Introduction

We now live in a world where we can obtain current information about a global pandemic from our smartphones and Internet of Things (IoT) devices.[1] The recent novel coronavirus (COVID-19) outbreak is not just a public health emergency. The pandemic has forced us to further evaluate the extent to which privacy should give way to public health threats and resulting technological innovations.[2] It directly raises questions about whether legal frameworks governing our privacy should be relaxed to address public health concerns, and if any such relaxation will continue post pandemic to permanently undermine our privacy.[3]

The outbreak also highlights privacy concerns about corporate and government actors' use of data collected from smartphones, mobile applications (mobile app(s)), facial recognition and geo-location technologies, and IoT devices, such as

[1] *See, e.g.*, Rebecca Heilweil, *Here's What Alexa and Other Smart Speakers Say About the Coronavirus*, Vox (Mar. 13, 2020, 3:40 pm), www.vox.com/recode/2020/3/13/21178361/alexa-google-assistant-coronavirus; Neil Selwyn & Mark Andrejevic, *The New Transparency: Smartphones, Data Tracking, and COVID-19*, Lens, Monash U. (Mar. 9, 2020), https://lens.monash.edu/@education/2020/03/09/1379796/the-new-transparency-smartphones-data-tracking-and-covid-19?amp=1&__twitter_impression=true; *see also* Dep't of Health & Human Servs., Ctr. for Disease Control, What You Should Know About COVID-19 to Protect Yourself and Others (2020), www.cdc.gov/coronavirus/2019-ncov/downloads/2019-ncov-factsheet.pdf ("The virus that causes COVID-19 is a new coronavirus").

[2] *See* Vincent Manancourt, *Coronavirus Tests Europe's Resolve on Privacy*, Politico, www.politico.eu/article/coronavirus-tests-europe-resolve-on-privacy-tracking-apps-germany-italy/ (last updated Mar. 11, 2020, 12:28 am); *see also* Carrie Cordero & Richard Fontaine, *Health Surveillance Is Here to Stay*, Wall St. J. (Mar. 27, 2020, 4:04 pm), www.wsj.com/articles/health-surveillance-is-here-to-stay–11585339451.

[3] *See* Simon Chandler, *Coronavirus Could Infect Privacy and Civil Liberties Forever*, Forbes (Mar. 23, 2020, 11:59 am), www.forbes.com/sites/simonchandler/2020/03/23/coronavirus-could-infect-privacy-and-civil-liberties-forever/#5583c1ba365d; Allison Grande, *COVID-19 Fuels Heated Fight over CCPA Enforcement Timing*, Law360 (Mar. 27, 2020, 8:39 pm), www.law360.com/articles/1257124/covid-19-fuels-heated-fight-over-ccpa-enforcement-timing; Ryan Grim, *Coronavirus Spending Bill Could Be Used to Cement Spying Powers, Surveillance Critics in Congress Warned*, Intercept (Feb. 27, 2020, 12:33 pm), https://theintercept.com/2020/02/27/coronavirus-spending-bill-surveillance-patriot-act/; Manancourt, *supra* note 2; *Statement of the European Data Protection Board on the Processing of Personal Data in the Context of the COVID Outbreak* (Mar. 19, 2020), https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

internet-connected thermometers and fever detection cameras.[4] The IoT is a network of internet-connected physical objects, systems, and software.[5] IoT devices and other technologies can be used to unmask our identities and monitor our health status, movements, location, and physical and behavioral responses to the pandemic, including assessing our compliance with social distancing guidelines and shelter in place orders.[6] To detect pandemic patterns, 2,000 health workers in San Francisco agreed to wear IoT rings manufactured by a startup firm.[7] The rings can monitor wearers' temperatures, heart rates, daily steps, and sleep patterns.[8] The city of St. Augustine, Florida plans to distribute hundreds of IoT thermometers to its citizens as part of a pandemic pilot study in partnership with an IoT thermometer

[4] *See, e.g.*, Dylan Byers, *The U.S. Wants Smartphone Location Data to Fight Coronavirus. Privacy Advocates Are Worried*, NBC NEWS (Mar. 18, 2020, 11:01 AM), www.nbcnews.com/news/amp/ncna1162821?__twitter_impression=true; Joseph Cox, *Surveillance Company Says It's Deploying "Coronavirus-Detecting" Cameras in US*, VICE (Mar. 17, 2020, 12:43 PM), www.vice.com/en_us/article/epg8xe/surveillance-company-deploying-coronavirus-detecting-cameras; April Glaser, "Fever Detection" Cameras to Fight Coronavirus? Experts Say They Don't Work, NBC NEWS (Mar. 27, 2020, 4:01 pm), www.nbcnews.com/tech/security/fever-detection-cameras-fight-coronavirus-experts-say-they-don-t-n1170791, Donald G. McNeil Jr., *Can Smart Thermometers Track the Spread of the Coronavirus*, N.Y. TIMES (Mar. 18, 2020), www.nytimes.com/2020/03/18/health/coronavirus-fever-thermometers.html#click=https://t.co/hzE6K2Fmtn; Jason Murdock, *Mobile App Could Help Stop Coronavirus Without Resorting to China-Like Surveillance*, NEWSWEEK (Mar. 17, 2020, 1:09 PM), www.newsweek.com/coronavius-covid19-mobile-app-alerts-trace-infections-oxford-university-research-1492754?amp=1&__twitter_impression=true.

[5] ARUBA, IOT AND THE SMART DIGITAL WORKPLACE: OPPORTUNITIES AND CHALLENGES 3 (2018), www.arubanetworks.com/assets/wp/WP_SmartDigitalWorkplaceIoT.pdf (The IoT "can be defined as a universe of devices, software, and systems that interact directly with the physical environment while communicating with each other and the IT infrastructure"); *see also* CISCO, AN INTRODUCTION TO THE INTERNET OF THINGS (IOT): PART 1. OF "THE IOT SERIES" 2 (2013), www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf (describing the IoT and noting that the term was coined by Kevin Ashton); INTEL, MAKING THE CONNECTION: HOW THE INTERNET OF THINGS ENGAGES CONSUMERS AND BENEFITS BUSINESS 3 (2016), www.intel.com/content/dam/www/public/us/en/documents/white-papers/how-iot-engages-consumers-benefits-business-paper.pdf (The IoT "uses the founding protocols of the internet to allow any electronic machine, device, object or sensor to send data to anywhere else on the network. This could be to another machine, database, application or device (e.g., smartphone).").

[6] *See, e.g.*, Kirsten Grind, Robert McMillan & Anna Wilde Mathews, *To Track Virus, Governments Weigh Surveillance Tools That Push Privacy Limits*, WALL ST. J. (Mar. 17, 2020, 7:55 PM), www.wsj.com/amp/articles/to-track-virus-governments-weigh-surveillance-tools-that-push-privacy-limits-11584479841; Tim Hornyak, *What America Can Learn from China's Use of Robot and Telemedicine to Combat the Virus*, CNBC, www.cnbc.com/2020/03/18/how-china-is-using-robots-and-telemedicine-to-combat-the-coronavirus.html (last updated Mar. 18, 2020, 9:06 AM); Issie Lapowsky, *Facebook Data Can Help Measure Social Distancing in California*, PROTOCOL (Mar. 17, 2020), www.protocol.com/facebook-data-help-california-coronavirus-2645513228.amp.html?__twitter_impression=true.

[7] Lisa Eadicicco, *Emergency Medical Workers in San Francisco Are Wearing Smart Rings that Can Monitor Body Temperature in an Effort to Detect COVID-19 Symptoms Early*, BUS. INSIDER (Mar. 24, 2020, 10:38 AM), www.businessinsider.com/coronavirus-smart-ring-san-francisco-hospitals-covid19-symptoms-study-oura-2020-3?amp.

[8] *Id.*

maker.[9] Amazon is already using IoT thermal cameras in some of its warehouses to identify and screen its workers who may be infected with the virus.[10] Government actors are reportedly already collecting the anonymized smartphone location data of millions of US citizens to track both the virus and individuals' movements.[11] The data are reportedly provided by mobile advertisers.[12]

As of the date of writing, it is unclear how much pandemic-related data will be collected, used, and disclosed and whether any corresponding limitations will be imposed. Depending on how these disease-related data are used and disclosed, there could be unintended consequences for COVID-19 victims, such as stigmatization. In South Korea, the government sends public safety text messages to citizens containing the location history, age range, and gender of those infected with the virus.[13] Although these disclosures may contribute to decreasing the spread of the virus, they have in some cases reportedly led to social shaming as well as embarrassing inferences of marital affairs, insurance fraud, and involvement with prostitutes.[14]

Containing the pandemic and ensuring public health and safety are without a doubt important societal and governmental goals. Many lives depend on these efforts. However, it is currently unclear whether a delicate and appropriate balance will be struck between public health protection and privacy, both of which have individual, collective, and societal value.[15] Privacy and public health goals can bolster and inform each other. They are not mutually exclusive. As legal scholars have noted, privacy can enable the development of civil society, "democratic deliberation," and individual autonomy.[16]

Technology giants' involvement in global pandemic responses also raises concerns about how much access, if any, these companies should have to our health-related and other pandemic-related data, and whether these companies can be

[9] Sheldon Gardner, *Coronavirus: St. Augustine to Use Smart Thermometers Against COVID-19*, St. Augustine (Mar. 31, 2020, 10:51 am), www.staugustine.com/news/20200331/coronavirus-st-augustine-to-use-smart–thermometers-against-covid-19.

[10] Jeffrey Dastin & Krystal Hu, *Exclusive: Amazon Deploys Thermal Cameras at Warehouses to Scan for Fevers Faster*, Reuters (Apr. 18, 2020, 4:07 am), www.reuters.com/article/us-health-coronavirus-amazon-com-cameras/exclusive-amazon-deploys-thermal-cameras-at-warehouses-to-scan-for-fevers-faster-idUSKBN2200HT.

[11] Byron Tau, *Government Tracking How People Move Around in Coronavirus Pandemic*, Wall. St. J. (Mar. 28, 2020), www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202.

[12] *Id.*

[13] Nemo Kim, *"More Scary than Coronavirus": South Korea's Health Alerts Expose Private Lives*, Guardian (Mar. 5, 2020, 11:46 pm), www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives.

[14] *Id.*

[15] *See generally* Priscilla M. Regan , Legislating Privacy: Technology, Social Values and Public Policy (1995) (noting that privacy has individual, collective, and societal value); James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 Wash. L. Rev. 1 (2003) (noting the same).

[16] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373, 1423–28 (2000); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L. Rev. 1609, 1647–58 (1999).

trusted to place societal interests above corporate goals. For example, Verily, Google's "sister company," is reportedly participating in pandemic relief efforts.[17] Apple and Google are working on a joint effort to enable pandemic contact tracing through users' devices.[18] Technology companies could use COVID-19 surveillance data about us to aid pandemic responses as well as to simultaneously or subsequently monetize and exploit these data to advance their own corporate objectives.[19] These companies' history of corporate data monetization and exploitation leaves some room for doubt. Only time can provide definitive answers to these questions. There is also the related question of whether changed circumstances resulting from the pandemic, such as the large number of individuals working from home, will contribute to data security vulnerabilities. Technology firms' participation in pandemic response efforts, and their resulting access to sensitive COVID-19 data, also raises concerns about whether effective measures will be taken to secure such data from unauthorized access. Data breaches are common, and many IoT devices are insecure.

The global pandemic is indeed the most recent development to generate privacy and security concerns. These issues are also germane and similar to pre-existing privacy and information security debates, including those involving IoT products. These questions include how to balance technological innovations against privacy, which is an important societal value, and how to regulate corporate and government actors' collection and processing of our data and surveillance of our activities.[20] The volume and types of data about us that are now easily available to companies have increased exponentially because of the IoT. The use of IoT devices, services, and systems in pandemic response efforts illustrates the established and ubiquitous nature of the IoT. What does the IoT's proliferation mean for us as consumers? This book seeks to shed light on this question by exploring the consumer ramifications of the IoT primarily through the lens of commercial law and privacy and security law, with a central focus on corporate conduct.

The IoT and various other technological developments allow companies to extend their digital dominance over our lives and activities and provide multiple opportunities for once-ordinary household objects to serve as surveillance equipment capable of continuously monitoring and collecting vast quantities of our data.

[17] *See* Mason Marks, *You Shouldn't Have to Give Google Your Data to Access a COVID-19 Test*, SLATE (Mar. 17, 2020, 3:05 PM), https://slate.com/technology/2020/03/covid19-coronavirus-testing-google-walmart-target-privacy.amp?__twitter_impression=true.

[18] *Apple and Google Partner on COVID-19 Contact Tracing Technology*, APPLE (Apr. 10, 2020), www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/; Russell Brandom, *Apple and Google Pledge to Shut Down Coronavirus Tracker When Pandemic Ends*, VERGE (Apr. 24, 2020, 12:15 PM), www.theverge.com/2020/4/24/21234457/apple-google-coronavirus-contact-tracing-tracker-exposure-notification-shut-down; Jack Nicas & Daisuke Wakabayashi, *Apple and Google Team Up to "Contact Trace" the Coronavirus*, N.Y. TIMES (Apr. 10, 2020), www.nytimes.com/2020/04/10/technology/apple-google-coronavirus-contact-tracing.html.

[19] Marks, *supra* note 17.

[20] REGAN, *supra* note 15, at 212–31.

Various IoT companies use privacy-invasive user default settings on IoT devices. Many smart televisions capture our viewing data by default.[21] To avoid data collection we must change default settings and, in some cases, must muddle through complicated privacy controls in order to do so.[22] In 2019, the average home had eleven connected products.[23] This number is expected to increase steadily as the IoT and mobile telecommunication systems expand.[24] If most IoT devices, mobile apps, and websites are collecting our data by default, how many mobile apps, websites, and device settings can each of us realistically review and revise to protect our privacy?

Consider that in 2019, Google and Amazon requested that IoT device makers who offer compatible devices design their products and services to ensure that they provide continuous streams of data to the technology giants.[25] For instance, an Alexa-enabled IoT device manufactured by a third-party IoT device maker must provide data to Amazon whenever the device is operational and also whenever it is turned off even if the consumer did not direct Alexa to turn the device on or off.[26] Similarly, IoT televisions can send continuous data streams about the channel they are tuned to, and IoT locks can send data about whether or not door bolts are engaged.[27] Prior to the change, these types of information were primarily provided to Amazon when a consumer issued a voice command to Alexa to operate third-party IoT devices.[28] These changes were reportedly made to increase IoT devices' performance and functionality.[29] From these continuous streams of data technology giants can glean unprecedentedly detailed information about us and our in-home behaviors, including our sleep and wake habits, the amount of time we spend at home, how frequently we use IoT products, and much more. Amazon dominates the

[21] Eli Blumenthal, *Just Got a New TV or Streamer? You Need to Change These Privacy Settings*, CNET (Dec. 30, 2019, 3:30 AM), www.cnet.com/google-amp/news/just-got-a-new-tv-or-streamer-you-need-to-change-these-privacy-settings/.

[22] *Id.*

[23] Todd Spangler, *U.S. Households Have an Average of 11 Connected Devices – and 5G Should Push That Even Higher*, VARIETY (Dec. 10, 2019, 8:48 AM), https://variety.com/2019/digital/news/u-s-households-have-an-average-of-11-connected-devices-and-5g-should-push-that-even-higher-1203431225/.

[24] *See* KEVIN WESTCOTT ET AL., DELOITTE CTR. FOR TECH., MEDIA & TELECOMM., BUILD IT AND THEY WILL EMBRACE IT 2(2019), www2.deloitte.com/content/dam/insights/us/articles/6457_Mobile-trends-survey/DI_Build-it-and-they-will-embrace-it.pdf.

[25] Matt Day, *Your Smart Light Can Tell Amazon and Google When You Go to Bed*, BLOOMBERG (Feb. 12, 2019, 2:00 AM), www.bloomberg.com/news/articles/2019-02-12/your-smart-light-can-tell-amazon-and-google-when-you-go-to-bed; *see also* David Priest, *Smart Home Developers Raise Concerns About Alexa and Google Assistant Security*, CNET (Mar. 15, 2020, 5:00 AM), www.cnet.com/news/smart-home-developers-raise-concerns-about-alexa-and-google-assistant-security/.

[26] Day, *supra* note 25.

[27] *See id.*

[28] *Id.*

[29] *See id.*; Terell Wilkins, *What You Need to Know About Amazon, Google, Smart Homes and Privacy*, SPECTRUM (Feb. 23, 2019, 8:59 AM), www.thespectrum.com/story/news/2019/02/23/p-c-periodicals-what-you-need-know-smart-home-privacy/2955184002/.

IoT smart speaker market.[30] Even if smaller IoT device manufacturers oppose technology giants' privacy-invasive practices, these smaller firms may be required to implement such practices or lose access to big technology firms' platforms, which could decrease consumers' willingness to purchase their products.[31]

Also, consider that Amazon's workers can listen to smart speaker users' Alexa conversations conducted in their homes.[32] Apple's external contractors can also reportedly review Siri conversations from users' Apple Watch and other Apple devices.[33] Technology giants' employees' and contractors' access to our IoT data is concerning in light of growing insider security threats.[34] Additionally, employees, contractors, and third parties with knowledge of the strength and weaknesses of related security infrastructure can pose a threat as well. It was, for example, a former Amazon employee who exploited a firewall weakness to carry out the 2019 Capital One data breach, which exposed the data of 106 million consumers that were stored in Amazon's cloud service.[35]

Design problems in IoT devices can also cause inadvertent data collection. Apple's Siri can mistakenly capture conversations when an individual wearing an Apple Watch lifts their wrist.[36] Similarly, smart speakers, including Amazon's Echo, can be accidentally activated and record in-home conversations.[37] One study of smart speakers found that these IoT devices could be erroneously activated nineteen times per day.[38]

[30] Kim Lyons, *Amazon Is Still Crushing Google and Apple in the Smart Speaker Market*, VERGE (Feb. 10, 2020, 4:57 PM), www.theverge.com/2020/2/10/21131988/amazon-alexa-echo-google-apple-smart-home-speaker.

[31] Priest, *supra* note 25.

[32] Kate O'Flaherty, *Amazon Staff Are Listening to Alexa Conversations – Here's What to Do*, FORBES (Apr. 12, 2019, 11:54 AM), www.forbes.com/sites/kateoflahertyuk/2019/04/12/amazon-staff-are-listening-to-alexa-conversations-heres-what-to-do/#756908e771a2.

[33] Kate O'Flaherty, *Apple Siri Eavesdropping Puts Millions of Users at Risk*, FORBES (July 28, 2019, 8:26 AM), www.forbes.com/sites/kateoflahertyuk/2019/07/28/apple-siri-eavesdropping-puts-millions-of-users-at-risk/#1d7d969ea530.

[34] *Insider Threats: How Co-Workers Became a Bigger Security Headache*, DICE (Feb. 27, 2020), https://insights.dice.com/2020/02/27/insider-threats-co-workers-bigger-security-headache/. *See generally* OBSERVE IT, 2020 COST OF INSIDER THREATS GLOBAL REPORT (2020), www.observeit.com/cost-of-insider-threats/.

[35] Robert McMillan, *Capital One Breach Casts Shadow over Cloud Security*, WALL ST. J. (July 30, 2019, 6:57 PM), www.wsj.com/articles/capital-one-breach-casts-shadow-over-cloud-security-11564516541; James Rundle & Catherine Stupp, *Capital One Breach Highlights Dangers of Insider Threats*, WALL ST. J. (July 31, 2019, 5:30 AM), www.wsj.com/articles/capital-one-breach-highlights-dangers-of-insider-threats-11564565402.

[36] O'Flaherty, *supra* note 33.

[37] Sara Morrison, *Alexa Records You More Often than You Think*, VOX (Feb. 21, 2020, 7:10 AM), www.vox.com/recode/2020/2/21/21032140/alexa-amazon-google-home-siri-apple-microsoft-cortana-recording; *see also* Kate O'Flaherty, *Amazon, Apple, Google Eavesdropping: Should You Ditch Your Smart Speaker?*, FORBES (Feb. 26, 2020, 10:12 AM), www.forbes.com/sites/kateoflahertyuk/2020/02/26/new-amazon-apple-google-eavesdropping-threat-should-you-quit-your-smart-speaker/#2f5cd710428d.

[38] *See* DANIEL J. DUBOIS ET AL., MON(IOT)R RESEARCH GRP., WHEN SPEAKERS ARE ALL EARS: UNDERSTANDING WHEN SMART SPEAKERS MISTAKENLY RECORD CONVERSATIONS, https://moniotrlab.ccis.neu.edu/smart-speakers-study/ (last updated Feb. 14, 2020).

The mobile fitness apps we download to our smartphones and use in conjunction with our IoT devices, such as smart watches, also raise privacy concerns. In 2020, an individual using the Runkeeper fitness app to track workouts became a suspect in a burglary after police obtained a geofence warrant to access data from all devices close to the crime scene.[39] The individual was subsequently cleared, but by using the mobile app he provided location data.[40] State actors' use of geofence warrants has increased steadily in the last few years.[41] IoT devices and associated mobile apps that collect our location data provide additional venues for data disclosures and geofence warrant requests. Solving crimes is an important government objective, but so too is privacy protection. The number of IoT devices that will needlessly collect our location data is only growing. In 2020, Asics announced plans to reveal a prototype of a smart running sneaker with embedded sensors that could work in conjunction with the company's Runkeeper app.[42] As more IoT devices flood the market, there are more potential methods for others to obtain access to information about us.

An increasing number of IoT devices are insecure. In 2019, the Food and Drug Administration announced that an implantable IoT cardiac device was susceptible to hacking.[43] IoT insulin pumps have also been found to have security flaws that allow hackers to remotely control the devices and revise dosage settings.[44] Some IoT companies and industries also have limited data security expertise.[45] A growing

[39] Kim Lyons, *Google Location Data Turned a Random Biker into a Burglary Suspect*, VERGE (Mar. 7, 2020, 5:23 PM), www.theverge.com/platform/amp/2020/3/7/21169533/florida-google-runkeeper-geofence-police-privacy.

[40] *Id.*

[41] Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html?mtrref=www.drudgereport.com&mtrref=www.nytimes.com.

[42] Vinciane Ngomsi, *ASICS to Launch an Entire Collection of Smart Shoes That Make You a Faster and Stronger Runner*, YAHOO SPORTS (Jan. 11, 2020, 10:21 AM), sports.yahoo.com/asics-to-launch-an-entire-collection-of-smart-running-shoes-heres-where-to-snag-your-own-pair-182150380.html; *see also ASICS Opens Doors to Innovation Labs at CES 2020*, PR NEWSWIRE (Jan. 7, 2020, 4:24 PM), www.prnewswire.com/news-releases/asics-opens-doors-to-innovation-labs-at-ces-2020-300983086.html.

[43] U.S. FOOD & DRUG ADMIN., CYBERSECURITY VULNERABILITIES AFFECTING MEDTRONIC IMPLANTABLE CARDIAC DEVICES, PROGRAMMERS, AND HOME MONITORS: FDA SAFETY COMMUNICATION (Mar. 21, 2019), www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home; *see also* Dave Johnson, *Can Pacemakers (and Other Medical Devices) Really Be Hacked?*, HOW-TO GEEK (July 18, 2019, 6:40 AM), www.howtogeek.com/427904/can-pacemakers-and-other-medical-devices-really-be-hacked/;
Liam Tung, *FDA Warning: Scores of Heart Implants Can Be Hacked from 20ft Away*, ZDNET (Mar. 22, 2019, 11:49 AM), www.zdnet.com/google-amp/article/fda-warning-scores-of-heart-implants-can-be-hacked-from-20ft-away/.

[44] Aimee Picchi, *Medtronic Recalls Insulin Pumps Because Hackers Could Hijack Device*, CBS NEWS (June 28, 2019, 9:16 AM), www.cbsnews.com/news/medtronic-insulin-pump-recall-fda-says-hackers-could-hijack-device/.

[45] Alison DeNisco Rayome, *Your Sex Tech Devices May Be Spying on You*, CNET (Jan. 18, 2020, 8:01 AM), www.cnet.com/google-amp/news/your-sex-tech-devices-may-be-spying-on-you/; *see also* Rose Minutaglio, *Is Your Sex Toy Spying on You?*, ELLE (Oct. 14, 2019), www.elle.com/culture/tech/

number of sex toys are now connected to the Internet and are controlled through mobile apps.[46] Many of these devices pose serious privacy risks and are insecure. They collect intimate data, including the exact date and time of use, frequency of orgasms, and vibration settings.[47] Consider that a Standard Innovation IoT sex toy and mobile app, which both users and their partners could remotely control, collected users' email addresses as well as information about their sexual habits without their consent.[48] These data could be used to identify users. The class action lawsuit that followed was subsequently settled.[49] IoT sex toys that are accompanied by cameras pose an even greater risk as they can capture users engaging in sexual acts.[50] For instance, researchers were able to easily hack the video feed of a Svakom IoT sex toy.[51] The data collected by these devices and the associated mobile apps could be used to stigmatize, blackmail, and harass victims.[52]

The IoT also allows companies to extend their digital control over us post transaction. In the subprime auto lending industry, lenders require subprime borrowers to accept installation of monitoring devices in their vehicles. These devices allow lenders to observe users' location and remotely disable their vehicles. Also, consider that in 2020, Tesla allegedly remotely disabled the autopilot feature in a consumer's vehicle after the car was sold without providing notice and obtaining prior consent.[53] IoT companies can also remotely disable our devices when we provide negative online reviews of their products.[54] IoT firms can "brick" our devices after we purchase them

a28846210/smart-sex-toy-dildo-butt-plug-hacking/; Danny Palmer, *Cybersecurity: These Are the Internet of Things Devices That Are Most Targeted by Hackers*, ZDNet (June 12, 2019, 9:00 AM), www.zdnet.com/google-amp/article/cybersecurity-these-are-the-internet-of-things-devices-that-are-most-targeted-by-hackers/.

[46] DeNisco Rayome, *supra* note 45; *see also* Press Release, Access Now, Access Now Asks U.S. FTC to Investigate Vulnerabilities in Internet-Enabled Sex Toy (Apr. 26, 2017, 9:04 AM), www.accessnow.org/access-now-asks-u-s-ftc-investigate-vulnerabilities-internet-enabled-sex-toy/.

[47] DeNisco Rayome, *supra* note 45; *see also* Shayna Possess, *Vibrator Gets Too Intimate by Tracking Usage Info, Suit Says*, Law360 (Sept. 15, 2016, 3:57 PM), www.law360.com/articles/840299/vibrator-gets-too-intimate-by-tracking-usage-info-suit-says.

[48] Possess, *supra* note 47.

[49] *See* Judgment, N.P. v. Standard Innovation, No. 1:16-cv-8655, 2017 WL 10544062 (N.D. Ill. Aug. 15, 2017); Report and Recommendation, N.P. v. Standard Innovation, No. 16-cv-8655, 2017 WL 10544061 (N.D. Ill. July 25, 2017); *see also* Ry Crist, *Screwed by Sex Toy Spying? You May Get $10k*, Cnet (Mar. 14, 2017, 8:30 AM), www.cnet.com/news/app-enabled-sex-toy-users-get-10000-each-after-privacy-breach/#ftag=CAD-00-10aag7d; Diana Novak Jones, *Web-Enabled Vibrator Class Action Ends with $3.75M Deal*, Law360 (Aug. 15, 2017, 4:39 pm), www.law360.com/articles/954375.

[50] Complaint and Request for Investigation, Injunction and Other Relief, *In re* Svakom Design USA Ltd. (Apr. 26, 2017), www.accessnow.org/cms/assets/uploads/2017/04/AccessNow-FTCComp-Svakom.pdf.

[51] *Id.* at 3–4.

[52] Access Now, *supra* note 46.

[53] Jason Torchinsky, *Tesla Remotely Removes Autopilot Features from Customer's Used Tesla Without Any Notice*, Jalopnick (Feb. 6, 2020, 4:10 PM), https://jalopnik.com/tesla-remotely-removes-autopilot-features-from-customer-1841472617.

[54] Rob Price, *The Maker of an Internet-Connected Garage Door Disabled a Customer's Device over a Bad Review*, Bus. Insider (Apr. 5, 2017, 3:51 AM), www.businessinsider.com/iot-garage-door-opener-garadget-kills-customers-device-bad-amazon-review-2017-4.

by failing to provide the necessary software updates and by also terminating the online services that are necessary for our devices to function. The Revolv smart hub is one such example. Thus, in the IoT setting we may purchase devices, but we now have significantly less control over how these devices function. Instead, it is the company that manufactures the device and provides the services required for device functionality that has true control over us and our devices.

The IoT may provide some benefits to individuals, including increased efficiency, convenience, and enhanced seamless and responsive user experiences.[55] It could also be beneficial to specific groups of consumers, such as those that are disabled, by increasing their access to services and goods and ability to participate in daily activities.[56] However, these groups of consumers are not immune to the privacy and security concerns the IoT raises. Moreover, while the IoT increasingly invades our lives and technology firms obtain more detailed access to information about us and our families, these companies are also able to simultaneously obfuscate their data mining and manipulation activities by using non-disclosure agreements, trade secrecy, and various other tactics.[57] Companies use these data analytics practices to determine how to treat us and what opportunities we will receive. Various legal frameworks strongly protect the secrecy of corporate entities in the commerce context, but the law fails to sufficiently do the same with respect to our privacy.[58] As a result, the various IoT concerns I have discussed so far are likely just the tip of the iceberg. If left unchecked, the harms the IoT generates will outweigh its possible benefits, if they do not already.

Many of the IoT examples discussed earlier raise several legal questions that implicate both privacy and security law and commercial law. For instance, companies often disclose their data collection and use practices in their privacy policies. Companies' online terms and conditions, which often contain mandatory arbitration provisions, can also incorporate privacy policies. Companies obtain rights in our data and permission to collect and use our data through these documents. Further, many IoT devices lack the traditional screens found on smartphones and computers that are typically used to display privacy policies and terms of service as well as any amended provisions. If an IoT company suffers a cybersecurity incident or if an IoT product causes physical or what are often seen as intangible privacy harms, are existing contract law principles addressing consent and products liability law adequate in today's IoT age? I argue in this book that they are not. Contract law is

[55] *See* Steve Ranger, *What Is the IoT? Everything You Need to Know About the Internet of Things Right Now*, ZDNET (Feb. 3, 2020, 2:45 PM), www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/.

[56] LAUREN SMITH ET AL., FUTURE OF PRIVACY FORUM, THE INTERNET OF THINGS (IOT) AND PEOPLE WITH DISABILITIES: EXPLORING THE BENEFITS, CHALLENGES, AND PRIVACY TENSIONS (2019), https://fpf.org/wp-content/uploads/2019/01/2019_01_29-The_Internet_of_Things_and_Persons_with_Disabilities_For_Print_FINAL.pdf.

[57] FRANK PASQUALE, BLACK BOX SOCIETY 2–3 (2015).

[58] *Id.*

a core source of technology giants' "economic power."[59] Contract law and products liability law must evolve to acknowledge the realities of the circumstances surrounding consent in the IoT era as well as the new types of harms that the IoT raises. Another complicating factor is the role of large technology companies, such as Amazon, that both manufacture IoT devices and provide a platform for third-party sellers to sell IoT devices and other items. Courts' interpretation of federal law and state products liability laws can limit platform companies' exposure to liability for privacy-invasive and insecure IoT devices sold by third parties on their platforms. Consider that a *Wall Street Journal* investigation determined that 4,152 items for sale on Amazon's website were "declared unsafe by federal agencies."[60] Many of these products were potentially deceptively labeled, including 2,000 toy and medication listings.[61]

In the IoT setting, not only must we concern ourselves with the prospect of insecure and privacy-invasive IoT devices that we purchase directly from companies, we must also consider largely overlooked risks that the IoT raises and which are enabled by multiple sources of commercial law and corporate law. Companies use corporate and commercial law frameworks to facilitate data transfers among themselves. Companies' privacy policies and terms of service often contain provisions that enable our data to be disclosed and transferred in corporate transactions. The data that IoT devices and connected mobile apps collect about us can be transferred and sold to others in bankruptcy proceedings. For instance, if the maker of an IoT sex toy goes bankrupt, one if its most valuable assets is likely to be the email addresses and masturbatory habits of individuals using its products. There is also the possibility that companies could use their rights in our data to secure loans by granting lenders a lien on those rights.

Technology giants, such as Amazon and Google, continue to solidify their data market dominance and power by acquiring smaller IoT companies. Google's acquisition of Nest and Amazon's acquisition of Ring are but a few of these examples. Through these acquisitions, technology companies not only acquire a steady stream of talent and the rights to products acquired companies offer, but they also obtain the data we provided to acquired companies. These data acquisitions allow technology

[59] Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism 63 (2019); Amy Kapczynski, *The Law of Information Capitalism*, 129 Yale L. J. 1460, 1482, 1489–90 (2020); Margaret Jane Radin , Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law 7–9, 12–15 (2013).

[60] Alexandra Berzon, Shane Shifflett & Justin Scheck, *Amazon Has Ceded Control of Its Site. The Result: Thousands of Banned, Unsafe or Mislabeled Products*, Wall St. J. (Aug. 23, 2019, 8:56 am), www.wsj.com/articles/amazon-has-ceded-control-of-its-site-the-result-thousands-of-banned-unsafe-or-mislabeled-products-11566564990 [hereinafter *Amazon Has Ceded Control*]; *see also* Alexandra Berzon, Shane Shifflett & Justin Scheck, *Senators Want Answers About Listings for Unsafe Merchandise on Amazon.com*, Wall St. J. (Aug. 29, 2019, 6:39 pm), www.wsj.com/articles/democratic-senators-want-answers-about-listings-for-unsafe-merchandise-on-amazon-com-11567101615.

[61] Berzon et al., *Amazon Has Ceded Control*, *supra* note 60.