the Comm. on the Judiciary*, United States Senate, 91st Cong. 1, 34 (1969) (statements of Sen. Tydings and Sen. Nader, respectively)).

[236] *See* SEAN FARHANG, THE LITIGATION STATE: PUBLIC REGULATION AND PRIVATE LAWSUITS IN THE UNITED STATES 12–13 (2010).

private bar, but on their own terms.[237] By incorporating private rights of action into federal statutes, Congress created an enduring and (comparably) efficient enforcement regime outside the purview of future contradictory executive interests.[238]

[56] The spike in popularity of generous private rights of action supplied ample economic incentives for private attorneys to sue as proxies for federal law enforcement.[239] The contemporaneous overhaul of the class action device granted these newly conscripted mercenaries a formidable deterrent: the aggregate pressure of thousands of claims exerted against a single malfeasor.[240] So, they happily spent the following decades assisting underfunded state attorneys general by enforcing compliance of federal employment discrimination, securities fraud, antitrust, and consumer protection statutes.[241] But as the class action device matured, it attracted

[237] *See id.* at 12–13, 32–33.

[238] *See id.*

[239] *See id.* at 33–34. For example, fee-shifting provisions decrease the expected costs of litigation, statutory damages increase its expected benefits, and burden-of-proof-shifting provisions—which place a thumb on the scale in favor of the plaintiffs—increase a suit's probability of success. *See id.* By infusing private rights of action with such incentives, canny Congressmen manipulated market forces to act on their behalf. *See id.* at 37.

[240] Marcus, *supra note* 231, at 593 ("Economies of scale reaped from claim joinder enable an independent, well-financed cadre of private attorneys general to compensate for the inadequacies of government regulators and individual litigants.").

[241] The enforcement provisions of Title VII of the Civil Rights Act of 1964 encouraged victims of employment discrimination to sue in federal court if the Equal Employment Opportunity Commission failed to take up their claim. *See* Victoria J. Meyers, *Title VII Class Actions: Promises and Pitfalls*, 8 LOY. U. CHI. L.J. 767, 767–68 (1977). Securities fraud class actions exploded in popularity after the Ninth Circuit adopted the fraud-on-the-market doctrine in 1975, which "created in effect an irrebuttable presumption of reliance upon proof of the misstatement's materiality." *See* Marcus, *supra* note 231, at 632 (citing Blackie v. Barrack, 524 F.2d 891, 906 (9th Cir. 1975)). Private antitrust claims spiked as progressive judges came to view the revised Rule 23 "as an extension

the attention of unscrupulous plaintiffs' attorneys seeking lucrative paydays, which led to the "litigation explosion" of the 1970s,[242] intense scrutiny of mass tort and securities fraud class actions in the 1980s, and a heated dispute over the limits of judicial legitimacy.[243] When the inevitable backlash came, it marked the beginning of the end of the class action's dominance over the litigation landscape.

B. Fall from Grace: The Narrative Shifts from Sincere to Cynical

[57] The last few decades have seen regular restrictions to the limits of class action litigation to increasingly favor defendants over plaintiffs in both the legislative and judicial branches. This shift began in the mid-1990s, as institutional critics stoked fears of collusion in mass tort settlements,[244] accounting firms and technology companies joined forces to denounce an explosion of securities fraud class actions,[245] and class-

. . . of the deterrent policies of . . . § 4 of the Clayton Act." *See id.* at n. 287 (*quoting* Ungar v. Dunkin' Donuts of Am., Inc., 68 F.R.D. 65, 150 (E.D. Pa. 1975)). And major consumer protection statutes, such as the Truth in Lending Act of 1968, the Magnuson-Moss Warranty Act of 1975, and the Fair Debt Collection Practices Act of 1977, were enacted with private rights of action reinforced with provisions endorsing class treatment. *See* 15 U.S.C. § 1640(a)(2)(B) (2012); 15 U.S.C. § 1692k(a)(1)(B) (2012); 15 U.S.C. § 2310(e) (2012).

[242] A proliferation of lawsuits during this period embedded the concept of the "right to sue"—perhaps the most distinctly American of all positive rights—firmly within the public consciousness. This pathological litigiousness is perhaps best characterized as a "national disease" that prevents Americans from "tolerat[ing] more than five minutes of frustration without submitting to the temptation to sue." *See* FARHANG, *supra* note 236, at 14.

[243] *See* David Marcus, *The History of the Modern Class Action, Part II: Litigation and Legitimacy*, 1981–1994, 86 FORDHAM L. REV. 1785, 1788–89 (2018).

[244] *See id.* at 1827–28.

[245] *See id.* at 1831 (citing AM. INST. OF CERTIFIED PUB. ACCOUNTANTS, *in* THE PUBLIC INTEREST: A SPECIAL REPORT BY THE PUBLIC OVERSIGHT BOARD OF THE SEC PRACTICE

actions-as-instruments-of-institutional-change became the exception, not the rule. A coincident series of watershed federal appellate decisions cemented the narrative of class action overreach[246] and signaled to Congress the need for reform of the reforming device.[247] This pressure

5 (1993)); *see also* Michael J. Cook et al., *The Liability Crisis in the United States: Impact on the Accounting Profession*, J. ACCT., Nov. 1992, at 18, 19; Richard I. Miller, *Litigation Crisis Imperils Accounting Profession,* ACCT. TODAY, March 14, 1994, at 32, 33.

[246] *See In re* Rhône-Poulenc Rorer, Inc., 51 F.3d 1293, 1299–1302, 1304 (7th Cir. 1995) (Posner, J.) (writing that certification of a class action forces defendants "to stake their companies on the outcome of a single jury trial, or be forced by fear of the risk of bankruptcy to settle even if they have no legal liability," determining the district court abused its discretion in certifying on an amalgam of negligence standards, and reversing with a writ of mandamus); Castano v. Am. Tobacco Co., 84 F.3d 734, 737, 741–44 (5th Cir. 1996) (decertifying a nationwide class of "nicotine-dependent persons" after chastising the district court for failing to consider the effect of variations in state law on FED. R. CIV. P. 23's commonality and manageability requirements); *In re* Am. Med. Sys., Inc., 75 F.3d 1069, 1084–85 (6th Cir. 1996) (finding that a class of plaintiffs claiming they had suffered assorted injuries from penile implants did not satisfy FED. R. CIV. P. 23's commonality requirement and decertifying with a writ of mandamus); Amchem Prods., Inc. v. Windsor, 521 U.S. 591, 617–18, 622, 625 (1997) (noting that plaintiffs had become ever more "adventuresome" in their deployment of the class action device in the decades since its introduction and decertifying a particularly adventuresome settlement-only class for its failure to comply with Fed. R. Civ. P. 23's commonality and adequacy requirements); Ortiz v. Fibreboard Corp., 527 U.S. 815, 863 (1999) (heightening the criteria for certifying a settlement class on a limited fund theory to such an extent as to spell the death knell of the doctrine).

[247] *See* Marcus, *supra* note 243, at 1832. In a direct response to the lobbying by business interests against the securities fraud class action, Congress passed the Private Securities Litigation Reform Act (PSLRA) in 1995 over President Clinton's veto, which cut down on the number of certifiable securities fraud class actions by heightening various pleading requirements, preventing discovery until after the motion to dismiss stage, and giving judges greater oversight over conflicts of interest between class counsel and class members. PSLRA, Pub. L. No. 104–67, 109 Stat. 737, 737-38, 741, 747, 764-65 (1995) (codified in scattered sections of 15 U.S.C.).

eventually led to the passage of the Class Action Fairness Act (CAFA) of 2005.[248]

[58] CAFA capitalized on an increasingly negative public perception of plaintiffs' lawyers[249] to create original federal diversity jurisdiction for class actions[250] and implement a special removal provision for state class actions[251] to combat unfair settlements and forum-shopping.[252] Consumer organizations and civil rights groups criticized these defendant-friendly initiatives for stripping states of their rights and overburdening the federal docket, to no avail.[253] The number of class actions in federal court soared

[248] *See* Anna Andreeva, *Class Action Fairness Act of 2005: The Eight-Year Saga is Finally Over*, 59 U. MIAMI L. REV. 385, 386–88 (2005) (describing how Congress began the long process of reforming the class action device in 1998 and re-introduced the bill which became CAFA six times before its successful passage in 2005).

[249] *See* Thomas A. Donovan, *Proposed Class Action Legislation Will Not Do Much to Improve a Lawyer's Image*, 50 FED. LAW. 30, 31 (2003).

[250] *See* 28 U.S.C. §§ 1332(d)(2) (5)(B)(6) (2019) (creating original diversity jurisdiction over class actions in which there is diversity of citizenship among parties, there are greater than 100 class members, and the aggregate amount in controversy exceeds $5 million).

[251] 28 U.S.C. § 1453(b) (2019) ("A class action may be removed to a district court of the United States . . . without regard to whether any defendant is a citizen of the State in which the action is brought, [and] such action may be removed by any defendant without the consent of all defendants.").

[252] *See* Andreeva, *supra* note 248, at 392–93.

[253] *See id.* at 405–10.

soon after CAFA's passage,[254] a boon for the most powerful plaintiffs' firms but a detriment to all others.[255]

[59] The United States Supreme Court has likewise whittled down the scope of class action litigation over the last decade,[256] mainly in a series of opinions enforcing class action waivers and arbitration clauses in consumer and employee contracts.[257] These business-friendly decisions

[254] *See* THOMAS E. WILLGING & EMERY G. LEE III, THE IMPACT OF THE CLASS ACTION FAIRNESS ACT OF 2005 ON THE FEDERAL COURTS: THIRD INTERIM REPORT TO THE JUDICIAL CONFERENCE ADVISORY COMMITTEE ON CIVIL RULES 21 (2007). Preliminary empirical studies on CAFA's impact showed the statute shifted class action activity from state courts to federal courts even as the number of class action filings increased. Emery G. Lee III & Thomas Willging, *The Impact of the Class Action Fairness Act on the Federal Courts: An Empirical Analysis of Filings and Removals*, 156 U. PA. L. REV. 1723, 1748 n.84 (2008).

[255] *See* Howard M. Erichson, *CAFA's Impact on Class Action Lawyers*, 156 U. PA. L. REV. 1593, 1621 (2008).

[256] *See, e.g.*, Microsoft v. Baker, 137 S. Ct. 1702, 1706–07 (2017) (holding that federal courts of appeals lack jurisdiction to review denials of certification after the plaintiffs have voluntarily dismissed their claims with prejudice); Bristol-Meyers Squibb Co. v. Superior Court, 137 S. Ct. 1773, 1779–84 (2017) (holding that state courts lack specific jurisdiction over claims by nonresidents unrelated to a defendant's activities in that state); Cal. Pub. Emps.' Ret. Sys. v. ANZ Sec., Inc., 137 S. Ct. 2042, 2048–54 (2017) (clarifying that *American Pipe* tolling is equitable rather than legal and thus only tolls statutes of limitation and not statutes of repose); China Agritech, Inc. v. Resh, 138 S. Ct. 1800, 1805-11 (2018) (further diminishing the scope of *American Pipe* tolling by holding that it only applies to individual suits after a denial of class certification and cannot be used to sustain subsequent class actions).

[257] *See* AT&T Mobility L.L.C. v. Concepcion, 563 U.S. 333, 348–52 (2011) (holding that the Federal Arbitration Act of 1925 preempts state laws which invalidate class arbitration waivers); Am. Express Co. v. Italian Colors Rest., 570 U.S. 228, 232–35 (2013) (extending *Concepcion's* holding to class action claims which had sought shelter from the

had the unintended effect of sanctioning deceitful practices such as predatory lending, wage theft, and discrimination because they lead corporations to realize that the simple act of inoculating contracts of adhesion with individual arbitration clauses would effectively bar all class challenges against them.[258] Just a few months ago, for example, T-Mobile moved to compel arbitration in a class action lawsuit of 50 million customers accusing it of selling their real-time location data to third parties in violation of federal law.[259] Unfortunately for the average citizens caught on the wrong side of this power imbalance, the conservative majority of the post-Scalia Court has made its position clear: individual arbitration is here to stay.[260]

FAA under the Sherman and Clayton Acts); DIRECTV, Inc. v. Imburgia, 136 S. Ct. 463, 466 (2015) (expanding *Concepcion* once again by extending the FAA's scope to state court proceedings); Lamps Plus, Inc. v. Varela, 139 S. Ct. 1407, 1419 (2019) (rejecting the application of a common-law rule that ambiguous contracts are construed against their drafters when the ambiguity in question related to whether plaintiffs may pursue class-wide as opposed to individual arbitration).

[258] *See* Jessica Silver-Greenberg & Robert Gebeloff, *Arbitration Everywhere, Stacking the Deck of Justice*, N.Y. TIMES (Oct. 31, 2015), https://www.nytimes.com/2015/11/01/business/dealbook/arbitration-everywhere-stacking-the-deck-of-justice.html [https://perma.cc/VC36-PTPB].

[259] *See* Jon Brodkin, *T-Mobile Says It Can't Be Sued by Users Because of Forced-Arbitration Clause*, ARS TECHNICA (July 9, 2019, 2:02 PM), https://arstechnica.com/tech-policy/2019/07/t-mobile-demands-forced-arbitration-to-avoid-lawsuit-over-selling-users-data/ [https://perma.cc/NA8T-568H].

[260] *See* Epic Sys. Corp. v. Lewis, 138 S. Ct. 1612, 1619 (2018) (cementing the FAA's dominance over other federal statutes by holding that individual arbitration agreements in employment contracts are enforceable despite § 7 of the National Labor Relations Act); *cf. id.* at 1633, 1647–48 (Ginsburg, J., dissenting) (characterizing the majority's decision as "egregiously wrong" and predicting that the majority's refusal to allow employees collective recourse against wage theft would only encourage their employers to underpay them all the more).

[60] The Supreme Court's contractions of the rights of putative class members extend beyond its fondness for arbitration clauses. *Wal-Mart Stores, Inc. v. Dukes* raised the standard for class certification from a mere formality to essentially on the merits by conflating 23(a)(2)'s "commonality" with 23(b)(3)'s "predominance."[261] *Comcast Corp. v. Behrend* established as prerequisites for certification that plaintiffs show their damages model be "capable of measurement on a class-wide basis" and "measure only those damages attributable to [the defendant's] conduct."[262] More recently, a pair of cases which tightened the requirements for Article III standing became especially relevant to potential class actions against the IoT: *Clapper v. Amnesty Int'l* and *Spokeo v. Robins*.

[61] For the purposes of this piece, Article III of the Constitution requires plaintiffs invoking federal jurisdiction to establish the existence of an "injury-in-fact," an infringement on a legal right both "concrete and particularized" and "actual or imminent" (as distinct from "conjectural" or "hypothetical").[263] In *Clapper*, the Court held that a speculative risk of future injury, even if "objectively reasonable," does not qualify as an "actual or imminent" injury-in-fact.[264] In *Spokeo*, the Court rejected the long-held belief that a violation of a statutory right attached to a private right of action can itself establish standing to vindicate that right in court, creating independent requirements for the "concrete" and "particularized" elements of an injury-in-fact.[265] *Clapper* and *Spokeo* suggest that a putative class of purchasers of an unreasonably insecure and dangerous

[261] *See* Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 349–52 (2011).

[262] Comcast Corp. v. Behrend, 569 U.S. 27, 34–35 (2013).

[263] Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992) (citations omitted).

[264] Clapper v. Amnesty Int'l U.S.A., 568 U.S. 398, 401–02, 409 (2013).

[265] *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016).

IoT device will be precluded from suing its manufacturer until the device actually causes them harm. Indeed, a 2017 Ninth Circuit decision subscribed to this line of reasoning when it refused to recognize a heightened risk of future cyberattacks against certain models of Toyotas as an injury-in-fact.[266]

C. Contemporary Public Policy Supports a Class Action Renaissance

[62] Like the Internet and the IoT, the class action is most readily explained by economics.[267] Rule 23 and its accompanying private rights of action came into being at the tail end of the Keynesian era, when the role of government in business was beyond dispute.[268] But the stagflation and social unrest of the 1970s led the Western world to gradually embrace "shareholder value maximization,"[269] the logical extreme of Hayek and Friedman's neoliberalism, in response to a zeitgeist of democracy in crisis.[270] This ideological revolution led to the era of corporate raiders and

[266] *See* Cahen v. Toyota Motor Corp., 717 Fed. App'x 720, 723 (9th Cir. 2017) (mem.).

[267] *See supra* Parts II(B)(2), III.

[268] *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 40 (2019).

[269] This stands for the idea that the singular responsibility of corporations is to increase profits by any means necessary. *See generally* Michael C. Jensen & William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*, 3 J. FIN. ECON. 306–307 (1976) (discussing literature on maximization and other approaches); Michael C. Jensen & Kevin J. Murphy, *CEO Incentives: It's Not How Much You Pay, But How*, HARV. BUS. REV. (May 1990), https://hbr.org/1990/05/ceo-incentives-its-not-how-much-you-pay-but-how [https://perma.cc/2KJF-T53Q] (arguing for a method of CEO pay that is best suited to maximizing shareholder value as an inherently necessary function of the business).

[270] *See* ZUBOFF, *supra* note 268, at 38–39, 41 ("[T]he cult of the 'entrepreneur' would rise to near-mythic prominence as the perfect union of ownership and management, replacing

Reaganomics and marked a profound reversal from the interventionist policies of the Progressive, New Deal, and Great Society eras[271] as a growing consensus on the "absolute authority of market forces,"[272] prompting policymakers to leave the free market to govern itself.[273] As a relic of the past, the class action fell from prominence as quickly as it had ascended.

[63] Given its thorny history, it is fair to question the class action's present-day viability as a regulatory tool. Still, economic theory is cyclical,[274] and the tides are turning. The primary causes of the 2008 global financial crisis were the "widespread failures in financial regulation . . . corporate governance, and risk management" within the shadow banking system[275] produced by decades of adherence to neoliberal doctrine. This near-total collapse of the American economy even plunged

---

the rich existential possibilities of the [historically marginalized] with a single glorified template of audacity, competitive cunning, dominance, and wealth.").

[271] *See id.* at 40.

[272] *Id.* at 39.

[273] *See id.* at 40.

[274] *See* Erik S. Reinert, *The Terrible Simplifiers: Common Origins of Financial Crises and Persistent Poverty in Economic Theory and the New '1848 Moment'*, *in* POOR POVERTY: THE IMPOVERISHMENT OF ANALYSIS, MEASUREMENT, AND POLICIES 11, 16 (Jomo Sundaram & Anis Chowdhury eds., 2011).

[275] *See* FIN. CRISIS INQUIRY COMM'N, FINANCIAL CRISIS INQUIRY REPORT xviii–xix (2011), http://fcic-static.law.stanford.edu/cdn_media/fcic-reports/fcic_final_report_full.pdf [https://perma.cc/49BX-WEWN]; s*ee also* Michael Simkowic, *Competition and Crisis in Mortgage Securitization*, 88 IND. L.J. 213, 214, 225–32 (2013); Daniel Immergluck, *Private Risk, Public Risk: Public Policy, Market Development, and the Mortgage Crisis*, 36 FORDHAM URB. L.J. 447, 465–85 (2009).

the International Monetary Fund (IMF), one of the most devout of free-market dogmatists, into agnosticism.[276] One of the few silver linings of this near-total collapse of the American economy was that it caused even the most devout of free-market dogmatists to second-guess themselves. It even made an agnostic out of the International Monetary Fund (IMF), one of the most venerable bastions of neoliberal policy; in 2016, the IMF made the extraordinary admission that, for decades, its ideology's "two main planks" had hindered rather than furthered economic growth,[277] and in 2019, its former chief economist made the shocking assertion that "public debt may have no fiscal cost."[278] But perhaps the most pronounced shift in corporate philosophy came in August 2019, when the CEOs of almost 200 of the U.S.' largest corporations issued a statement repudiating their long-held adherence to shareholder value maximization and redefining the purpose of a corporation as advancing the interests of all stakeholders: employees, consumers, suppliers, communities, the environment, and shareholders.[279]

---

[276] *See* Ben Norton, *Wrong All Along: Neoliberal IMF Admits Neoliberalism Fuels Inequality and Hurts Growth*, SALON (May 31, 2016, 3:59 PM), https://www.salon.com/2016/05/31/wrong_all_along_neoliberal_imf_admits_neoliberalism_fuels_inequality_and_hurts_growth/ [https://perma.cc/KR3E-UAKB].

[277] *See* Jonathan D. Ostry et al., *Neoliberalism: Oversold?*, FIN. & DEV., June 2016 at, 38, 40–41 (2016).

[278] Olivier Blanchard, Peterson Inst. for Int'l Econ. and MIT, Presidential Address at the 2019 Meeting of the American Econ. Association: Public Debt and Low Interest Rates (Jan. 4, 2019). Commentators characterized the IMF's first about-face as "like the Pope declaring that there is no God" and the second as if the Pope had flat-out "endors[ed] the devil." Norton, *supra* note 276; Neil Irwin, *How America Learned to Stop Worrying and Love Deficits and Debt*, N.Y. TIMES (Feb. 23, 2019), https://www.salon.com/2016/05/31/wrong_all_along_neoliberal_imf_admits_neoliberalism_fuels_inequality_and_hurts_growth/ [https://perma.cc/XL8G-TPR9].

[279] *See Business Roundtable Redefines the Purpose of a Corporation to Promote 'An Economy That Serves All Americans,'* BUSINESS ROUNDTABLE, (Aug. 19, 2019), https://www.businessroundtable.org/business-roundtable-redefines-the-purpose-of-a-

[64] While the quasi-supply-side policies of the current administration fail to deliver their promised results,[280] prominent Democratic Party figures such as Rep. Alexandria Ocasio-Cortez (D–NY), Sen. Elizabeth Warren (D–MA), and Sen. Bernie Sanders (I–VT) have cited contemporary adaptations of Keynes such as Modern Monetary Theory[281]

corporation-to-promote-an-economy-that-serves-all-americans [https://perma.cc/SJ38-2V3V] (announcing a new statement on the purpose of a corporation).

[280] According to its supporters, the $2.3 trillion in tax breaks granted to the rich by the GOP's Tax Cuts and Jobs Act (TCJA) of 2017 would—ostensibly—increase capital expenditures and lead to higher wages for the middle- and lower-class, generating enough extra taxable income to "pay for itself." *See* ECONOMIST, *Some Fights About the Tax Cuts and Jobs Act Seem Over* (Feb. 9, 2019), https://www.economist.com/finance-and-economics/2019/02/09/some-fights-about-the-tax-cuts-and-jobs-act-seem-over [https://perma.cc/VD55-SPU4]. In reality, the TCJA's passage benefited only shareholders and executives: stock buybacks and dividends sharply increased in 2018 while business investments and wages remained in line with historical norms. *See* Thomas Heath, *A Year After Their Tax Cuts, How Have Corporations Spent the Windfall?*, WASH. POST (Dec. 14, 2018), https://beta.washingtonpost.com/business/economy/a-year-after-their-tax-cuts-how-have-corporations-spent-the-windfall/2018/12/14/e966d98e-fd73-11e8-ad40-cdfd0e0dd65a_story.html?noredirect=on. [https://perma.cc/9A67-9VZ9]. In its analysis of the TCJA's effects, the Urban-Brookings Tax Policy Center concluded that "TCJA will, under the most plausible scenarios, end up making most households worse off than if it had not been enacted." William G. Gale et al., *Effects of the Tax Cuts and Jobs Act: A Preliminary Analysis*, URBAN-BROOKINGS TAX POLICY CTR. 1 (June 13, 2018); *see also* Jane G. Gravelle & Donald J. Marples, *The Economic Effects of the 2017 Tax Revision: Preliminary Observations*, CONG. RESEARCH SERV. 1, (May 22, 2019), https://www.everycrsreport.com/files/20190522_R45736_8a1214e903ee2b719e00731791d60f26d75d35f4.pdf [https://perma.cc/D8R7-E23K].

[281] Modern Monetary Theory (MMT)—an upstart, controversial school of thought which has seized the imagination of many on Wall Street—argues that the U.S. can always print more money to pay its interest and thus need not worry about the deficit so long as inflation is kept in check. *See* Patricia Cohen, *Modern Monetary Theory Finds an Embrace in an Unexpected Place: Wall Street*, N.Y. TIMES (Apr. 5, 2019), https://www.nytimes.com/2019/04/05/business/economy/mmt-wall-street.html [https://perma.cc/GJ55-ADST]. *See generally* WILLIAM MITCHELL ET AL., MACROECONOMICS (1st ed. 2019) (textbook "based on the principles of Modern Monetary Theory"); Stephanie Kelton, *The Clock Runs Down on Mainstream*

and the French school of inequality economics[282] to lend credence to their ambitious policy proposals.[283] So, as the pendulum begins to swing the

Keynesianism, BLOOMBERG OPINION (Mar. 4, 2019, 3:55 PM), https://www.bloomberg.com/opinion/articles/2019-03-04/krugman-s-macroeconomics-is-no-match-for-mmt [https://perma.cc/AMZ2-776L] (recounting an exchange over MMT theory). Ray Dalio, the founder of one of the world's largest hedge funds, has said the adoption of MMT is "inevitable." Ray Dalio, *It's Time to Look More Carefully at 'Monetary Policy 3 (MP3)' and 'Modern Monetary Theory (MMT)'*, LINKEDIN (May 1, 2019), https://www.linkedin.com/pulse/its-time-look-more-carefully-monetary-policy-3-mp3-modern-ray-dalio/ [https://perma.cc/F44B-4QBL].

[282] The French school of inequality economics argues that a return to the Great Society's high marginal tax rates and a significant increase on capital income tax would maximize both revenue and welfare while reducing income inequality. *See generally* Peter Diamond & Emmanuel Saez, *The Case for a Progressive Tax: From Basic Research to Policy Recommendations*, 25 J. ECON. PERSP. 165 (2011); Emmanuel Saez et al., *The Elasticity of Taxable Income with Respect to Marginal Tax Rates: A Critical Review*, 50 J. ECON. LIT. 3 (2012); Thomas Piketty & Emmanuel Saez, *A Theory of Optimal Inheritance Taxation*, 81 ECONOMETRICA 1851 (2013). *See generally* THOMAS PIKETTY, CAPITAL IN THE TWENTY-FIRST CENTURY (Arthur Goldhammer trans., 2014) (describing the history of French economic inequalities); Thomas Piketty et al., *Optimal Taxation of Top Labor Incomes: A Tale of Three Elasticities* 6 AM. ECON. J.: ECON. POL'Y 230 (2014) (outlining optimal tax rate formulas).

[283] *See, e.g.*, Elizabeth Warren, *I'm Calling for Something Truly Transformational: Universal Free Public College and Cancellation of Student Loan Debt*, Medium (Apr. 22, 2019) (announcing her new policy), https://medium.com/@teamwarren/im-calling-for-something-truly-transformational-universal-free-public-college-and-cancellation-of-a246cd0f910f [https://perma.cc/X9HW-P6GH]; Sahil Kapur & Laura Davison, *Warren Pushes New Corporate Tax on Profits Above $100 Million*, BLOOMBERG (Apr. 11, 2019, 9:00 AM), https://www.bloomberg.com/news/articles/2019-04-11/warren-pushes-new-corporate-tax-on-profits-above-100-million [https://perma.cc/4QFE-FMJA]; Victoria Guida, *Ocasio-Cortez Boots Progressive Theory That Deficits Aren't So Scary*, POLITICO (Feb. 6, 2019 3:10 PM), https://www.politico.com/story/2019/02/06/alexandria-ocasio-cortez-budget-1143084 [https://perma.cc/V794-ZGR7]; Bernie Sanders, *For the 99.8% Act*, SANDERS.GOV (Jan. 28, 2019), https://www.sanders.senate.gov/download/estate-tax-one-pager?id=DE8AEADA-A3F5-4D26-8517-F6730F161E29&download=1&inline=file

other way, an innovative car-hacking case in the Southern District of Illinois appears poised to be a watershed moment not only in the campaign for IoT reform[284] but also for the significance of the class action in the years to come.

VII. BACK TO ITS ROOTS: EXERCISING THE CLASS ACTION DEVICE TO BYPASS THE BUREAUCRACY OF THE INTERNET OF THINGS

[65] The significant public interest in IoT safety reform and the collective inaction by corporations, Congress, and administrative agencies in promulgating effective safety standards weighs in favor of the immediate deployment of consumer class actions, patterned on *Flynn v. FCA*, against all unsafe and unsecured IoT devices.

A. The Silver Bullet: *Flynn v. FCA*

[66] In a July 2015 article for the technology journal *Wired*, journalist Andy Greenberg illustrated the dangers of an unsecured IoT with this harrowing firsthand account:

> As the two hackers remotely toyed with the air-conditioning, radio, and windshield wipers, I mentally congratulated myself on my courage under pressure. That's when they cut the transmission. Immediately my accelerator stopped working. As I frantically pressed the pedal and watched the RPMs climb, the Jeep lost half its speed, then slowed to a crawl. This occurred just as I reached a long overpass, with no shoulder to offer an

[https://perma.cc/GHH5-VYDX]; Jeff Stein & Christopher Ingraham, *Elizabeth Warren to Propose New 'Wealth Tax' on Very Rich Americans, Economist Says*, WASH. POST (Jan. 24, 2019, 1:40 PM), https://www.washingtonpost.com/business/2019/01/24/elizabeth-warren-propose-new-wealth-tax-very-rich-americans-economist-says/ [https://perma.cc/9UH3-UKXT].

[284] *See* Yannella, *supra* note 39.

> escape . . . . [A] semi loomed in the mirror, bearing down on my immobilized Jeep . . . . I didn't panic. I did, however, drop any semblance of bravery, grab my iPhone with a clammy fist, and beg the hackers to make it stop.[285]

[67] Greenberg's article revealed a fatal vulnerability in the Uconnect infotainment systems of 2013–2015 model year Chrysler, Jeep, Dodge, and Ram vehicles.[286] Charlie Miller[287] and Chris Valasek,[288] the security researchers credited with the exploit, showed Greenberg that because each Uconnect system was perpetually connected to the Internet through Sprint's wireless network, any Sprint device—even a cheap cell phone—could be configured to "talk" to any Uconnect system at any range.[289] This method enabled Miller and Valasek to extract the VINs, makes, models, IP addresses, and current GPS locations of unsuspecting drivers dotted across the country with chilling ease.[290]

---

[285] Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, WIRED (July 21, 2015, 6:00 AM), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [https://perma.cc/BJ54-VGPD].

[286] *See id.*

[287] Miller, a security researcher at Twitter when he discovered the wireless car-hacking exploit, *see id.*, now works for autonomous vehicle company Cruise. *See* Chris Valasek & Charlie Miller, *How to Prioritize Self-Driving Car Security*, MEDIUM: CRUISE (Apr. 18, 2019), https://medium.com/cruise/how-to-prioritize-self-driving-car-security-4293c480c75d [https://perma.cc/N6FU-MKFM].

[288] Valasek, who was director of Vehicle Security Research at IOActive when the *Wired* article was published, *see* Greenberg, *supra* note 285, now works for autonomous vehicle company Cruise. *See* Valasek and Miller, *supra* note 287.

[289] *See* Greenberg, *supra* note 285.

[290] *See id.*

[68] To illustrate to Greenberg the lethal implications of this data harvest, Miller and Valasek bundled him into a Jeep Cherokee and pointed him in the direction of the nearest highway.[291] As Greenberg accelerated away, the two researchers commandeered several cell phones to comb through Sprint's wireless network, locate the car he was driving, collect its IP address, and gain access to its Uconnect system through that unique identifier.[292] With the Jeep's innards now displayed on the screen of their laptop, Miller and Valasek rewrote one of its chips with a few lines of malicious code, and the trap was set.[293]

[69] The failing of the Uconnect system exploited by Miller and Valasek was deceptively simple. It had been connected to a wiring component called a CAN bus, which was itself connected to the various computer networks responsible for controlling critical vehicle systems such as the steering, brakes, engine, and transmission.[294] By traveling from the IP address entry point in the Uconnect system through the CAN bus and into the critical vehicle systems, Miller and Valasek wrested control of the Jeep from Greenberg and took turns disabling its transmission, cutting its brakes, hijacking its steering, and killing its engine—all while sitting on a couch ten miles away.[295]

[70] Greenberg's exposé forced consumers to face a harsh truth: when it comes to the IoT, companies tend to connect first and ask cybersecurity questions later.[296] The story's publication drove FCA to issue a hasty

[291] *See id.*

[292] *See id.*

[293] *See id.*

[294] *See id.*

[295] *See* Greenberg, *supra* note 285.

[296] *See* SCHNEIER, *supra* note 14, at 106–07. *See also* Greenberg, *supra* note 285.

recall of 1.4 million affected vehicles and a statement assuring its customers a simple software patch would cure the problem.[297] But consumer advocates branded the recall as both superficial and performative because it overlooked the critical flaw of the CAN bus's physical connection to critical vehicle systems[298] and because FCA allegedly knew of the Uconnect vulnerability for months before the *Wired* report was published.[299] A putative class action seeking meaningful relief quickly followed: *Flynn v. FCA*.[300]

[71] *Flynn* alleged a laundry list of warranty, consumer fraud, negligence, and unjust enrichment claims under federal law as well as the laws of Illinois, Michigan, and Missouri.[301] After years of pretrial maneuvering by both sides, the district court eventually certified three classes: an Illinois class against FCA under the MMWA;[302] a Missouri class against FCA under Missouri's Merchandising Practices Act;[303] and a Michigan class against both FCA and Harman International (the manufacturer of the Uconnect systems) under the MMWA and Michigan's

[297] *See* Amended Class Action Complaint at *9, *20, Flynn v. FCA U.S. L.L.C., 2015 WL 11018515 (S.D. Ill. 2018) (No. 3:15–CV–855) (Not reported in Fed. Supp.).

[298] *See id.* at 9–10. *But see supra* Part V(A) (the connected-car bill proposed by Sens. Markey and Blumenthal would ban this practice).

[299] *See* Amended Class Action Complaint at *19, Flynn v. FCA U.S. L.L.C., 2015 WL 11018515 (S.D. Ill. 2018) (No. 3:15–CV–855) (Not reported in Fed. Supp.).

[300] *See id.* at 35–36.

[301] *See Id.* at 33–110.

[302] Flynn v. FCA U.S. LLC, 327 F.R.D. 206, 227 (S.D. Ill. 2018).

[303] *Id.*

Consumer Protection Act.[304] The defendants delayed the trial date for almost a year by appealing the class certifications to both the Seventh Circuit and the United States Supreme Court, but both petitions were denied[305] and so the parties will go to trial in October 2019 with over $440 million at stake.[306]

[72] Flynn and his fellow class representatives fought tooth and nail for certification, undaunted by the barriers to litigation erected over the last 30 years by Congress and the federal judiciary. The shadow of CAFA forced them to file in federal court, a slow-moving purgatory for civil litigants[307] because the federal bench has grown just 4 percent since 1990 although filings have increased by more than 38 percent in the same time.[308] They

[304] *Id*. at 221, 227.

[305] FCA U.S. LLC v. Flynn, 139 S.Ct. 797 (Jan. 7, 2019) (No. 18-398).

[306] FCA U.S. LLC v. Flynn, 139 S.Ct. 797 (2018), *petition for cert. filed*, 2018 WL 4731876 (U.S. Sept 26, 2018) (No. 18-398).

[307] Max Kennerly, *Why Civil Defendants Want to Be in Federal Court: Judicial Vacancies*, LITIG. AND TRIAL (Jan. 7, 2013), https://www.litigationandtrial.com/2013/01/articles/series/special-comment/judicial-vacancies/ [https://perma.cc/GY7U-4SW5]; *See also* Nicole Ochi, *Are Consumer Class and Mass Actions Dead? Complex Litigation Strategies After CAFA & MMTJA*, 41 LOY. L.A. L. REV. 965, 980-81 (2008).

[308] Cara Bayles, *As Judicial ranks Stagnate, 'Desperation' Hits the Bench*, LAW360 IN-DEPTH (Mar. 19, 2019), https://www.law360.com/in-depth/articles/1140100 [https://perma.cc/RPE2-Z923]. For Judge Lawrence O'Neill, who sits on the Eastern District of California, the workload created by judicial vacancies is escalating from "crisis" to "catastrophe." *Id.* But "[t]he same partisanship that's blocked judicial nominees has effectively halted new judgeships as well," according to Senator Mike Lee (R–UT), "[Congress isn't] interested in adding judgeships that a president of the other party can fill." *Id.*

lost a major battle when the warranty claims of the Missouri class representatives were doomed to arbitration[309] by the precedent set by *Concepcion* and its progeny.[310] But in the end, they won the war[311] by asserting an "overpayment" theory of damages which alleged FCA's recall failed to cure the underlying defects in the affected vehicles and so caused them to decrease in value.[312] By supplementing this claim with market research data obtained through conjoint analysis (a demand-side modeling technique which calculates class-wide expectation damages by quantifying the relative values of product features according to consumer expectations),[313] the class representatives not only survived *Comcast* scrutiny[314] but also overcame the heightened definition of Article III

[309] Flynn v. FCA U.S. LLC (No. 15-CV-0855), 2016 WL 5341199, at *3–*4, *6 (S.D. Ill. Sept. 23, 2016).

[310] *See* AT&T Mobility L.L.C. v. Concepcion, 563 U.S. 333, 348–52 (2011); Am. Express Co. v. Italian Colors Rest., 570 U.S. 228, 232–35 (2013); DIRECTV, Inc. v. Imburgia, 136 S. Ct. 463, 466 (2015); Lamps Plus, Inc. v. Varela, 139 S. Ct. 1407, 1419 (2019).

[311] Because a certified class is a powerful bargaining chip in settlement negotiations the outcome of a motion to certify is often more decisive than the trial itself. *See* LEE III & WILLGING, supra note 34; see, e.g., Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co., 559 U.S. 393, 445 (2010) (Ginsburg, J., dissenting).

[312] Flynn v. FCA U.S. LLC (No. 15-CV-0855), 2016 WL 5341749, at *3 (S.D. Ill. Sept. 23, 2016).

[313] Comparing a reasonable consumer's willingness to pay for a product absent a given feature with that product's actual sale price (while considering relevant supply-side factors) satisfies the stringent requirements of *Comcast*. *See e.g.*, *In re* Lenovo Adware Litig. (No. 15-md-02624), 2016 WL 6277245, at *21 (N.D. Cal. Oct. 27, 2016); *See also* Sanchez-Knutson v. Ford Motor Co., 181 F.Supp.3d 988, 995–96 (S.D. Fla. 2016); Khoday v. Symantec Corp., 93 F.Supp.3d 1067, 1082–83 (D. Minn. 2015).

[314] *See* Flynn v. FCA U.S. L.L.C., 327 F.R.D. 206, 225 (S.D. Ill. 2018). Plaintiffs' attorneys seeking certification of generic false advertising and product defect claims have

standing established by *Clapper* and *Spokeo*,[315] potentially opening the floodgates for preemptive class actions against all unsafe and unsecured IoT devices.

B. Application of *Flynn's* Theories of Liability Against the Automotive Industry at Large

[73] NHTSA, like many other agencies, has adopted cybersecurity guidelines based on best practices promulgated by a preeminent technical organization, the Department of Commerce's National Institute of Standards and Technology (NIST).[316] Still, industry compliance with this framework is voluntary[317] and de facto nonexistent.[318] To remedy this, MMWA and fraudulent concealment claims should immediately be brought against all automakers which, like FCA, know their vehicles are fatally insecure but offer them for sale regardless. Both species of claims will hinge on *Flynn's* application of conjoint analysis to real-world market

been referencing demand-side models to satisfy *Comcast* for some time, *see infra* note 321, but *Flynn* is the first class action to successfully apply this tactic to cybersecurity litigation.

[315] *See Flynn*, 2016 WL 5341749, at *2–3.

[316] *See Vehicle Cybersecurity*, NAT'L HIGHWAY HIGHWAY TRAFFIC SAFETY ADMIN., https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity [https://perma.cc/PC5C-2GUC].

[317] *See Cybersecurity Framework*, NAT'L INST STANDARDS & TECH., https://www.nist.gov/cyberframework [https://perma.cc/PX6M-6LWF].

[318] *See* SCHNEIER, *supra* note 14, at 109. This is an example of rent-seeking in action. *See also* FED. TRADE COMM'N, *supra* note 15, at 48–49; Thierer & Skorup, *supra* note 221, at 133–136, 142; SCHNEIER, *supra* note 14, at 153–55.

conditions to prove overpayment damages, establishing Article III standing while complying with *Comcast*.[319]

1. Breach of Implied Warranty of Merchantability Claims Filed Under Federal Law

[74] A plaintiff who brings a MMWA claim for a breach of implied warranty of merchantability is essentially alleging a product was designed or manufactured with flaws so fundamental it should have never been sold.[320] For example, the MMWA class in *Flynn* secured certification by arguing the vulnerabilities in the Uconnect systems rendered their cars so unsafe that they were not fit for their ordinary purpose as passenger vehicles.[321] FCA is not the only company failing to construct vehicles which cannot easily be hacked. In fact, a 2015 investigation by Senator Markey revealed that there may be latent cybersecurity flaws comparable

[319] *See, e.g.*, *Hilsley v. Ocean Spray Cranberries, Inc.*, No. 17-CV-2335-GPC(MDD), 2018 WL 6300479, at *1, *10, *13, *16, *18 (S.D. Cal. Nov. 29, 2018) (certifying a food labeling class alleging Ocean Spray violated California consumer fraud statutes by misrepresenting its juices as containing no artificial flavors after the plaintiffs' experts established consumers were willing to pay a premium of 61 cents for juices without artificial flavoring and extrapolated that figure to Ocean Spray's actual unit sales during the class period, satisfying *Comcast's* requirement of a damages model "sufficiently traceable" to the plaintiffs' liability case); Glazer v. Whirlpool Corp. (*In re* Whirlpool Corp. Front-Loading Washer Prods. Liability Litig.), 722 F.3d 838, 856 (6th Cir. 2013) (finding that Whirlpool's breach of warranty in selling washing machines which tended to develop mold was sufficient to find all members of a liability-only class had suffered an injury-in-fact at the moment they bought the overvalued machines).

[320] *See* U.C.C. § 2-314(2)(c) (AM. LAW INST. & UNIF. LAW COMM'N 1977) (defining "merchantable" as "fit for the ordinary purposes for which the goods are used").

[321] *See* Amended Class Action Complaint at *33–*34, Flynn v. FCA U.S. L.L.C., 2015 WL 11018515 (S.D. Ill. 2018) (No. 3:15–CV–855) (Not reported in Fed. Supp.).

to FCA's Uconnect vulnerability in most modern cars.[322] For example, both the 2014 Infiniti Q50 and 2015 Cadillac Escalade have large attack surfaces[323] directly connected to their critical systems[324] just like the affected vehicles in *Flynn*. Thus, MMWA class actions should be brought against Nissan,[325] GM,[326] and all similarly situated auto manufacturers without delay—especially because if those cars are defective, they are likely defective by design.

[75] As elaborate IoT devices, modern cars are subject to the economic factors responsible for unsafe IoT devices introduced in Part II(B)(2): the

[322] *See* ED MARKEY, TRACKING AND HACKING: SECURITY AND PRIVACY GAPS PUT AMERICAN DRIVERS AT RISK 1–2 (2015) (determining that "nearly 100 percent" of vehicles on the market were being sold with potentially unsafe wireless connections, that the automotive industry had employed "inconsistent and haphazard" protections for these vulnerable wireless connections, and that the "clear lack" of extant cybersecurity safeguards demanded NHTSA and the FTC promulgate meaningful standards to protect driver safety after compiling responses from BMW, Chrysler, Ford, General Motors, Honda, Hyundai, Jaguar Land Rover, Mazda, Mercedes-Benz, Mitsubishi, Nissan, Porsche, Subaru, Toyota, Volkswagen (with Audi), and Volvo); *see id.* at 10 (concluding with the remarkable assertion that "most" of the automotive industry was guilty of substandard cybersecurity practices).

[323] *See* Lily Hay Newman, *Hacker Lexicon: What is an Attack Surface?*, WIRED (Mar. 12, 2017, 8:00 AM), https://www.wired.com/2017/03/hacker-lexicon-attack-surface/ [https://perma.cc/8RLY-3KJ9] (defining attack surface).

[324] *See* CHRIS VALASEK & CHARLIE MILLER, A SURVEY OF REMOTE AUTOMOTIVE ATTACK SURFACES 30–32, 48–50, 86 (2014).

[325] The parent company of Infiniti. *See Infiniti Brand History*, INFINITI NEWS, https://infinitinews.com/en-US/infiniti/usa/channels/us-united-states-nissan-heritage-infiniti-heritage/releases/a956b628-24a9-46ce-9b7c-67fa7d9e4947?la=1 [https://perma.cc/9U3X-EXVJ].

[326] The parent company of Cadillac. *See Our Brands*, GM, https://www.gm.com/our-brands [https://perma.cc/W2TZ-AGPP].

race among auto manufacturers for first-mover advantage and the corporate executive's dogged pursuit of short-term profits.[327] Evidence obtained during *Flynn*'s discovery process revealed Miller and Velasek's Jeep hack was only possible because FCA and Harman broke several fundamental cybersecurity rules.[328] They failed to periodically scan the system for open ports such as the one Miller and Velasek used to gain entry.[329] They took no precautions to prevent unauthorized messages from being sent through the CAN bus.[330] Even after the vulnerabilities were discovered, they failed to implement a firewall to prevent future harmful intrusions.[331] There is no question FCA and Harman could have taken any number of steps to cure their products of these unacceptable flaws but instead rushed to market out of a fear of obsolescence and a misplaced assurance that their consumers either wouldn't notice or wouldn't care.

[76] Congress passed the MMWA in response to consumer product safety concerns and the impotence of the administrative state.[332] Its private right of class action and fee-shifting provisions imbued it with quasi–regulatory power, conscripting the plaintiffs' bar to enforce consumer warranty infringements on behalf of underfunded state attorneys general.[333] Senator Markey's report shows that FCA's bare-minimum

[327] *See* COPELAND & SHAPIRO, *supra* note 95, at 3,4.

[328] *See* Amended Class Action Complaint at *6, Flynn v. FCA U.S. L.L.C., 2015 WL 11018515 (S.D. Ill. 2018) (No. 3:15–CV–855) (Not reported in Fed. Supp.).

[329] *See id.* at *10.

[330] *Id.*

[331] *Id.*

[332] *See* H.R. REP. 93–1107, at 24–25 (1974); *supra* Part VI(A).

[333] 15 U.S.C. § 2310(d)(1)–(2), (e) (2012); *see* FARHANG supra note 236, at 33–34, 37; *see also* Michael S. Greve, *The Private Enforcement of Environmental Law*, 65 TUL. L. REV. 339, 339–40 (1990) ("Congress has increasingly come to rely upon private law enforcement as a means of attaining public objectives . . . . Groups and individuals suing

cybersecurity philosophy is likely the rule, not the exception.[334] NHTSA's voluntary cybersecurity standards are a byproduct of the rent-seeking that the MMWA was designed to circumvent. Because few situations are more deserving of MMWA treatment than an entire industry riddled with fatal yet curable cybersecurity defects,[335] plaintiffs' attorneys should immediately file class actions *á la Flynn* in states with consumer-friendly interpretations of the MMWA against all manufacturers of vehicles which suffer from material cybersecurity vulnerabilities.

2. Fraudulent Concealment Claims Filed Under State Law

[77] While MMWA claims ask whether a defendant's product was unreasonably defective, fraudulent concealment claims ask whether a defendant knowingly concealed its product's defectiveness from consumers. The fraudulent concealment claims certified in *Flynn* turn on the allegation that FCA knew of the Uconnect vulnerabilities in its affected vehicles for years but failed to disclose them.[336] Because Senator

---

under [citizen suit] provisions have sustained . . . at most, a minimal injury-in-fact. They act not as victims who redress a wrong done to them but as 'private attorneys general.'").

[334] *See* MARKEY, *supra* note 322, at 1–2.

[335] *Cf.* The TJ Hooper, 60 F.2d 737, 740 (2d Cir. 1932) ("Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission.").

[336] *See* Flynn v. FCA U.S. LLC, 327 F.R.D. 206, 214 (S.D. Ill. 2018). FCA, like other major corporations, has a strong incentive to treat security vulnerabilities as public relations issues and keep them concealed for as long as possible, even in the face of civil and criminal liability. *See* SCHNEIER, *supra* note 14, at 124. For instance, Yahoo kept its 2013 hack a secret until December 2016, when a law enforcement investigation threatened public disclosure. *See id*. at 124–125 (citing Jamie Condliffe, *A History of Yahoo Hacks*, MIT TECH. REV., Dec. 15, 2016, https://www.technologyreview.com/s/603157/a-history-of-yahoo-hacks/ [https://perma.cc/P6CD-FWRD]). Uber also lost the private information of 57 million people in October 2016 and not only failed to tell the

Markey's 2015 report intimated that many automakers have offered their products for sale even though they knew or should have known their existing cybersecurity practices created only an illusion of safety,[337] FCA is likely not the only major auto manufacturer vulnerable to liability for fraudulent concealment. Thus, *Flynn's* certification of two fraudulent concealment classes opens the door for plaintiffs' attorneys to file similar

FTC but *paid the hackers a $100,000 ransom* to delete the data and keep the breach a secret for more than a year. *See id*. at 125 (citing Andy Greenberg, *Hack Brief: Uber Paid Off Hackers to Hide a 57-Million User Data Breach*, WIRED (Nov. 21, 2017, 7:56 PM), https://www.wired.com/story/uber-paid-off-hackers-to-hide-a-57-million-user-data-breach/ [https://perma.cc/38H8-TPFU]).

[337] The Senator asked each manufacturer to describe the precautions they had taken to prevent remote access to their vehicle electronics. *See* MARKEY, *supra* note 322, at 4. According to automobile security experts consulted by the Senator's staff, over half of the security measures cited by respondents would provide little defense against a determined hacker. *See id*. at 6. The Senator also specifically asked whether the manufacturers were monitoring their vehicle's CAN buses for unauthorized activity. *See id*. at 6–7. Two of the eight companies admitted they did not currently have CAN bus monitoring features, and five out of the six companies which claimed to have CAN bus monitoring features in fact described processes which could easily be bypassed or did not actually examine the content of the data being transmitted. *See id*. at 7. In total, only two automakers out of sixteen "described credible real-time reactions to an intrusion event." *See id.* at 6. The July 2015 *Wired* article confirmed modern vehicles could in fact be hacked through the CAN bus under real-world conditions, exactly as Senator Markey had predicted. *See* Greenberg, *supra* note 284; MARKEY, *supra* note 322, at 3. Following its publication, Senators Markey and Blumenthal immediately wrote to the administrator of NHTSA, shocked FCA had waited to recall its vehicles "despite being aware of this vulnerability for almost nine months" and concerned the article's revelations were only "the tip of the iceberg." *See* Amended Class Action Complaint, Flynn v. FCA U.S. LLC, 2015 WL 11018515 at *9 (S.D. Ill. 2015) (No. 3:15-cv-0855) (Not reported in Fed. Supp.).

class actions[338] in states with consumer-friendly Unfair and Deceptive Acts and Practices statutes (UDAPs)[339] against all auto manufacturers which have concealed material cybersecurity vulnerabilities in their vehicles. In particular, attorneys should seek certification in the federal courts of those jurisdictions with UDAPs that include fraudulent concealment clauses, do not require a showing of reliance, and grant victorious plaintiffs' recovery of punitive damages and attorney fees.[340]

[338] Statutory fraudulent concealment claims, which do not require a showing of reliance, are far more suitable for class-wide treatment than affirmative misrepresentation claims, which are particularly susceptible to Rule 23(b)(3) predominance issues. *See, e.g.*, Wells v. Allstate Ins. Co., 210 F.R.D. 1, 9 (D.D.C. 2002) ("[Defendant] assumes that Wells' misrepresentation claim is premised on false or misleading advertising—in other words, an affirmative misrepresentation . . . . Only plaintiff's alternate theory, misrepresentation based on a material omission . . . , remains as a potential class issue. Allstate essentially ignores this theory of liability, *which is much more amenable to class resolution*.") (emphasis added).

[339] These states have the *least* favorable UDAPs for IoT class action purposes and should generally be avoided: Alabama, Alaska, Arizona, Colorado, Delaware, Florida, Georgia, Indiana, Iowa, Louisiana, Minnesota, Mississippi, Montana, Nevada, New York, North Dakota, Ohio, Oregon, South Carolina, South Dakota, Tennessee, Texas, Virginia, Washington, and Wyoming. The UDAPs of these states make them poor forum choices for one or more of these reasons: either they do not broadly prohibit deceptive acts; they do not provide for private rights of action; they incorporate complicated public interest tests; they undermine themselves with outdated damage caps; they have no fee-shifting provision (or worse, a defendant-friendly fee-shifting provision); or they simply ban enforcement by class action altogether. *See* CAROLYN L. CARTER, NAT'L CONSUMER L. CTR., CONSUMER PROTECTION IN THE STATES: A 50-STATE REPORT ON UNFAIR AND DECEPTIVE ACTS AND PRACTICES STATUTES 13, 21–22 (2009).

[340] A non-exhaustive list of these especially favorable forums: California, Connecticut, D.C., Kansas, Massachusetts, Missouri, New Jersey, Vermont, and West Virginia. *See generally* NAT'L CONSUMER L. CTR., CONSUMER PROTECTIONS IN THE STATES: STATE-BY-STATE SUMMARIES OF STATE UDAP STATUTES, app. B (2009) (detailing the strength of UDAP statutes in each state).

C. *Flynn's* Theories of Liability Translate to Every Segment of the Internet of Things

[78] *Flynn*'s successful certifications reverberate beyond the automotive industry. They prove that the plaintiffs' bar need not wait for reform of products liability law to hold IoT manufacturers accountable.[341] Instead, attorneys should immediately sue all unreasonably unsafe and unsecure IoT devices, such as Google's Works With Nest platform,[342] the Philips Hue lighting system,[343] Samsung's SmartThings automation system,[344] and Owlet's baby monitoring Smart Sock.[345] Security researchers have discovered serious and fundamental design flaws within each of these popular products which could cause injury or death if exploited with ill intent: unforeseen interactions among smart devices within the Works With Nest and Hue networks make burglaries trivial.[346]

---

[341] *See* SCHNEIER, *supra* note 14, at 128–32; *cf.* Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers be Liable for Damage Caused by Hacked Devices?*, 50 U. MICH. J.L. REFORM 913, 924–930 (2017) (describing applications of current products liability law to IoT manufacturers).

[342] *See What's Happening at Nest?*, NEST, https://nest.com/whats-happening/#faq-consumers [https://perma.cc/AX44-JUHC].

[343] *See Philips Hue*, PHILIPS, https://www.meethue.com/en-us [https://perma.cc/YHB6-9NSM].

[344] *See* Samsung, SMARTTHINGS, https://www.smartthings.com/ [https://perma.cc/E3LH-M5H9].

[345] *See Smart Sock 2*, OWLET, https://owletcare.com/products/owlet-smart-sock [https://perma.cc/XTZ8-BHXK].

[346] Kaushall Kafle, et al., *A Study of Data Store-based Home Automation*, *in* CODASPY '19 PROCEEDINGS OF THE NINTH ACM CONFERENCE ON DATA & APPLICATION SECURITY & PRIVACY 73, 73-74 (2019) (A 2018 study by William & Mary computer scientists exposed flaws in home automation platforms Google Nest and Philips Hue caused by unexpected interactions between low-security smart devices (such as sprinklers and light

Cybersecurity oversights within the SmartThings system allow hackers to unlock smart locks with a simple phishing email.[347] Those alerts that the Smart Sock sends when its wearer's vital signs deviate from safe levels can be remotely diverted with ease;[348] thus, parents relying on the device

switches) and high-security ones (such as cameras and smart locks)). The scientists showed that a hacker connected to the same public network as a homeowner (for example, a Starbucks WiFi) could access her smart home's central automation platform through one of its low-security devices and temporarily disable the entire system by manipulating data the platform shared between its low- and high-security devices. *See id*. at 81-82. *See also* Adrienne Berard, *Smart Home Security Devices may be Vulnerable to Smart Hackers*, WILLIAM & MARY (Dec. 6, 2018), https://www.wm.edu/news/stories/2018/smart-home-security-devices-may-be-vulnerable-to-smart-hackers.php [https://perma.cc/ED8C-6J8Q] (These vulnerabilities were judged to be so intrinsic to the design of these systems that no patch could eliminate them).

[347] *See* Earlence Fernandes, et al., *Security Analysis of Emerging Smart Home Applications*, *in* 2016 IEEE SYMPOSIUM ON SECURITY & PRIVACY 636, 645-647 (2016). A recent paper by University of Michigan and Microsoft researchers described four proof-of-concept attacks against Samsung's SmartThings home automation platform, the worst of which would plant a backdoor in the smart locks of owners who clicked on fake links in phishing emails. *See id.* at 645-646. Clicking on one of these links would send the unsuspecting victim to the actual SmartThings website—to avoid raising suspicion—but would also send the victim's login information to the hacker, who could then access the victim's smart lock account and add a new four-digit PIN without the victim's knowledge. *See* Andy Greenberg, *Flaws in Samsung's 'Smart' Home let Hackers Unlock Doors & Set off Fire Alarms*, WIRED (May 2, 2016, 7:00 AM), https://www.wired.com/2016/05/flaws-samsungs-smart-home-let-hackers-unlock-doors-set-off-fire-alarms/ [https://perma.cc/32ZB-LK6L] (When reached for comment, a SmartThings spokesperson blamed the defects on third-party developers).

[348] *See* Iain Thomson, *Wi-Fi Baby Heart Monitor May Have the Worst IoT Security of 2016*, THE REGISTER (Oct. 13, 2016, 11:26 PM), https://www.theregister.co.uk/2016/10/13/possibly_worst_iot_security_failure_yet [https://perma.cc/GR48-TF2C]. A security researcher's 2016 report disclosed a critical vulnerability in the Owlet smart sock he had bought to monitor his newborn's heart rate, oxygen levels, and sleep patterns. The sock sent the data it collected over a WiFi network to a central hub, which would alert his smartphone if his baby's vital signs deviated from their normal levels. But the researcher determined the WiFi network created by the base station was so unsecure that a hacker could remotely take control of it and block alerts from being sent to him with just a few commands. *See id*.

could be led to believe that all is well when in fact their infant's life is in peril. Evidence suggests these flaws were caused by shortsighted design decisions arising out of the pressure on these companies to secure first-mover advantage.[349] These facts establish that Google, Philips, Samsung, and Owlet knew, or should have known, that their products were unfit for sale but failed to cure or disclose those products' defects. Each company is therefore a prime candidate for class claims of MMWA and fraudulent concealment based on overpayment damage models backed by conjoint analysis.[350]

[79] There are likely many more dangerously defective IoT devices in existence susceptible to the theories of liability presented in this article. When filing class actions against those devices' manufacturers, plaintiffs' attorneys are limited only by their creativity and by the soundness of the scientific literature supporting their claims.

VIII. CONCLUSION

[80] IoT manufacturers will not independently improve the cybersecurity of their devices because they are insulated from the consequences of poor cybersecurity.[351] The IoT is a lemons market, meaning that IoT manufacturers can advertise their devices as secure and

[349] *See* Berard, *supra* note 346 ("For software developers, this centralized data store solution is very easy to implement, so that could be one of the reasons why it was part of the original design. It's a very straightforward, simple implementation, but we can see that it's ineffective from a security point of view.") (statement of computer scientist Denys Poshyvanyk).

[350] The feasibility of these potential class actions is not evaluated with respect to statutes of limitation, arbitration clauses, or other fact-specific concerns.

[351] *See* Bruce Schneier, *Security and the Internet of Things*, SCHNEIER ON SECURITY (Feb. 1, 2017, 8:05 AM), https://www.schneier.com/blog/archives/2017/02/security_and_th.html [https://perma.cc/E4WF-9Z2N].

consumers are none the wiser.[352] Government stakeholders must correct this market failure through technology-neutral, flexible policies[353] supplemented by practicable enforcement mechanisms. But the developmental arc of privacy governance signifies that policymakers will take no action to reform the IoT until public scrutiny on corporate malfeasance reaches a fever pitch. Because this scrutiny will either follow or preempt catastrophic IoT hacks, the public interest weighs in favor of the immediate deployment of prophylactic MMWA and fraudulent concealment class actions against all IoT manufacturers which have discounted the value of human life against their bottom lines. This litigation campaign must proceed until the industry joins with consumers in lobbying for IoT reform, and it must proceed at once, before inventive cybercriminals exploit the IoT's glaring defects at the expense of human lives.

[352] *See* discussion, *supra* para. [24].

[353] *See* SCHNEIER, *supra* note 14, at 153; *see also* STAFF OF THE FED. TRADE COMM'N'S BUREAU OF CONSUMER PROT., COMMENTS ON THE INTERNET OF THINGS AND CONSUMER PRODUCT HAZARDS, at 10 (June 15, 2018), https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-federal-trade-commissions-bureau-consumer-protection-consumer-product-safety/p185404_ftc_staff_comment_to_the_consumer_product_safety_commission.pdf [https://perma.cc/9RSS-KKME].