REGULATING THE INTERNET OF THINGS: DISCRIMINATION, PRIVACY, AND CYBERSECURITY IN THE ARTIFICIAL INTELLIGENCE AGE

CHARLOTTE A. TSCHIDER[†]

ABSTRACT

The field of consumer Internet of Things (IoT) has exploded as business and researchers have sought to not only develop Internet-connected products but also define the common structure in which IoT devices will operate, including technological standards and responsive architectures. Yet, consumer IoT continues to present a host of potential risks to consumers, cascading from the multidimensional nature of IoT devices: IoT combines well-known consumer products with cutting-edge infrastructures including big data solutions, distributed data storage or "cloud," and artificial intelligence (AI) utilities. The consumer device is no longer only the product, it is the product, the data, the algorithms, and the infrastructure.

Consumer products have shifted from analog to connected technologies, introducing new risks for consumers related to personal privacy, safety issues, and potential for discriminatory data. Broad, ubiquitous data collection, internet connectivity, predictive algorithms, and overall device functionality opacity threaten to undermine IoT market benefits by causing potential consumer injury: broad unfairness and disparate impact, data breaches, physical safety issues, and property damage. Existing regulatory regimes have not anticipated these damages to effectively avoid injury, and it is yet unknown how existing products liability, common law civil recovery under contracts or torts schemes, and due process procedures will apply to these products and the data they process. This Article explores the technology and market of IoT, potential consumer impacts resulting from a lack of consistent and complete legal framework, whether IoT regulation is appropriate, and how the United States can balance market needs for innovation with consistent oversight for IoT manufacturers and distributors.

---

† Charlotte A. Tschider is the Jaharis Faculty Fellow for the DePaul University College of Law and a Fulbright Specialist in cybersecurity and privacy law. Professor Tschider writes on a variety of topics involving law and technology, including information privacy, artificial intelligence, health technology policy, and regulation of corporate cybersecurity. I would like to thank Professor Nicholson Price, Professor Sharon Sandeen, and Leona Lewis for useful discussions leading to this Article and the 2017 Internet Works in Progress conference attendees and ISC2 2017 Security Congress attendees for their helpful directional comments on an early form of this Article.

TABLE OF CONTENTS

> "Technology only gives us tools. Human desires and institutions decide how we use them."[1]
>
> Freeman J. Dyson

INTRODUCTION

Since 1999, the field of consumer Internet of Things (IoT) has exploded, as business and researchers have sought to not only develop internet-connected products but also define the common structure in which IoT devices will operate: cybersecurity standards, flexible and responsive architectures, and reasonable legal frameworks.[2] The challenge of regu-

1. FREEMAN J. DYSON, THE SUN, THE GENOME, AND THE INTERNET: TOOLS OF SCIENTIFIC REVOLUTIONS, at xii (1999).

2. *See, e.g.*, Existing Standards, Tools and Initiatives Working Grp., Nat'l Telecomms. & Info. Admin., Catalog of Existing IoT Security Standards Version 0.01 (Sept. 12, 2017) (draft), https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog_draft_09.12.17.pdf; *see also* M.A. Burhanuddin et al., *Internet of Things Architecture: Current Challenges and Future*

lating consumer IoT cascades from the multidimensional nature of IoT devices. IoT combines well-known consumer products with cutting-edge infrastructures including: big data solutions, distributed data storage or "cloud," and artificial intelligence (AI) utilities.[3] Consumers, organizations, and governments have already begun to install these devices in a variety of sectors: home, cities, environment, energy, retail, logistics, agriculture, industrial applications, health, and lifestyle.[4]

Consumer products have shifted from analog to connected technologies, introducing new risks for consumers related to personal privacy, safety issues, and potential for discriminatory data. Broad, ubiquitous data collection, internet connectivity, predictive algorithms, and overall device functionality opacity threaten to undermine IoT market benefits by causing potential consumer injury: broad unfairness and disparate impact, data breaches, physical safety issues, and property damage.[5] Existing regulatory regimes have not anticipated these damages to effectively avoid injury, and it is yet unknown how existing products liability, common law civil recovery under contracts or torts schemes, and due process procedures will apply to these products and the data they process.

In Part I, this Article explores the IoT market and technology as developed today to illustrate complexities and considerations that underlie a privacy and cybersecurity regulatory approach for consumer IoT. Part II describes discrimination, privacy, and cybersecurity risks, examining the multidimensional nature of IoT devices and impact on both consumers and business. In Part III, this Article explores existing *ex ante* cybersecurity and privacy statutes in the United States and the European Union (EU) to identify potential regulatory opportunities and models. In

---

Direction of Research, 12 INT'L J. APPLIED ENGINEERING RES. 11,055, 11,055–59 (2017), https://pdfs.semanticscholar.org/b41e/c7a3a1d26c84893684d4ba110a7af4887a14.pdf (describing existing architectures for IoT and potential issues associated); Laura DeNardis & Mark Raymond, *The Internet of Things as a Global Policy Frontier*, 51 U.C. DAVIS L. REV. 475, 479 (2017) (introducing a framework for understanding potential public interest impacts).

3. Critically, IoT devices integrate physical devices with big data repositories and increasingly opaque advanced algorithms, whether created by machine learning or data scientists. For these reasons, concerns related to algorithmic decision-making necessarily apply to IoT device use too. *See* Mika Tanskanen, *Applying Machine Learning to IoT Data*, SAS (Aug. 18, 2018), https://www.sas.com/en_us/insights/articles/big-data/machine-learning-brings-concrete-aspect-to-iot.html.

4. ARSHDEEP BAHGA & VIJAY MADISETTI, INTERNET OF THINGS: A HANDS-ON APPROACH 21 (2014).

5. W. Nicholson Price II and Roger Allan Ford identify two crucial challenges for opaque algorithm usage for healthcare data, yet these concerns also apply to additional data types. *See generally* Roger Allan Ford & W. Nicholson Price II, *Privacy and Accountability in Black-Box Medicine*, 23 MICH. TELECOMM. & TECH. L. REV. 1, 12–21 (2016) (identifying these two areas of emphasis as they apply to opaque healthcare algorithms). The two challenges include algorithmic accountability, which encourages accuracy and unbiased outputs, and privacy, which may run at cross-purposes with accountability goals. *Id.* Although consumer IoT applications incorporate broader concepts, these dual concerns necessarily apply to new contexts outside the healthcare sector. *See id.* at 29.

Part IV, the Article suggests future efforts for an appropriate IoT regulatory approach to effectively manage consumer safety and create balanced expectations for market competition.

I. THE IOT MARKET AND TECHNOLOGY

Kevin Ashton first coined the term, "Internet of Things," or IoT, to give special distinction to internet-connected consumer products.[6] Modern IoT has since evolved to include consumer-facing, industrial, and medical products, a market-differentiating offering from traditional, analog, or untethered products.[7] The value proposition for IoT products includes greater connectivity and therefore utilization, with enhanced convenience and the potential for regular feature updates.[8]

Consumer-facing devices, such as those used in the home, can be scheduled and monitored remotely, improving an individual's ability to manage household activities when traveling, completing errands, or working.[9] Manufacturers market IoT devices as enabling convenience and efficiency: IoT devices can run the washing machine you forgot to start, provide a shopping list and order items to arrive at your door, or provide visibility to who visits your home when children arrive after school.[10] Businesses have similarly identified potential benefits for such devices, as has the U.S. government, and both have already begun using and heavily investing in IoT.[11]

---

6. W. Kuan Hon et al., *Twenty Legal Considerations for Clouds of Things* 4 (Queen Mary Univ. of London, Sch. of Law, Research Paper No. 216, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2716966. Hon et al. have established key classes and associated terms for discussing and defining concepts associated with IoT. *Id.* at 6–8.

7. *See* Marco Iansiti & Karim R. Lakhani, *Digital Ubiquity: How Connections, Sensors, and Data Are Revolutionizing Business*, HARV. BUS. REV., Nov. 2014, at 90, 92, 98; Michael E. Porter & James E. Heppelmann, *How Smart, Connected Products Are Transforming Competition*, HARV. BUS. REV., Nov. 2014, at 64, 66; Jacob Morgan, *A Simple Explanation of 'The Internet of Things,'* FORBES (May 13, 2014, 12:05 AM), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand. The use of the term "analog" devices by the Author is meant to illustrate a distinct difference between consumer devices that may have embedded software, but are not networked, and those properly considered consumer IoT devices.

8. Porter & Heppelmann, *supra* note 7, at 66, 79.

9. Darla Scott, *ISTR Insights: The Internet of Things (IoT) and the Concerns of Convenience*, SYMANTEC CONNECT: THOUGHT LEADERSHIP (Sept. 14, 2016), https://www.symantec.com/connect/blogs/istr-insights-the-internet-of-things-iot-and-the-concerns-of-convenience. Convenience drives much of IoT adoption; risks accompany such convenience. *Id.*

10. *See* Ramsay Henderson, *How the IoT Offers Efficiency and Convenience in Your Home and Workplace*, LINKEDIN (Mar. 14, 2017), https://www.linkedin.com/pulse/how-iot-offers-efficiency-convenience-your-home-ramsay-henderson. Convenience and efficiency, however, may come at a cost in the form of poor cybersecurity. Andy Thomas, *Beware the Trade-Off Between IoT Convenience and Security*, INTERNET BUS. (Jan. 28, 2016), https://internetofbusiness.com/beware-trade-off-iot-convenience-security.

11. *Business Is Embracing Internet of Things as Most Important Technology, Says New Study*, FORBES (Jan. 16, 2018), https://www.forbes.com/sites/forbespr/2018/01/16/business-is-embracing-internet-of-things-as-most-important-technology-says-new-study; Andrew Meola, *The US Government Is Pouring Money into the Internet of Things*, BUS. INSIDER (May 31, 2016, 3:38 PM), http://www.businessinsider.com/the-us-government-is-pouring-money-into-the-internet-of-things-2016-5.

Internet connectivity drives a significant convenience factor through remote direction or information gathering, which translates to substantial market growth. Gartner, International Data Corporation, and HIS have estimated the total active number of IoT devices to be between 6.4 billion and 17.6 billion.[12] The same organizations have projected IoT to grow to 30 billion devices by 2020, along with other organizations predicting $470 billion in revenue by 2020.[13] Cisco analysts have projected $14.4 trillion in global value by 2022.[14] IoT presents enormous market potential for the United States, incentivizing manufacturers to enter a market previously occupied by technology giants and internet companies.

IoT devices also require access to cable or other high-performance internet resources to optimize service.[15] For IoT devices to maximize their potential benefit, consumers must connect these devices pervasively to the internet to facilitate real-time software updates or support interactive features, as with virtual multiplayer games or learning systems.[16] When a product enables real-time updates, new content and improved services become compelling reasons to purchase IoT devices.[17] A consumer does not need to purchase the newest version as frequently when the product updates its own software to include new features.[18] IoT technology infrastructure often includes decentralized, high performance big data solutions enabled by cloud services and dynamic learning systems, including AI.[19] With this infrastructure, IoT devices perform more effectively but also require collection and retention of substantially more device data and personal information.[20]

---

12. Amy Nordrum, *Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated*, IEEE SPECTRUM (Aug. 18, 2016, 1:00 PM), http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated.

13. Louis Columbus, *Roundup of Internet of Things Forecasts and Market Estimates, 2016*, FORBES (Nov. 27, 2016, 1:06 PM), http://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016; Nordrum, *supra* note 12.

14. Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J. L. & TECH. 6, 15 (2015).

15. *See* Gaël Hernández et al., Org. for Econ. Co-operation & Dev. [OECD], *The Internet of Things: Seizing the Benefits and Addressing the Challenges*, at 5, DSTI/ICCP/CISP(2015)3/FINAL (May 24, 2016), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2015)3/FINAL&docLanguage=En.

16. *See id.* at 18, 38.

17. *See* Gatis Paeglis, *Over-the-Air Updates, Part 1: Introduction*, QT BLOG (May 31, 2016), https://blog.qt.io/blog/2016/05/31/over-the-air-updates-part-1-introduction.

18. *See id.*; *see also* Hernández et al., *supra* note 15, at 38.

19. *See* Hannah Williams, *IoT Trends 2018: Artificial Intelligence, Security, and Edge Solutions*, COMPUTERWORLD UK (Dec. 27, 2017), https://www.computerworlduk.com/iot/iot-trends-2018-artificial-intelligence-cybersecurity-edge-solutions-3669388.

20. *See* Tim Allen, *How to Solve IoT's Big Data Challenge with Machine Learning*, FORBES (Feb. 2, 2017, 8:35 AM), http://www.forbes.com/sites/sap/2017/02/02/how-to-solve-iots-big-data-challenge-with-machine-learning; Daniel Gutierrez, *Unlock the Potential of IoT with Real-Time Data*, INSIDEBIGDATA (Sept. 26, 2016), http://insidebigdata.com/2016/09/26/unlock-the-potential-of-iot-with-real-time-data.

A. Consumer IoT: New Service, New Hardware

IoT devices can be divided into three functional groups: physical components (such as mechanical, electrical, and housing); smart components (such as enhanced sensors, microprocessors, software, operating system, and applications); and connectivity components (ports, antennae, and protocols enabling wired or wireless reception or transmission of information).[21]

IoT products require technical upgrades in the form of smart components and connectivity components; therefore, a new technology infrastructure or "stack" is required for IoT devices, and presumably new infrastructure manufacturers must purchase to create IoT products.[22] This stack includes not only the device, device operating system, smart components, and software applications but also a product cloud or software running on the manufacturer's (or manufacturer's third party's) server.[23] The product cloud is a crucial part of an IoT implementation as it controls not only what information or commands are sent to IoT devices but also which data are collected and how data are analyzed.[24]

Within the product cloud, a product data database, application platform, rules engine, and analytics platform work together to both receive and process data from the device and also send application content and other information to the IoT device.[25] Depending on the IoT device, external sources of data might be integrated with the manufacturer's data, or applications could be connected to additional, synchronized backend business systems.[26] IoT devices can be integrated into larger systems, where devices depend on each other to trigger behavior.[27] For example,

21. *See* Hon et al., *supra* note 6, at 5–6. IoT must be able to actuate, which involves transmitting or receiving data, and conducting some action upon or within themselves or their environments. *Id.* This aspect delineates between computerized things and IoT devices specifically. *See id.* This actuation of data transmission, reception, and resulting action creates new threat vectors through which cyberattackers may steal data or service interruption and data integrity issues may occur. *Id.* at 9–10.

22. Porter & Heppelmann, *supra* note 7, at 68–69.

23. *See id.*

24. *See id.*; Hon et al., *supra* note 6. In the context of IoT, the technology stack might include a "product cloud," but implementation itself is a cloud service. Hon et al., *supra* note 6. By definition, this is a service managed in a physically separate location from the device itself, which may or may not be hosted by the manufacturer. *See id.* at 4–6. In some cases, a manufacturer for ease of use may select a third-party cloud provider to host the product cloud, which could in many cases involve a large data store of product data and an application server which uses code both to derive analytics from product data but also to run applications on connected devices. *Id.* at 8, 14. Cloud implementations may pose more significant risk to consumers under these circumstances, since third parties often subcontract to other third parties down the line, which can make it difficult for manufacturers to ensure appropriate privacy and cybersecurity requirements are implemented. *See infra* Part II; *see also* Hon et al., *supra* note 6, at 9–12. Although the use of cloud computing is not required for IoT functionality, cloud computing is considered an enabling technology, as an efficient, scalable means to provide IoT service. *Id.* at 4. As such, manufacturers will likely turn to cloud computing. *See id.*

25. Porter & Heppelmann, *supra* note 7, at 67–68.

26. JR Fuller, *The 4 Stages of an IoT Architecture*, TECHBEACON (May 26, 2016), https://techbeacon.com/4-stages-iot-architecture.

27. *See id.*

connected and integrated farm-equipment devices may use information that a certain activity has been done to signal the start of another activity.[28] Similarly, a connected home could program a digitally unlocked door to trigger a temperature increase, turn on lights, and disable the home security system.[29]

In addition to backend technical components, IoT devices pose unique challenges in terms of usability and ongoing support. Designs now must support customization, personalization, software upgrades, and remote service, as well as new hardware standardization.[30] The introduction of a connected service creates additional service and maintenance requirements.[31] Collecting product data should improve user experience and product performance over time, and help organizations avoid future issues.[32]

IoT requires substantial aggregation of data cross device and cross geographies to effectively fulfill its value proposition.[33] Unfortunately, data aggregated, transmitted, stored, and used by manufacturers may increase the potential for discriminatory practices and pose substantial privacy and cybersecurity challenges. The data processed and stored in many cases includes geolocation information, product-identifying data, and personal information related to use or owner identity, such as biometric data, health information, or smart-home metrics.[34] IoT devices may also capture personal information through audio or video, or include communication capabilities, such as those used in children's devices.[35] Data stored in an IoT system will often reside in the product cloud or other backend systems, and devices may also store this data within de-

28. *See id*.

29. Jennifer Schlesinger & Andrea Day, *Suddenly Hot Smart Home Devices Are Ripe for Hacking, Experts Warn*, CNBC (Dec. 25, 2016, 5:06 PM), http://www.cnbc.com/2016/12/25/suddenly-hot-smart-home-devices-are-ripe-for-hacking-experts-warn.html; *see* Porter & Heppelmann, *supra* note 7, at 73.

30. Nancy Spurling Johnson, *Internet of Things: What It Means for Designers and Their Companies*, CADALYST (Jan. 22, 2015), http://www.cadalyst.com/cad/product-design/internet-things-what-it-means-designers-and-their-companies-22132.

31. *See id.*

32. *See id.*

33. *The Importance of Defining a Value Proposition for the Internet of Things*, IRONPAPER: INSIGHTS (June 1, 2016), https://www.ironpaper.com/webintel/articles/the-importance-of-defining-a-value-proposition-for-the-internet-of-things; *see* Spurling Johnson, *supra* note 30.

34. GREG LINDSAY ET AL., ATLANTIC COUNCIL, SMART HOMES AND THE INTERNET OF THINGS 2–8 (2016), https://otalliance.org/system/files/files/initiative/documents/smart_homes_0317_web.pdf (describing cybersecurity and privacy protections for smart home technologies); David C. Vladeck, *Consumer Protection in an Era of Big Data Analytics*, 42 OHIO N.U. L. REV. 493, 498 (2016); Janice Phaik Lin Goh, *Privacy, Security, and Wearable Technology*, LANDSLIDE, Nov./Dec. 2015, at 30, 30–32; Stacey Higginbotham, *Companies Need to Share How They Use Our Data. Here Are Some Ideas.*, FORTUNE (July 6, 2015), http://fortune.com/2015/07/06/consumer-data-privacy; *see* Vassiliki Andronikou et al., *Biometric Implementations and the Implications for Security and Privacy*, FIDIS (Jan. 2007), http://www.fidis.net/fileadmin/journal/issues/1-2007/Biometric_Implementations_and_the_Implications_for_Security_and_Privacy.pdf.

35. TREND MICRO, INTERNET OF THINGS BUYER'S GUIDE FOR SMART PARENTS AND GUARDIANS 5–9 (2016), https://documents.trendmicro.com/assets/guides/eguide-iot-for-kids.pdf.

vice memory.[36] IoT data storage in backend systems and on the IoT device itself both present challenges to protect data and devices from cyberattacks.[37]

In addition to personal-information privacy concerns, IoT devices create data used for system operation, which is not typically considered personal information.[38] Cyberattackers could misuse these data by compromising data availability or changing data, causing data integrity issues,[39] and using big data insights to reinforce or create discriminatory outcomes.[40] When data is not available, causing a system to fail, damage could result—for example a smart home's furnace overheats or an individual's medical device cannot function.[41] Data integrity may cause more substantial issues. When attackers change data, such as scrambling, changing values, or replacing data with its own, information provided to users could be misleading, or previously established limits or algorithms directing device functionality could change.[42] For example, a smart oven could exceed manufacturer recommendations or a child could receive inappropriate messages on a connected toy. These types of data misuse can cause property damage and personal safety issues in addition to previously established privacy concerns.[43]

IoT devices, in addition to actuating behavior, have the unique ability to communicate with each other.[44] Machine-to-machine communication (M2M) could improve IoT cross communication and, ultimately, functionality, especially where IoT benefit from data aggregation and associated insights.[45] However, the ability of IoT devices to exchange data and connect with one another via standardized M2M communication, or "interoperability," could exacerbate infrastructures making decisions that could lead to discriminatory impact, multiply inherent IoT

---

36. *See id.* at 10.

37. Ashwin Pal, *The Internet of Things (IoT)—Threats and Countermeasures*, CSO, http://www.cso.com.au/article/575407/internet-things-iot-threats-countermeasures (last visited Oct. 4, 2018).

38. *See id.*

39. *Id.*

40. Richard Lee, *Discrimination Drives the Need for Ethics in Big Data*, IBM BIG DATA & ANALYTICS HUB (Oct. 13, 2014), http://www.ibmbigdatahub.com/blog/discrimination-drives-need-ethics-big-data; *see infra* Section II.A and accompanying notes.

41. Jeff Kitson, *Turning Up the Heat on IoT: TRANE Comfortlink XL850*, TRUSTWAVE: SPIDERLABS BLOG (Aug. 8, 2016), https://www.trustwave.com/Resources/SpiderLabs-Blog/Turning-Up-The-Heat-on-IoT--TRANE-Comfortlink-XL850 (analyzing the potential for cyberkinetic attacks for home IoT devices); Fred Pennic, *FBI Issues IoT Security Warning for Medical Devices, Wearables*, HIT CONSULTANT (Sept. 17, 2015), https://hitconsultant.net/2015/09/17/fbi-issues-iot-security-warning-medical-devices-wearables.

42. *See* Hernández et al., *supra* note 15, at 19. Multiple examples exist for how a lack of data integrity could lead to damaging consequences, including everything from malfunctioning medical devices to autonomous vehicles. *Id.*

43. *See generally* Vladeck, *supra* note 34, at 501, 514 (describing privacy concerns for IoT and other big data aggregation).

44. Hon et al., *supra* note 6, at 9.

45. *See id.*

cybersecurity issues, and compromise consumer privacy across multiple products and features.[46]

B. Big Data, Artificial Intelligence, and Cloud Services

"Ubiquitous computing" has become synonymous with IoT and associated infrastructure.[47] IoT requires big data and creates big data: because IoT devices are always tethered to the internet, real-time data creation requires storage and analysis.[48] Further, data analyses conducted on big data stores improve functionality of IoT devices and identify device upgrades or changes needed for more efficient or effective devices.[49] Data collected, especially demographic data and use statistics, also improve manufacturer marketing, sales, and product offerings.[50] Data collection enhances market offerings and device efficacy, which improves customer opportunities.[51]

Large data volumes also enable data aggregation for purposes of sale, transfer, and exchange.[52] Manufacturers may combine IoT-created data with other information about IoT device users such as: buying habits, web browsing history, demographic data, or other codified behaviors. The manufacturers may sell or transfer this data to a third party.[53] This type of data may prove highly lucrative both for manufacturers selling

---

46. Ellyne Phneah, *M2M Challenges Go Beyond Technicalities*, ZDNET (June 19, 2012, 10:34 AM), http://www.zdnet.com/article/m2m-challenges-go-beyond-technicalities. M2M and other interoperability standards are valuable for reliability, for maintenance, and for market development overall. *Id.* Interoperability has tremendous promise for reducing costs and increasing efficiency within and between devices, yet such standards could also exacerbate discriminatory impact, cybersecurity issues, and privacy impacts if not executed taking these potential risks into account. Consider, for example, broad adoption of a training database with test data used in AI: if all manufacturers use the same training database with the same test data, and both the training features and the data codify discriminatory impact. In this example, it is more likely than not that manufacturers will codify discriminatory impact into their systems. The same concerns apply for cybersecurity and privacy impacts.

47. ETHEM ALPAYDIN, MACHINE LEARNING: THE NEW AI 9 (2016).

48. *See* Hon et al., *supra* note 6, at 4–5.

49. *See id.* at 4; Daniel Graham, *How the Internet of Things Changes Big Data Analytics*, LINKEDIN (Oct. 6, 2016), https://www.linkedin.com/pulse/how-internet-things-changes-big-data-analytics-daniel-graham. The scale of data transmitted by IoT is substantially larger than other data collection activities. WORLD ECON. FORUM & THE BOS. CONSULTING GRP., UNLOCKING THE VALUE OF PERSONAL DATA: FROM COLLECTION TO USAGE 7–8 (2013), http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf. As a result, IoT will not be usable without big data use and appropriate big data analytics strategies.

50. *Should Companies Profit by Selling Customers' Data?*, WALL ST. J. (Oct. 24, 2013, 1:22 PM), https://www.wsj.com/articles/SB10001424052702304410204579143981978505724 (interviewing Noreena Hertz). Different perspectives exist for whether companies should profit by selling data; nevertheless, data sales (or barter) is a lucrative market, albeit more difficult outside of the United States. *See, e.g.*, *id.* (interviewing Noreena Hertz, Rosabeth Moss Kanter, and Jeff Jonas).

51. *See generally* Johannes Deichmann et al., *Creating a Successful Internet of Things Data Marketplace*, MCKINSEY & COMPANY (Oct. 2016), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/creating-a-successful-internet-of-things-data-marketplace (describing monetization strategies for IoT data).

52. *See id*. Shelly Blake-Plock, *Where's the Value in Big Data?*, FORBES (Apr. 14, 2017, 8:00 AM), https://www.forbes.com/sites/forbestechcouncil/2017/04/14/wheres-the-value-in-big-data.

53. Deichmann et al., *supra* note 51.

data and for organizations purchasing or using data for targeted marketing activities.[54] While big data of this type could increase market share and improve product personalization, cross-platform or industry aggregation may also increase individual privacy risks.[55] Even if organizations pursue robust anonymization or de-identification programs, the more data collected, the more likely individuals could be re-identified and have their private, personal information exposed.[56] Indeed, data volume without additional IoT data already poses privacy issues for individuals: Acxiom alone has aggregated 3,000 data points per person.[57]

AI challenges previous conceptions of data collection and use by both requiring larger data volumes than ever before and by using data in new and unexpected ways, or "non-linear reasoning."[58] AI includes a wide variety of capabilities, from less advanced standard technology automation to fully functional robots and self-driving cars. Machine learning (ML), a concentration within AI, will enable manufacturers to fully analyze big data to identify trends and relationships between data points not previously anticipated by data scientists.[59] These trends inform complex algorithms used to advance any number of manufacturer goals, such as: increased use, optimal setting values, improved efficiencies, and which features to retire and which to add.[60] These insights can revolutionize not only IoT device functionality but can also provide a view into human behavior as a whole. This potential poses a dark side: unsupervised learning, or learning without human intervention and structure, could learn from data that codifies unfavorable or damaging social constructs (codified discrimination) or create its own discriminatory inferences (inferential discrimination).[61] When an AI utility creates an algo-

54. *Id.*

55. Joseph Jerome, *Big Data: Catalyst for a Privacy Conversation*, 48 IND. L. REV. 213, 213–17 (2014) (highlighting challenges in consumer autonomy for making decisions regarding how an individual's data is used).

56. *See id.*; Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 129–30 (2014).

57. *See* Vladeck, *supra* note 34, at 498–99.

58. *See* INFO. COMM'R'S OFFICE, BIG DATA, ARTIFICIAL INTELLIGENCE, MACHINE LEARNING AND DATA PROTECTION 6–7 (2017), https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

59. *See id*. at 6–8.

60. *See* ALPAYDIN, *supra* note 47, at 14–17; Allen, *supra* note 20.

61. *See* Alyx Baldwin, *The Hidden Dangers of AI for Queer and Trans People*, MODEL VIEW CULTURE (Apr. 25, 2016), https://modelviewculture.com/pieces/the-hidden-dangers-of-ai-for-queer-and-trans-people (describing how AI can be used to reinforce gender and racial biases, for example in neural technology and machine biases). Baldwin's article illustrates just one of many types of discriminatory application, which could be codified in automated systems using AI. *Id.* The Author proposes the two discrimination titles, codified discrimination and inferential discrimination, to delineate between direct discrimination resulting from sensitive personal information collection and discrimination resulting from proxies or other inferential automated decision-making.

rithm from existing data and executes the algorithm, it is possible AI will further marginalize protected classes or demographics.[62]

Cloud services, or shared technology resources usually maintained by a third party, have made it both convenient and cost-efficient for non-internet companies to manufacture IoT products.[63] Cloud services improve IoT device sales margins by reducing capital infrastructure investments: instead of operating a physical data center, manufacturers need only lease space at a cloud provider, which supports resource sharing across organizations and provides reliability and scalability at a low cost.[64] While financially desirable, cloud computing also may introduce cybersecurity issues.[65]

IoT technologies are built on continuously evolving technologies: big data, AI, and cloud computing. The presence of these technologies multiplies potential challenges for preventing discrimination, ensuring privacy, safeguarding individual safety, and protecting property by introducing advantages that simultaneously increase risk.

II. CONSUMER RISK AND REGULATION

IoT device consumers will likely benefit substantially from improved IoT services resulting from data fungibility, data commingling, data transfer flexibility, interoperability, and data exchange.[66] While IoT device consumers expect safe and reasonably fit goods, consumers also

---

62. *See id.*; *see* Stephen Gardner, *Artificial Intelligence Poses Data Privacy Challenges*, BLOOMBERG BNA (Oct. 26, 2016), https://www.bna.com/artificial-intelligence-poses-n57982079158.

63. Cloud services are collocated services that provide application functionality, such as an Interface or a mobile application, or services that simply store data to be used by IoT. Goran Čandrlić, *Cloud Computing—Types of Cloud*, GLOBALDOTS (Mar. 19, 2013), http://www.globaldots.com/cloud-computing-types-of-cloud. With collocation, organizations using cloud services benefit from shared facility costs (many organizations house data in one location, reducing cost for brick and mortar investments) and complementary resource use (some organizations have higher consumption at times, other organizations may have higher consumption at others; this balances resource consumption, reducing bandwidth needed for an individual organization). *See id.* Cloud services can include Infrastructure as a Service (IaaS), Software as a Service (SaaS), Platform as a Service (PaaS), or other support. *See id.*

64. KAI HWANG ET AL., DISTRIBUTED AND CLOUD COMPUTING 192 (2012).

65. Jaydip Sen, *Security and Privacy Issues in Cloud Computing* 7–8, 12–15 (2016) (conference paper), https://pdfs.semanticscholar.org/4dc3/70d253020947a8e66b701e12dd0233161229.pdf (describing the various cybersecurity concerns for cloud computing). Manufacturers must rely on cybersecurity measures cloud providers apply to protect consumers from cyberattacks that could compromise data confidentiality, integrity, or availability. *See id.* at 14–15. Specific issues include lack of encryption, which means data will be immediately readable upon compromise, and low-cost engagements usually involve collocation of data, meaning that in some cases access to one manufacturer's data set could result in access to all manufacturers' data stored by the cloud provider. *See Cloud-10 Multi Tenancy and Physical Security*, OWASP FOUND., https://www.owasp.org/index.php/Cloud-10_Multi_Tenancy_and_Physical_Security (last modified Aug. 30, 2010).

66. *See* WORLD ECON. FORUM & INSEAD, THE GLOBAL INFORMATION TECHNOLOGY REPORT 2014, 35–38 (Beñat Bilbao-Osorio et al. eds., 2014), http://www3.weforum.org/docs/WEF_GlobalInformationTechnology_Report_2014.pdf (describing the changing nature of data use and connectivity in IoT).

prefer low-cost, simple and usable goods.[67] The polarity of these forces creates a unique challenge for developing a market-friendly IoT legal framework.

IoT device infrastructure design will collide with traditional notions of privacy and emerging concerns for cybersecurity. Ubiquitous data collection, insufficient cybersecurity controls, and automated decision-making could compromise consumer privacy, physical safety, and property value.[68] Taken together, existing laws will not adequately protect consumers purchasing average household IoT products from potential risks.[69]

IoT implementations pose inherent consumer risks related to IoT functionality and architecture because they involve a front-end consumer manufactured device paired with big data collection infrastructure, decentralized data storage and transfer, and AI utilities. As originally introduced by Scott R. Peppet, at least four risks apply to IoT: discrimination, privacy, consent, and security.[70] Despite Peppet's prescient perspective in 2014, the scale and nature of these risks has changed and intensified amid technological paradigm shifts, creating a far greater need for a timely, effective legal framework.[71]

A. Large Data Stores Could Lead to Discriminatory Impact Through Codified and Inferential Discrimination

Discrimination could result from big data collection and analyses that codify historical and intentional discriminatory treatment or result in other disparate impacts on identified groups or individuals. Usually, discrimination is discussed in relation to web or app-based automated decision-making based on large, historical data stores, but discrimination is a real concern for IoT data use as well.[72] Solon Barocas and Andrew D.

---

67. Nicole Kobie, *The Internet of Things: Convenience at a Price*, GUARDIAN (Mar. 30, 2015, 11:32 AM), https://www.theguardian.com/technology/2015/mar/30/internet-of-things-convenience-price-privacy-security (reporting on the high cost of connected devices and potential privacy and cybersecurity issues). Consumer pressures for low-cost options in connected devices will make it appealing for manufacturers to strip out certain protection to maximize returns, especially where not mandated by law. *Id.*

68. *See infra* Sections II.A–II.D and accompanying notes. These combined risks must be evaluated within the context of IoT consumer devices and reviewed in light of existing or potential legal (or other) solutions.

69. *See infra* Sections II.A–II.D and accompanying notes. Statutes like the FDCA and FDA oversight may provide some level of enforcement for privacy and cybersecurity considerations for medical devices. *See infra* Section III.A. Likewise, COPPA could provide some level of enforcement, at least for privacy-related matters for children under thirteen years of age. *See infra* Section III.B.

70. *See generally* Peppet, *supra* note 56, at 117–45 (describing, in detail, each of these key challenges in IoT).

71. *See* Richard Tynan, *Why the Internet of Things Begs for a Paradigm Shift in Internet Security*, MEDIUM (Nov. 2, 2016), https://medium.com/privacy-international/why-the-internet-of-things-begs-for-a-paradigm-shift-in-internet-security-2287c3ecf802.

72. Scholars have associated discrimination with large data stores that either reinforce stereotypes or codify previous discrimination of protected classes and minorities. *See infra* notes 73–109

Selbst have explored how data mining might result in discriminatory disparate treatment and disparate impact.[73]

IoT devices could potentially codify disparate treatment and impact by incorporating algorithmic results into device functionality. Algorithms driving device functionality could include aggregation across multiple sources, increasing the likelihood for organizations to make decisions that reinforce discriminatory behavior.[74] Under some circumstances, automated decision-making may directly affect an individual's economic prospects: employment, housing, or credit worthiness.[75] Although most consumer IoT devices would be less likely to directly facilitate decisions affecting an individual's economic prospects, manufacturers could transfer IoT device data—seemingly innocuous data that could nevertheless serve as proxies for protected classes—to organizations who do make these decisions.[76]

Consumer IoT devices could lead to previously unanticipated discriminatory impact for an individual or group. For example, an individual using an IoT gaming device might receive different options than someone in a different demographic, based on seemingly innocuous data like home address, social-media relationship, music preferences, and so forth. Similarly, a "crime detection" device could encourage someone to avoid specific neighborhoods, impacting local businesses. These algorithms might not smack of overt discriminatory intent and disparate treatment, but the result is at a minimum ethically problematic or potentially evidence of disparate impact.[77]

It is not terribly difficult to anticipate that devices could indirectly imply people's race or national origin to define their interests or direct an individual to avoid an ethnically diverse neighborhood, depending on

---

and accompanying text. Usually, scholars discuss such discrimination from the perspective of significant life events and activities affecting an individual's economic choices (e.g., establishing a credit rating, receiving a loan, or qualifying for housing). *See infra* notes 73–109 and accompanying text.

73. *See* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 694–715 (2016). Barocas and Selbst fully illustrate the relationships between big data and potential discrimination. This Article aims to illustrate broad IoT challenges and therefore does not explore this concept in more depth.

74. *Id.* at 674; *see* Peppet, *supra* note 56, at 118–122; *see also* Max N. Helveston, *Consumer Protection in the Age of Big Data*, 93 WASH. U. L. REV. 859, 897 (2016). Although state statutes and regulations prevent state actors from discriminating based on certain types of sensitive data, big data could increase probability of these actions. *See* Barocas & Selbst, *supra* note 73, at 694–95. Because this data might lead to disparate impact but might not qualify as disparate treatment, it is questionable the degree to which these actions might lead to a determination that discrimination has occurred. *Id.*

75. *See supra* note 74.

76. An organization may not intend to collect data, which could be used for discriminatory purposes, with enough data points; however, it can be relatively easy to determine more sensitive or protected information about an individual and make automated decisions based on these proxies. *See infra* note 92; *see also* DINO PEDRESCHI ET AL., DISCRIMINATION-AWARE DATA MINING (2008), https://www.researchgate.net/publication/221654695_Discrimination-aware_data_mining.

77. *See* Barocas & Selbst, *supra* note 73, at 694–712 (contrasting disparate treatment and disparate impact in relation to data-mining activities); PEDRESCHI ET AL., *supra* note 76.

which data and rules the algorithm uses. These scenarios may be offensive and discriminatory, yet it is still unknown to what extent these types of scenarios trigger existing protections against discrimination under U.S. law. The General Data Protection Regulation (GDPR) in the EU has at least anticipated direct, economic, and moral types of potential discrimination.[78]

Research at the intersection of AI and big data has raised awareness to specific concerns regarding fairness, accountability, transparency, and ethics (FATE).[79] FATE research focuses on technological solutions for fair treatment of individuals or groups;[80] accountability of responsible parties; and transparency of information for individuals prior to, during, or after AI application or interaction.[81] Ryan Calo has identified the potential for discrimination in AI as "inequality in application," in which AI can result in disproportionate impact or discriminatory treatment of certain groups without human involvement.[82] Such application inequality may apply to circumstances that do not implicate legally recognized rights yet result in unfairness and disproportionate offerings to particular groups.[83]

Fairness, as a technical matter, poses certain challenges to implementing decision-making algorithms and AI utilities that form an IoT infrastructure. The process of actually removing potentially discriminatory data, or "regulating algorithms," appears to be a "non trivial task."[84]

---

78. Some discrimination does not fit the typical model. For example, an individual using an IoT device who is presented with certain gaming options because of an algorithmic calculation might receive different options than someone in a different neighborhood with different Facebook friends. In certain circumstances, it is not hard to anticipate that recommendations could be made that impliedly make assumptions about an individual's race or national origin to define these interests. The GDPR has at least anticipated direct, economic, and moral types of potential discrimination. The GDPR combines notice requirements, data subject rights, and use restrictions to achieve a reduced potential for discrimination: organizations must provide transparency via notice to the presence of automated decision-making and profiling activities, a data subject has a right to object to automated decision-making, and organizations cannot use certain categories of data for any purpose. The GDPR has no specific disclosure of specific algorithmic functionality that might compromise trade secrets, at least at the time of writing. *See* Regulation 2016/679, of the European Parliament and of the Council of Apr. 27, 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1, 40–42, 45–46 [hereinafter GDPR]. However, transparency under the GDPR still follows the traditional notice model, which is complicated by IoT technology. *See infra* Section II.B and accompanying notes.

79. *See FATE: Fairness, Accountability, Transparency, and Ethics in AI*, MICROSOFT, https://www.microsoft.com/en-us/research/group/fate (last visited Aug. 26, 2018).

80. *See infra* note 93.

81. *See* Bruno Lepri et al., *Fair, Transparent and Accountable Algorithmic Decision-Making Processes* (forthcoming) (manuscript at 2, 5, 8), http://www.nuriaoliver.com/papers/Philosophy_and_Technology_final.pdf (describing various studies to improve algorithmic fairness and proposing techniques to improve accountability and transparency).

82. Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. DAVIS L. REV. 399, 411–12 (2017).

83. *Id.* at 413 (describing circumstances involving "consequential decision-making," which presumably lead to greater risk to legal rights of individuals).

84. *See* PEDRESCHI ET AL., *supra* note 76.

From a data management perspective, discrimination falls into two categories: direct discrimination and indirect discrimination.[85] Direct discrimination explicitly places disproportionate discriminatory burdens on an individual, usually via direct or discoverable rules and specific discriminatory attributes that generate an outcome (e.g., burdens such as directly listing race or ethnic background and using this information as an input into an algorithmic decision).[86] Indirect discrimination includes nonspecific attributes that together result in an objectively discriminatory result or disproportionate burden on an individual.[87]

Direct discrimination usually results from collection and pervasive storage of sensitive personal information (SPI), which could lead to discrimination on the basis of health condition or sexual preference.[88] Direct discrimination would likely include collection of specific data categories. Therefore, regulating direct algorithmic discrimination could be as simple as establishing collection, use, and retention limitations, or barring data category inclusion in algorithms based on specifically defined "sensitive" or "potentially discriminatory" data categories, as many countries already established.[89] In data science, this concept is called "treatment parity," or noninclusion of specific data types to make a decision.[90]

Another version of direct discrimination involves use of a proxy for sensitive information prone to discriminatory use, or data collection that

---

85. *Id*. Direct discrimination is simultaneously easier to identify by examining algorithmic rules. In contrast, indirect discrimination requires more scrutiny, because indirect discrimination can result from proxies or combined data sets.

86. *Id.*

87. *Id.*

88. For this reason, the GDPR has similarly erected substantial limitations on sensitive personal information (SPI), or protected data categories by requiring strict use limitations and explicit consent from the data subject, and allowing for specific derogations (deviations) from the GDPR for complete bans on certain types of data collection at the member state level. *See* GDPR, *supra* note 78, at 38–39. For example, France could determine that a health condition, such as AIDS, cannot ever be collected and retained as a matter of course except in very limited circumstances, such as specifically for provisioning healthcare. *See id*. The GDPR would call sensitive personal information "special categories" meriting exceptional attention and restraint in terms of collection and transfer (requiring explicit consent). *See id.* For example, the GDPR permits individual member states to independently determine legal obligations for special category data transfer outside a particular country. *Id*. at 64–65. This has meant substantial restraint on data transfer in the form of data localization (prohibition) on special category data transfer for some countries or exceptionally robust conditions for doing so including, for example, additional administrative and technical cybersecurity measures. *See generally GDPR Local Implementation*, MORRISON FOERSTER, https://www.mofo.com/special-content/gdpr-readiness-center/gdpr-local-implementation.html (last updated Sept. 20, 2018).

89. *See* GDPR, *supra* note 78, at 1, 3, 5, 12, 14, 15, 19; *see generally* CHARLOTTE A. TSCHIDER, INTERNATIONAL CYBERSECURITY AND PRIVACY LAW IN PRACTICE (2018) (describing omnibus privacy laws, including Canada, Argentina, Uruguay, Japan, and the EU's GDPR, which collectively require special protection and limited collection for sensitive personal information).

90. *See* Pratik Gajane, *On Formalizing Fairness in Prediction with Machine Learning* tbl.1 (Research Paper) (2017), https://www.researchgate.net/publication/320297065._On_formalizing_fairness_in_prediction_with_machine_learning. Gajane further explains a proposed notion of fairness: "since individuals should not be held responsible for the attributes they can not change or had no say in, the social benefits they receive, which in turn affect their prospects in life, should not depend upon those attributes." *Id.*

can cumulatively identify sensitive information about an individual with high accuracy.[91] An individual who purchases diabetes test strips, low-glycemic crackers, an exercise mat, and a mobile diet macronutrient planning device *may* have Type II diabetes; however, this proxy is inferential rather than dispositive.[92] Although it is somewhat difficult to prevent the creation of proxies, data modeling may be able to identify proxy data sets in algorithms.[93]

Preventing truly indirect discrimination is substantially more challenging, especially with increased use of ML in data science, because it focuses on discriminatory outputs rather than discriminatory inputs, usually aimed at concepts of fairness.[94] Broader than antidiscrimination statutes and constitutional guarantees, the notion of fairness in ethics addresses concepts of equality that exceed what the law protects.[95] Goals to prevent indirect discrimination include "group fairness" and "individual fairness."[96]

Group fairness is statistical/demographic parity when different groups of individuals receive almost equal treatment; individual fairness means that similar people receive similar results.[97] In both cases, machine-created algorithms require rigorous testing, which is often human-supervised.[98] For this reason and due to the relative infancy of ML, it is tremendously difficult to develop technical standards and regulate organ-

---

91. *See, e.g.*, Michael McFarland, *Ethical Implications of Data Aggregation*, SANTA CLARA U. MARKKULA CTR. FOR APPLIED ETHICS (June 1, 2012), https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/ethical-implications-of-data-aggregation (describing the ability of large data sets to identify sensitive data, such as gender and sexual preference).

92. Because proxies are not exact representations of the actual data element they proxy, they can be prone to fairness issues both because they could be used for discriminatory purposes (disallowed for specific data elements) and they might lead to inaccurate inferences with little opportunity for awareness of decisions, objection to such decisions, or responsive action. In short, what is done is done, often without explanation. CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION 106–08 (2017). O'Neil describes *Griggs v. Duke Power Company*, 401 U.S. 424 (1971), which deemed intelligence tests discriminatory and illegal as an early precursor to the type of decisions we might anticipate. O'NEIL, *supra*, at 108.

93. Data used to proxy for SPI can even be determined from publicly available data. *See* CONSUMER FIN. PROT. BUREAU, USING PUBLICLY AVAILABLE INFORMATION TO PROXY FOR UNIDENTIFIED RACE AND ETHNICITY 1, 12 (2014), http://files.consumerfinance.gov/f/201409_cfpb_report_proxy-methodology.pdf. It should be noted that proxies can be used for positive actions to prevent discrimination (e.g., for fair lending analysis). *Id.* at 23.

94. Most existing concerns around proxy use include overt determination of proxy categories, which could emerge following fact-based determinations and expert evaluation. In short, proxies include human algorithmic creation, whereas ML utilities could derive unfair algorithms without human intervention that nevertheless result in disproportionate impact to a protected group.

95. Terry T. Ray, *Differentiating the Related Concepts of Ethics, Morality, Law, and Justice*, NEW DIRECTIONS FOR TEACHING & LEARNING, Summer 1996, at 47, 51 (distinguishing between what law establishes and what social goals prompt individual actors to do).

96. *See* Gajane, *supra* note 90.

97. *Id.*

98. *See* Barocas & Selbst, *supra* note 73, at 674. The Uniform Guidelines on Employment Selection Procedures published by the Equal Employment Opportunity Commission have developed validation standards to address correlative relationships between data collected and important elements of job performance. *See* 29 C.F.R. § 1607.4(D) (2018).

izations on the basis of indirect discrimination.[99] Legal responses to algorithmic decision-making should consider which fairness aspects the United States can and should reasonably regulate.

To address discrimination concerns, legal scholars have proposed responding to accountability and transparency with notice and procedural due process considerations.[100] Notice focuses on upfront education, facilitating consumer choice; procedural due process considerations contemplate interruption or responsive legal measures consistent with the Fourteenth Amendment.[101] If a consumer has fair warning of expected automated decision-making and the opportunity to decline or avoid these activities, less harm will likely result—assuming such warnings are effectively informational, accessible, usable, and the individual has an alternative option.[102]

Kate Crawford and Jason Schultz have proposed a corollary to responsive or interventional due process proceedings related to big data decisions.[103] This corollary involves technological due process for private entities modeled after Danielle Keats Citron's model for govern-

---

99. Indirect discrimination is based on results of analysis with regard to a single individual, or effects on that individual, rather than data already collected that directly identifies an individual as potentially subject to discrimination (i.e., legally protected statuses, such as gender, sexual preference, race or national origin, disability status, health status). *See* Michael Veale & Reuben Binns, *Fairer Machine Learning in the Real World: Mitigating Discrimination Without Collecting Sensitive Data*, BIG DATA & SOC'Y, July–Dec. 2017, at 1, 2. Indirect discrimination relies on extensive modeling, testing, and analysis, but often cannot exactly predict specific effects on an individual person, rather than effects on a particular group. *See* Barocas & Selbst, *supra* note 73, at 686. Although these processes can be developed, processes usually reflect the data set and may be different depending on what is collected. *Id.* at 675. For these reasons, it could be very difficult to directly regulate indirect discrimination via ML applications through statute. *See* Veale & Binns, *supra*, at 4–5; Jeremy Kun, *Big Data Algorithms Can Discriminate, and It's Not Clear What to Do About It*, CONVERSATION (Aug. 13, 2015, 1:56 AM), http://theconversation.com/big-data-algorithms-can-discriminate-and-its-not-clear-what-to-do-about-it-45849. Indirect discrimination may also be discussed as "bias," wherein results favor one individual over another.

100. *See infra* note 101.

101. The question of applicability of due process is a central question in relation to information, as the algorithmic decision-making about information has an impact on life, liberty, and property, but is not defined individually as any one of these. *See* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 110–11 (2014). Notice is not only an independent standard for data processing purposes and one of the FIPPs established by the Federal Trade Commission, the notice concept is also a preliminary step to ensure fundamental fairness via procedural due process. *See* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 27–28 (2014); *see also* FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 7–8 (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf (describing the FIPPs in detail). Certainly, the question of due process related to automated processing is an incredibly important topic, though one substantially more nebulous than can be sufficiently described here.

102. Alternative options are an important distinction because some automated decision-making could provide the only option for an individual. If someone declines, the individual could fall victim to a more damaging situation: lack of services. Under these circumstances, a greater risk of coercion results.

103. Crawford & Schultz, *supra* note 101, at 124–25; *see generally* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1249–50, 1304–05 (2008) (adapting procedural due process to circumstances involving automated decisioning technologies).

ment data use to address these issues.[104] Because due process proceedings require notice and an opportunity to be heard, which can be difficult and inefficient for organizations to facilitate, models incorporating due process activities usually focus on process-based activities.[105]

Citron has proposed an alternative model for meeting due process requirements in relation to big data use, including education related to biases and fallacies in big data algorithmic decision-making and a description, in detail, of reliance on automated decisions.[106] Crawford and Schultz advocate for notice and an opportunity to intervene, which could take a number of different forms.[107] One example is on-time notification when alternative big data sources have been used to make a decision about an individual (as in employment or housing).[108] This model has been, to some extent, replicated in the GDPR.[109]

B. IoT Device Architectures Reduce De-Identification Possibilities

Data identifiability is the main trigger for determining applicability of privacy laws, which restrict data collection, use, processing, transfer, and sales for particular markets.[110] IoT devices could generate many data types, including nonpersonal information, while privacy laws generally establish data-subject rights with respect to personal information and may also mandate protective measures.[111] Privacy laws protect specifically defined personal information types because their misuse or unauthorized disclosure could result in inherent injury to the individual (the data subject).[112] U.S. privacy laws directly protect electronic Protected Health Information (ePHI), children's information in online environments, nonpublic financial data, genetic data, medical data, and U.S. resident data used by government, amongst others.[113] Some laws additionally require organizations to minimize injury through breach notification.[114]

---

104. Crawford & Schultz, *supra* note 101, at 121–22; *see also* Citron, *supra* note 103, at 1251–58.

105. *See* Crawford & Schultz, *supra* note 101, at 123.

106. *Id.* In traditional computing contexts, Citron's recommended path would likely improve overall big data fairness, especially communicating reliance on algorithmic decision-making.

107. *Id.* at 125–26. Scholars have proposed algorithmic transparency as one model for improving transparency.

108. *Id.* at 126.

109. *See infra* Section III.F and accompanying notes.

110. *See* Crawford & Schultz, *supra* note 101, at 106–07.

111. *See id.*

112. *See id.*

113. *See generally* Charlotte A. Tschider, *Experimenting with Privacy: Driving Efficiency Through a State-Informed Federal Data Breach Notification and Data Protection Law*, 18 TUL. J. TECH. & INTELL. PROP. 45, 52–53, 63 (2015) (describing an empirical analysis of all state data breach notification laws).

114. *See* Hilary G. Buttrick et al., *The Skeleton of a Data Breach: The Ethical and Legal Concerns*, 23 RICH. J.L. & TECH. 2, 11–14 (2016).

Practices reducing the risk of identification or re-identification improve flexibility of data transfer to third parties and dynamic data usage.[115] These techniques involve a combination of removing data elements, segregating data, and using cybersecurity technologies to render data unreadable. Limited data sets reduce the number of data elements to only those strictly necessary for specified purposes, while de-identification procedures remove specific data elements to reduce data-subject risk to a level highly unlikely to result in data-subject injury.[116]

Anonymization procedures strip primary (independently identifiable) and secondary identifiers (potentially identifying a data subject when used in combination with other identifiers) to render re-identification *impossible*, also making data usage less practical.[117] Differential privacy procedures add statistical white noise to large data sets to obscure relationships between data elements and data subjects.[118] Data scientists created differential privacy to maximize data retention while simultaneously making it highly difficult, if not impossible, to identify an individual data subject from a data set.[119] Any and all of these practices would reduce potential privacy risks and likely some cybersecurity risks.

Data protection procedures also reduce identifiability risk. Data segregation involves bifurcation of primary identifiers from secondary identifiers using a common key, a linkage key.[120] This common key may be a pseudonym, or a unique identifier that is not derived from personal information.[121] Obfuscation and encryption techniques render data less accessible.[122] Obfuscation involves techniques like masking, which obscures all or parts of data elements to reduce visibility (e.g., covering all but the last four digits of a social cybersecurity number with an "X").[123] Organizations apply masking depending on the data use, which means some individuals at an organization may see the full number, while oth-

115. The identifiability of data related to an individual natural person (data subject) drives downstream restrictions in data fungibility overall, limiting an organization's ability to use, process, transfer, or sell data for its own purposes and benefit. With less identifiable or de-identified data, organizational obligations involving the data subject will be comparatively reduced while simultaneously reducing risk to natural persons.

116. *See* TSCHIDER, *supra* note 89, at 228.

117. *Id.* at 229.

118. *Id.* at 229–30.

119. *Id.*

120. DANIEL C. BARTH-JONES, UNDERSTANDING DE-IDENTIFICATION, LIMITED DATA SETS, ENCRYPTION AND DATA MASKING UNDER HIPAA/HITECH 8 (2011), http://www.ehcca.com/presentations/HIPAA19/barth_2.pdf.

121. Dale McDiarmid et al., *Protecting GDPR Personal Data with Pseudonymization*, ELASTIC (Mar. 27, 2018), https://www.elastic.co/blog/gdpr-personal-data-pseudonymization-part-1.

122. Omer Ramić, *Encryption vs Encoding vs Hashing vs Obfuscation*, RAMIĆOMER (Nov. 19, 2016), https://www.ramicomer.com/en/blog/differences-encryption-vs-encoding-vs-hashing-vs-obfuscation.

123. *See* TSCHIDER, *supra* note 89, at 227.

ers may see the masked version. In contrast, redaction removes or completely covers data to make it permanently or partially unreadable.[124]

Encryption is a commonly used technical method for making data inaccessible.[125] Encryption does not directly reduce identifiability in a permanent way but rather renders data unreadable when accessed by an unauthorized user.[126] Encryption protocols vary tremendously, depending both on the application (for data in transmission or data in storage) and the methodology to render data unreadable.[127] Some protocols have been exploited and are easily broken, while others would require hundreds of years to break the encryption key.[128]

The less identifiable or accessible a particular data set, generally the less likely privacy injury will result.[129] Laws like the Health Insurance Portability and Accountability Act (HIPAA) establish encryption "safe harbors" for data set treatment, which reduce organizational obligations when organizations reduce data subject risk.[130] Reduced risk to a data subject loosens data usage restrictions, enabling subsequent market benefit.[131] The HIPAA de-identification safe harbor permits an organization to remove specified identifiers to defensibly have de-identified PHI, or a manufacturer to procure an expert determination of very low risk to data subjects.[132]

IoT device infrastructures present challenges to de-identification, especially due to big data collection schemas and AI utilities.[133] Consider the following example:

> An IoT wearable day planner makes recommendations based on pre-recorded daily activities. The IoT device syncs with the user's mobile device, which contains fitness and dietary data, as well as calendar

---

124. *See id.*

125. Carey Wodehouse, *Encryption Basics: How It Works & Why You Need It*, UPWORK (Aug. 10, 2016), https://www.upwork.com/hiring/development/introduction-to-encryption-data-security.

126. *Id.*

127. *Id.*

128. *Id.*

129. *See* BARTH-JONES, *supra* note 120, at 3. Barth-Jones describes the various models in relation to HIPAA-established risk (from least risk to most): no information, de-identified data, breach safe data, limited data set, and fully identified. *Id.*

130. *Id.* at 4–6. Both lack of information and too much information can lead to risk or efficacy issues. While de-identification is a worthy goal in many cases, sometimes identifiability is critically important, for example when provisioning health services.

131. *See, e.g.*, U.S. Dep't of Health & Human Servs., *Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (content last reviewed Nov. 6, 2015) (describing methods for reducing identification risk for individuals with two methods: a safe harbor and an expert determination, based on risk to the individual).

132. *See* BARTH-JONES, *supra* note 120, at 5–7. Barth-Jones criticizes the use of a de-identification safe harbor, as it does not work well with large and complex data sets and for adequate software and system testing. *See id.* at 5.

133. *See* Manon Oostveen, *Identifiability and the Applicability of Data Protection to Big Data*, 6 INT'L DATA PRIVACY L. 299, 302 (2016).

> information and connectivity with social media apps and e-mail. The day planner works most effectively by collecting as many data points as possible, from various data sources, and combining these data to generate complex algorithms that identify the optimal activity for a particular time. The wearable day planner could remind a user to eat at an optimal time, schedule exercise, or determine the most effective meditation time.

In this example, data will both be generated by the device as the user interacts with it and transferred to backend systems, which take data from other applications and potentially public data sources, then compare data against other users' data sets to optimize an individual user's daily activities. The larger the data set, the more likely a data subject will be identified, yet modern IoT maximizes data collection to improve functionality and effectiveness.[134]

IoT devices create unique types of personal information, such as sensor data produced through IoT device use.[135] Because these data elements relate specifically to individual device use, data may be identifiable to some extent, yet present less privacy risk to an individual than typical personal information collection due to location tracking or home activity, amongst other data elements not previously collected and retained.[136] Sensor data will likely be considered difficult to de-identify because sensor data concerns an individual's daily activities or location.[137] Objectively, these data would not likely pose the same privacy risks as highly identifiable information or SPI, which is more likely to adversely affect individuals by increasing the potential of unauthorized access and identity theft.[138]

Historically, the concept of identifiability has been the *sine qua non* for privacy protection: if a data set is rendered nonidentifiable or does not match definitions of personal information, privacy laws do not apply.[139] Risk-mitigating approaches similarly emerged to balance market

---

134. *Id.* at 302.

135. *See* Peppet, *supra* note 56, at 90, 94, 143.

136. *See* OFFICE OF PRIVACY COMM'R OF CAN., THE INTERNET OF THINGS: AN INTRODUCTION TO PRIVACY ISSUES WITH A FOCUS ON THE RETAIL AND HOME ENVIRONMENTS 2, 8–11, 16–18 (2016), https://www.priv.gc.ca/media/1808/iot_201602_e.pdf.

137. *See* Peppet, *supra* note 56. HIPAA was likely the first law to connect removal of data elements with mathematical probability of privacy risk to an individual. Since that time, new models for de-identification have been developed, specifically for use with data sets similar to IoT. The Author should mention that since Peppet's article was published, some specific advancements have been made in de-identification procedures, for example the widely publicized differential privacy approach, which would apply to these types of problems. *See, e.g.*, Andy Greenberg, *Apple's 'Differential Privacy' Is About Collecting Your Data—But Not* Your *Data*, WIRED (June 13, 2016, 7:02 PM), https://www.wired.com/2016/06/apples-differential-privacy-collecting-data. Differential privacy was originally created in 2006, s*ee* Michael Hilton, *Differential Privacy: A Historical Survey*, U. KY. C. ENGINEERING, http://www.cs.uky.edu/~jzhang/CS689/PPDM-differential.pdf (last visited Oct. 1, 2018), but only recently has found high-profile use, as with Apple Computers. *See* Greenberg, *supra*.

138. *See* Peppet, *supra* note 56.

139. *See* Crawford & Schultz, *supra* note 101, at 98–101.

access to personal information with reduced risk to individuals, such as the limited data set under HIPAA, which encourages Covered Entities (CEs) and Business Associates (BAs) to reduce the volume of identifiable elements collected and retained.[140] Scholars such as Daniel Solove have proposed mid-level data classification, or data types that could exist between the dichotomy of personally identifiable information (meriting full-scale protection) and nonidentifiable information (afforded no protection) for purposes of balancing legitimate data needs and consumer protection.[141]

IoT devices will likely create data types that are much broader and multidimensional than previously conceived, prompting the question of whether any IoT data can truly be nonidentifiable or whether IoT data should adopt a mid-identifiability classification.[142] IoT data would likely include secondary identifiers, or "quasi-identifiers," data that indirectly identifies a data subject, yet in aggregate could prove identifiable.[143] Privacy risk-reduction models, or Privacy Enhancing Technologies (PET)—including de-identification, limited data sets, and pseudonymization—focus on reducing or obscuring primary identifiers or connectivity between primary and secondary identifiers, reducing the potential for misuse or unauthorized access in traditional privacy contexts.[144] However, these risk-reduction methods would not necessarily address identifiability issues for big data sets, which despite integrating some PET, could nevertheless reidentify an individual, making anonymization nearly impossible.[145] The use of big data infrastructures for IoT may create new data insights that could identify an individual or produce reasonably accurate SPI, which are then used for automated decision-making.

When an organization creates a big data set from collected data, public data sources, data exchanges, or simply stores substantial data sets, the insights an organization can identify could constitute even more sensitive data than what the organization directly solicits.[146] Large data

140. The limited data set has not proved effective, as HIPAA does not provide any incentives for reducing identifiability overall, such as increased fungibility, transfer, or sales. The dichotomy between identifiable and non-identifiable data enshrined in the law has therefore prevented substantially more flexibility and less identifiable data sets, and could have actually resulted in higher volumes of aggregated identifiable data.

141. *See* Peppet, *supra* note 56, at 132 (citing Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1877 (2011)). Mid-level data classifications would allow for substantially more flexibility under privacy laws. *See* Schwartz & Solove, *supra*, at 1886, 1894. However, reduced obligations for mid-level data classifications might not transfer to other types of obligations regarding discriminatory data use or cybersecurity measures. *See id.* at 1884–85.

142. *See* Peppet, *supra* note 56, at 131–32.

143. *See* BARTH-JONES, *supra* note 120, at 10.

144. *See generally* Johannes Heurix et al., *A Taxonomy for Privacy Enhancing Technologies*, COMPUTERS & SECURITY, Sept. 2015, at 2–3 (2015) (describing available PET that can reduce risk to individual privacy).

145. Frank Buytendijk & Jay Heiser, *Confronting the Privacy and Ethical Risks of Big Data*, FIN. TIMES (Sept. 24, 2013), https://www.ft.com/content/105e30a4-2549-11e3-b349-00144feab7de.

146. Crawford & Schultz, *supra* note 101, at 98–99.

sets have already been collected through traditional data analytics, which have begun identifying sensitive characteristics with reasonably high accuracy.[147] In a notable example, Target Corporation was able to predict that a woman was pregnant from buying habits alone, without directly collecting data about her pregnancy.[148]

Data may be collected or it may be bought. Many organizations, including manufacturers that lack historical data or are unable to aggregate big data sources on their own, will purchase data sets from IBM, Cisco, or other prominent analytics companies to enhance data sets for big data solutions or to seed ML training.[149] These data sources could increase the probability of identification by increasing the number of data points available, even if purchased data is publicly available.[150] Further, the ability of internet-enabled technologies to identify, match, and recombine data sets has also reduced data obscurity for public but hard to find information, increasing the potential for new insights as well as individual harms.[151] Data element-oriented concepts of reduced identifiability via data classification will not likely solve privacy risks presented by IoT infrastructures.

The contents of data sets might also present substantial IoT safety issues apart from privacy concerns.[152] IoT data elements have broader utility and introduce higher attendant risks than traditional notions of personal information: IoT systems transmit data back and forth between large databases and devices, delivering instructions and facilitating services to IoT devices.[153] If attackers compromise IoT data, data subjects not only suffer potential privacy injury but also experience physical injury, property damage, or other service unavailability due to unauthorized data change (data-integrity issues) or service interruption (data-availability issues).[154] Reduced identifiability does not necessarily address substantial safety risks to data subjects using IoT devices.[155]

---

147. Arvind Narayanan et al., *A Precautionary Approach to Big Data Privacy*, *in* DATA PROTECTION ON THE MOVE 357, 365, 368–69 (Serge Gutwirth et al. eds., 2016).

148. Crawford & Schultz, *supra* note 101, at 98.

149. *See* Helveston, *supra* note 74, at 870.

150. *See id.*

151. *See* Woodrow Hartzog & Evan Selinger, *Big Data in Small Hands*, 66 STAN. L. REV. ONLINE 81, 83 (2013). Big data have the potential to collectively identify more sensitive insights that, in turn, lead to more sensitive disclosures.

152. *See infra* Sections II.D, III.A and accompanying notes (describing issues directly related to cybersecurity).

153. Consider a traditional IoT implementation, which involves backend, near real-time data aggregation and analysis: systems work better when additional data can inform device functionality and systems work more effectively with very large volumes of data. The larger the volume of data in a data set about an individual, the more identifiable a data set potentially could be. *See* Buytendijk & Heiser, *supra* note 145.

154. *See infra* Section II.D and accompanying notes.

155. *See infra* Section II.D and accompanying notes.

C. IoT Devices Frustrate the Purpose of Traditional Notice and Consent

As a cornerstone of privacy, notice and consent proceduralize individual choice.[156] In relation to notice and consent, Peppet notes the difficulty of managing this historical privacy construct, wherein manufacturers must facilitate consent through indirect and inefficient means.[157] When manufacturers rely on a screen and consent (such as clicking a check box), it is typically found on a website or web application because space and functionality limitations on the device itself render privacy notice display impossible.[158] Most manufacturers that do provide a privacy notice defer to outdated, inaccurate, misleading, or difficult-to-locate privacy notices on a website,[159] rather than privacy terms included within the device's packaging or contextual notice on the device itself.[160] Manufacturers may also require connectivity to a mobile device to agree to privacy notice terms, especially where IoT device settings can be controlled by a mobile device.

Despite challenges regarding delivery of a privacy notice and definitions of personal information, an additional challenge for notice includes questions of individual agency and actual choice, rather than objectively constructed choice. IoT devices disrupt the historical informed consent model, which includes notice temporally followed by consent, a fixed model that may be ill-suited for dynamic engagement.[161] Dynamic engagement models usually involve data collection, use, and algorithmic decision-making change based on an aggregate of data collected, which informs algorithms and, subsequently, new product feature deployment.[162] A traditional model of prior notice followed by consent is not

---

156. Notice and consent is used as a mechanism to shortcut more comprehensive investigations into fairness and bargaining power: "consent legitimizes nearly any form of collection, use, or disclosure of personal data." Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1880 (2013).

157. *See* Peppet, *supra* note 56, at 139.

158. *Id.* at 140–42.

159. *Id.* at 141–43.

160. *Id.* at 140–41. Peppet conducted a survey of devices and found that none included privacy information in the box, though some depended on connectivity with a mobile app, which would allow for display of a privacy notice there. *Id.* In practice, however, most of these interfaces made it tremendously difficult to locate a privacy notice, and when located many only referenced the website, not the device or data use terms. *Id.* Whether IoT devices create "personal information" also informs how an organization can use data, including data sales or transfer to third parties, and whether individuals own the data. *See id.* at 142–43. Privacy notices do not seem to address these questions, which could mean that manufacturers do not associate IoT device data as being personal information. *See id.*

161. *See* Thierer, *supra* note 14, at 79–81. Thierer describes the Obama Administration's consideration of notice and consent as complicated by wearable devices and modern mobile technologies and quotes Scott R. Peppet: "sensor-device firms seem stuck in a notice paradigm designed for web sites rather than connected consumer goods." *Id.* (quoting Peppet, *supra* note 56, at 148).

162. *Id.* AI-enabled devices rely on AI utilities that are not designed by humans and that benefit from big data. The beauty of AI utilities is that they find complex relationships amongst data sets, including data elements that may seem trivial or unnecessary. For this reason, it is tremendously difficult to inform individuals prior to data collection how their data will be used within a given system.

compatible with real-time improvements precipitated by the "always-on" nature of pervasively connected devices, often resulting in user fatigue.[163] Manufacturers and consumers might be caught in a continuous loop of notice followed by consent, followed by a material system change and new notice followed by new consent, *ad infinitum*: high-change frequency would likely result in continuous notice deployment and subsequent consent demands on product users.[164]

Some devices may be designed as stand-alone units that "plug and play," which automatically turn on, connect to an available wireless network, and begin receiving and transmitting data.[165] Once connected, these devices may include periodic feature or functionality changes, including additional data solicitation (connect with other devices) or auto collection of new data. How IoT data is processed, secured, or analyzed might differ tremendously from day to day precisely because connected devices benefit from continuous activity and pervasive internet connectivity. Presumably IoT devices will provide relevant, useful services and new insights to drive those services based on continuous change.[166] Assuming manufacturers provide accurate, available, and contextual privacy notices for an individual's consent, a question remains: Must manufacturers recycle this same process every time data use and functionality changes?

Traditional privacy models usually require an individual to complete any applicable privacy notice and consent process again following any material changes.[167] This model, applied to IoT, likely would create efficiency and reasonableness concerns when users must review the notice to protect their own privacy interests. Because IoT devices depend on broad data-element collection and alternative data sources to inform

---

163. *See* Article 29 Data Protection Working Party, *Guidelines on Consent Under Regulation 2016/679*, at 17, WP259 (Nov. 17, 2017), https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2017/12/guidelines-on-ADM-and-Profiling.pdf.

164. It is not hard to imagine circumstances where every time new data are collected or data use changes, which might be increasingly frequent with the responsive IoT environment, communication of the user is required. With high frequency of this communication, it is increasingly likely that individuals will pay less attention to notice contents, a type of notice fatigue.

165. *See, e.g.*, *Smart Devices*, WAVIOT, https://waviot.com/products/smart-devices (last visited Oct. 7, 2018) (describing "plug-and-play" home devices for smart meters and other industrial IoT applications). Increasing concern has emerged for plug-and-play children's toys and other devices where cybersecurity is not configured appropriately. *See* VIPRE Security, *FBI Issues Security Warning About Internet of Things Toys*, VIPRE (July 23, 2017), https://www.vipre.com/blog/fbi-issues-security-warning-internet-things-toys.

166. *See* Guido Noto La Diega & Ian Walden, *Contracting for the 'Internet of Things': Looking into the Nest*, 7 EUR. J. L. & TECH., no. 2, 2016, at 1, 3. Noto La Diega and Walden raise this issue with respect to other contract terms applicable in IoT outside privacy and cybersecurity, as typically communicated in terms of use and other product disclosures. *See id.*

167. *See, e.g.*, Press Release, FTC, Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep (illustrating the FTC's practice of alleging unfair or deceptive trade practices for failing to change a privacy policy although data uses change).

algorithms and improve ML accuracy, manufacturers may struggle to notify data subjects in a manner that definitively appraises individuals of expected data-processing activities.[168] It may also be difficult to adhere to data-minimization principles when data maximization stands to improve service offerings.[169]

In deferring to a formalistic, linear privacy notice and consent model, three untenable IoT expectations emerge, or the "consent myth": (1) individuals have meaningful choice with respect to the privacy notice, (2) an individual reasonably should and can invest time in reviewing a privacy notice as part of a contractual bargain, and (3) individuals can understand what privacy notices mean in terms of real-life impact.[170]

Traditional privacy models may have been historically reasonable, for example paper-based engagement models and reasonably static web pages. However, IoT device data management models and functionality challenge a traditional notice and consent model. First, for relatively inexpensive devices, it may be unreasonable to expect an individual to locate and read a privacy notice—especially when not displayed within the product itself at the point of use—simply to protect information produced by the individual.[171] Indeed, a 2011 survey illustrated that only 7%

168. *See* Jedidiah Bracy, *On Building Consumer-Friendly Privacy Notices for the IoT*, IAPP (Nov. 6, 2015), https://iapp.org/news/a/on-building-consumer-friendly-privacy-notices-for-the-iot.

169. *See* Christopher Mims, *Size Matters: Why the Only Thing Better than Big Data Is Bigger Data*, QUARTZ (Feb. 3, 2014), https://qz.com/169206/why-the-only-thing-better-than-big-data-is-bigger-data.

170. Traditional models of notice and consent require "informed consent," which is intended to provide a procedural mechanism for ensuring individuals have an opportunity to read and refuse to consent, if so desired. *See* Chunlin Leonhard, *The Unbearable Lightness of Consent in Contract Law*, 63 CASE W. RES. L. REV. 57, 67 (2012). However, this traditional, linear model presupposes that an individual has a choice, rather than a contract of adhesion. *See, e.g.*, Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?* 111 PENN ST. L. REV. 587, 617–19 (2007) (describing how privacy policies may indicate lack of mutual assent when consent is not provided; other circumstances may indicate unconscionability). The FTC has not proposed a solution, but commissioners, such as Commissioner Ramirez, had previously noted the difficulty associated with providing notice and consent for technologies where there are "practical obstacles." *See* Thierer, *supra* note 14, at 77–78 (quoting FTC Chairwoman Edith Ramirez). It is unlikely that an average time commitment of forty minutes a day, every day, is a reasonably efficient time investment that would lead to a more productive marketplace. *See* Shankar Vedantam, *Do You Read Terms of Service Contracts? Not Many Do, Research Shows*, NPR (Aug. 23, 2016), https://www.npr.org/2016/08/23/491024846/do-you-read-terms-of-service-contracts-not-many-do-research-shows. Indeed, an opportunity to read paired with consent constructively illustrates informed consent, which is a historically preferred model. *See* Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy Norms, and Consent*, 14 J. HIGH TECH. L. 370, 379–81 (2014). Privacy notices, even when written at an acceptable reading level, often include abstract concepts that make it difficult for an individual to understand long-term impacts that would facilitate actual, rather than constructive, choice. *See id.* at 379–81, 391–93.

171. It is probably reasonable to expect a duty to read reasonably proportionate to the product value and potential risk. For example, a mortgage document might merit more thorough review than a privacy notice for a connected hair brush. The point of use or the point of registration is typically the moment where a manufacturer or developer displays a privacy notice, as the notice serves as a gatekeeping mechanism preventing data collection and processing prior to the user's consent. Unlike Terms of Use, which may be shrink-wrapped, the requirement of explicit consent under some privacy laws, at least for more sensitive data collection, requires a non-shrink-wrapped model for notice display. *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15

of Britons read the full terms when buying a product or service online.[172] A 2015 survey found that 30% of people never read social networking terms, with an additional 50% only reading them "sometimes."[173]

An experiment conducted by Jonathan Obar illustrated that it would take an additional forty minutes every day of the week to read all of the privacy and service terms encountered, and when actually tested on terms, 98% of study participants would have agreed to share personal information with the National Security Agency and give up their first-born child.[174] Another study resulted in over twenty-two thousand users over two weeks unknowingly agreeing to clean port-a-potties for free wireless internet access, while only .000045% of users spotted the clause.[175] These studies suggest that under most circumstances, traditional notions of prior notice and informed consent do not actually result in notice or informed consent.[176] Presumably, terms of use and privacy notices might be more effective in some contexts, and it would be unwise to reinvest in ineffective notice and consent models, given additional IoT design constraints and data use challenges.

When individuals do read a privacy notice, questions remain as to whether an individual not only can *functionally* read the notice but also whether an individual *reasonably ascertains* actual downstream impacts related to data use.[177] California's Online Privacy Protection Act of 2003 (CalOPPA) established privacy notice requirements most U.S.-based organizations follow as the most restrictive and prescriptive standard

---

U.S.C. § 7704(a)(5)(A)(ii) (2018). Under U.S. law, less sensitive data might benefit from shrink-wrapped communication, in the form of an opt-out consent model wherein an individual transmits data until she decides to revoke consent by opting out of further data processing. CAN-SPAM follows a similar consent model for marketing e-mail communications. *See id.* § 7704(a)(4)–(5).

172. Rebecca Smithers, *Terms and Conditions: Not Reading the Small Print Can Mean Big Problems*, GUARDIAN (May 11, 2011, 2:00 AM), https://www.theguardian.com/money/2011/may/11/terms-conditions-small-print-big-problems.

173. Kimberlee Morrison, *Survey: Many Users Never Read Social Networking Terms of Service Agreements*, ADWEEK (May 27, 2015), http://www.adweek.com/digital/survey-many-users-never-read-social-networking-terms-of-service-agreements.

174. Vedantam, *supra* note 170.

175. Rebecca Wilkin, *Thousands Obliviously Agree to Clean Port-a-Potties for Free Wi-Fi*, N.Y. POST (July 17, 2017, 3:32 PM), https://nypost.com/2017/07/17/thousands-obliviously-agree-to-clean-port-a-potties-for-free-wi-fi.

176. Presumably individuals acting in their own interests outside of a study might exhibit more care in agreeing to terms; however, these studies suggest that individuals likely do not have the time or expect some implicit reasonableness in the terms. *See* Vedantam, *supra* note 170. Alternatively, it is possible individuals simply do not care what happens with their data, but other studies seem to dispel this argument. For example, 93% of adults want to control who can get information about them and 90% of adults want to control the type of information shared. *See* Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RES. CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance. It appears that individuals do care about privacy, just not about quasi-contractual forms.

177. *See* Sloan & Warner, *supra* note 170, at 380–81, 405. Although an "opportunity to read" approach to privacy notice and consent has long served, the Author notes that privacy concepts specific to data collection, management, and transfer are highly abstract concepts that even privacy scholars struggle to understand at times. It is not a foregone conclusion that well-written privacy notices help individuals understand real impacts to them.

today.[178] CalOPPA requires organizations to include a description of personal information collected (broadly defined under California law) and display the notice in a clear and conspicuous location on the organization's website.[179] However, CalOPPA does not require disclosure of potential risk to an individual, the volume of data collected, whether data might be commingled with other identifiable data sources, algorithms or AI utilities used, or if the data could be transferred to partners or affiliates for their use—typical data-management practices in IoT.[180] If the privacy notice is the preferred communication mechanism to appropriately put an individual on notice, actual notice (or verifiable evidence of notice actually being displayed prior to proceeding/consenting) is conspicuously absent from existing privacy-notice requirements.[181]

If an individual does read a privacy notice or terms of use and can accurately understand its impact, a question remains as to whether the individual truly has meaningful choice. Privacy notices are usually defined as a type of "quasi-contract," where despite applying contract principles where both parties perform as if a contract is in place, true offer and acceptance often does not usually factually occur.[182] Privacy notices often receive this categorization because in many cases one party does not consent.[183] Rather, consumers object by not purchasing the product, a typical adhesive contract.[184] The question remains whether having only one choice, "take it or leave it," as is typical in adhesive contracting, sufficiently ensures individual choice with respect to IoT data and potential risks.[185]

Where U.S. privacy laws apply, they generally restrict data uses to those disclosed in the privacy notice or additional authorizations for limited organizations and data types. Under HIPAA, CEs or BAs collecting or processing electronic ePHI must receive explicit authorization for

178. *See* CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2018).
179. *Id.*
180. *Id.*
181. *See id.*
182. Timothy J. Sullivan, *The Concept of Benefit in the Law of Quasi-Contract*, 64 GEO. L.J. 1, 2–5 (1975). Quasi-contracts are often resolved as contractual relationships for equitable purposes. *Id.*
183. *See* Sloan & Warner, *supra* note 170, at 381–82, 400–01.
184. *See* Haynes, *supra* note 170, at 619–20.
185. *See id.* Certainly, it is possible to envision circumstances wherein there are limited options for IoT, or where multiple options do not leave an individual with alternative market options, while under some circumstances, adhesive contracting could benefit the individual when limited information, needed for device operation, is processed. In other circumstances, adhesive contracting could result in broad-scale data processing for reasons unrelated to device purchase. The degree of coercive practices for consumer IoT devices might appear negligible when considering a connected device with an available analog equivalent (a connected hair brush or a traditional hair brush), but at some point in time consumer products may no longer be available in analog (e.g., only connected thermostats are available and may be a required purchase by electrical companies for service operation). The lack of contractual commitment to continue service for these digital devices may also result in less useful devices, as new devices must be purchased to continue service. *See* Woodrow Hartzog & Evan Selinger, *The Internet of Heirlooms and Disposable Things*, 17 N.C. J. L. & TECH. 581, 584 (2016).

processing purposes outside the Notice of Privacy Practices displayed at the time of treatment and for additional unrelated purposes.[186] The net effect of such restriction is that downstream data use is curtailed by the requirement to return to a patient and receive additional consent.[187]

The Gramm-Leach Bliley Act (GLBA), applicable to financial institutions, requires consumer notice followed by an opportunity to object for Non-Public Information (NPI) data sharing beyond that specified under GLBA, which permits third-party data sharing under limited circumstances.[188] The Children's Online Privacy Protection Act (COPPA), enforced by the Federal Trade Commission (FTC), also requires disclosure to parents of planned uses for the data of children under the age of thirteen prior to soliciting consent.[189] For other data collection, the FTC established the Fair Information Practice Principles (FIPPs), which position notice and consent as two distinct, though connected, principles.[190] For consent to be valid, a consumer should be informed prior to consenting (prior notice), whether such consent is implied (opt out) or expressed.[191]

The inability to predict potential identifying data elements also complicates the concept of notice and consent. Big data algorithms will likely categorize and attach new personal identifiers through data-mining activities, which frustrates the purpose of notice and consent: organizations cannot anticipate downstream data insights at the time of providing notice.[192] ML utilities running on big data sets increase the probability of data creation by identifying new connections between data that are not predictably related or reasonably foreseeable by either the consumer or the manufacturer.[193] In a traditional privacy notice and consent model, these two natural results of IoT functionality run afoul of transparency and choice principles: if organizations cannot reasonably anticipate potential uses at the time of providing notice, they risk providing inaccurate

186. HIPAA requires annual display of a Notice of Privacy Practices (or when material changes are made), but does not specifically require consent, although state medical laws may require consent. *See* 45 C.F.R. § 164.520 (2018). Authorization is required when using data for purposes not specific to treatment, payment, or healthcare operations. *See id.* § 164.508. Consent is required in the form of specific authorization that notates specific data type, data uses, an expiration date, party to which disclosure will be made, and right to revoke authorization. *See id.*

187. HIPAA requires specific authorization for uses outside the Notice of Privacy Practices and GLBA provides opt-out rights for marketing activities. *See id.* § 164.508. Logically, when an organization must continue to return to a patient and receive new authorization, there is likely to be a chilling effect on data collection and further processing. Further, because HIPAA applies to CEs and BAs, specifically demarcated market roles, *see id.* § 164.104, many manufacturers will not need to meet these requirements.

188. *See* 15 U.S.C. § 6802 (2018).

189. The Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2018).

190. FTC, *supra* note 101, at 7–8.

191. *Id.* at 8–9.

192. *See* Crawford & Schultz, *supra* note 101, at 108.

193. *See supra* Section II.B and accompanying notes.

or misleading information to consumers, potentially risking an FTC Section 5 unfair-or-deceptive-practices administrative action.[194]

Adam Thierer has described an alternative to the traditional notice and consent model, the "responsible use" model,[195] a transparency approach that gained popularity with President Barack Obama's Big Data Commission in 2014.[196] The concept of responsible use focuses on controlling data at the moment when potential injury could occur: when it is used.[197] This approach, in part championed by Fred H. Cate, Peter Cullen, and Viktor Mayer-Schönberger, focuses on activities perpetuated by data collectors and data users, shaped by context.[198]

Responsible use models might appear to be a strong option, but limiting data use for organizations instead of facilitating consumer choice also limits data use flexibility, which might benefit both consumers and manufacturers. Cate et al. propose relaxed conditions for data collection to those "not incompatible" with previous uses, which could apply in limited conditions where high-risk data elements are collected.[199] IoT functionality, especially where it employs AI, will likely benefit from maximized processing uses across user groups.[200] For this, an alternative privacy model might balance market and consumer interests more effectively than traditional notice and consent models.

D. Cyberkinetic Attacks Pose Substantial Risk to IoT Consumers

Once an individual enters data within a system, organizations must facilitate its processing, transfer, and storage, all of which could compromise confidentiality, integrity, availability of personal information, device data, and device instructions or other commands. Cybersecurity implicates safety and privacy risks due to IoT's intersection of physicali-

194. *See* 15 U.S.C. § 45 (2018).

195. *See* Thierer, *supra* note 14, at 83–88.

196. *See* FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 21–22 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

197. *See* Thierer, *supra* note 14, at 64–65.

198. *Id.*

199. FRED H. CATE ET AL., DATA PROTECTION PRINCIPLES FOR THE 21ST CENTURY 10 (2013), https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1022&context=facbooks.

200. *See* Aman Brar, *What Does the GDPR Mean for IoT?*, IOT AGENDA (May 21, 2018), https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/What-does-the-GDPR-mean-for-IoT. Data analytics based on big data sets often are stored in databases without attendant rules. Associating limited data uses with specific data elements is cumbersome. Further, the nature of ML running on big data sets necessarily means that data may not be anticipated as useful when collected, but may be useful for other purposes. ML in conjunction with human actors may find relationships between data elements in a data set that improve service, or "unknown unknowns," yet nevertheless are not cognizable from the point of forming a relationship with a customer. *The "Unknown Unknowns" of Machine Learning*, NYU CTR. FOR DATA SCI. (June 2, 2016), https://cds.nyu.edu/unknown-unknowns-machine-learning.

ty (the device) and functionality (the service), at times resulting in a physical manifestation, a cyberkinetic attack.[201]

According to Peppet, IoT devices have been compromised in past years largely because engineers did not architect IoT devices with cybersecurity in mind.[202] Certainly, many recent examples of poor IoT cybersecurity exist in the IoT marketplace.[203] A lack of cybersecurity considerations, such as the ability to patch or update systems, demonstrates that traditional manufacturers design these devices, rather than technology companies.[204] The law also does not adequately protect potential interruptions or losses: the FTC's broad enforcement authority has only begun to focus on poor data-cybersecurity practices as unfair or deceptive trade practices, and data-breach notification statutes do not necessarily apply to IoT data.[205]

Potential privacy harms resulting from broad information collection in some cases may be necessary for optimum IoT device functionality. These privacy harms include: ubiquitous data collection, data breach, and identity theft; unrestrained collection of SPI; and the use of algorithmic decision-making to make consequential decisions.[206] Ubiquitous data collection, when properly structured, increases the probability of data breach and subsequent identity theft. [207]

Unrestrained collection of SPI inherently poses unauthorized disclosure risk to individuals, due to the notion that SPI is usually data an individual person wishes to keep private or share with only a few people, such as health conditions, sexual preference, or detailed financial rec-

---

201. *See* Hon et al., *supra* note 6, at 10. IoT cybersecurity issues implicate the Things, cloud services and data, and communication between Things. *Id.* This technology infrastructure presents new and more serious issues than previously identified in internet connectivity. *See* Marin Ivezic, *Our Smart Future and the Threat of Cyber-Kinetic Attacks*, HELP NET SECURITY (Dec. 15, 2017), https://www.helpnetsecurity.com/2017/12/15/cyber-kinetic-attacks.

202. Peppet, *supra* note 56, at 133–36.

203. Nicolas P. Terry, *Will the Internet of Things Transform Healthcare?*, 19 VAND. J. ENT. & TECH. L. 327, 338 (2016).

204. Peppet, *supra* note 56, at 134.

205. *Id.* at 136–40.

206. *See* Vladeck, *supra* note 34, at 501–12; *see also* Goh, *supra* note 34, at 1. Wearable technologies, as a subset of IoT technologies, collect a continuous stream of data about an individual. Please note: Goh defines wearables in much the same way as IoT are defined within this Article, including both implanted and "wearable" devices in this definition. *See id.*

207. Large data stores, when appropriately organized, are often seen as a treasure trove of data, especially when such data includes sensitive data elements more likely to be sold at a high value, such as health data. *See* AJIT GADDAM, SECURING YOUR BIG DATA ENVIRONMENT 4 (2015), https://www.blackhat.com/docs/us-15/materials/us-15-Gaddam-Securing-Your-Big-Data-Environment-wp.pdf. The volume, variety, and veracity of big data magnify cybersecurity risks. Attackers, or threat sources, may come from a variety of backgrounds and typically have different motivations. *Id*. at 1. Financial motivation is very common, although other motivations could lead to kinetic attacks, such as revenge or state-sponsored terrorism. *See Cyber Threat Source Descriptions*, U.S. DEP'T HOMELAND SECURITY, https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions (last visited Oct. 7, 2018). Similarly, healthcare environments require very large data sets to power algorithmic engines. *See* Hon et al., *supra* note 6, at 5–6.

ords.[208] Overcollection of highly sensitive data increases the odds of unapproved disclosure of such data, even if accidental and nonmalicious in nature.

The use of algorithmic decision-making poses two separate issues. First, any changes to the algorithm, especially when created via unsupervised ML, cannot be "caught" by a human when processed automatically.[209] Second, altered algorithms could result in damaging decisions to an individual apart from discriminatory effect, such as being rejected for financial assistance or not receiving credit approval. Serious cybersecurity concerns emerge when both data creating algorithms and algorithms could be altered by an attacker without the knowledge of a manufacturer or consumer.[210]

Because IoT devices are built to transmit and receive almost real-time data, often including information provided from other sources to improve IoT product commercialization, cyberattackers could target IoT devices to harvest large data sets and perpetuate broadscale data breaches or identity theft.[211] Cyberattackers would most likely target more sensitive and financially commercial data: financial data, biometric data, insurance data, tax identifiers, employment data, health data, or other identification numbers.[212] Despite higher risk to IoT devices using sensitive and financially commercial data, attackers might also seek embarrassing or personally (rather than objectively) sensitive data that users expect has been fully secured or anonymized.[213]

IoT devices can be configured to send a wide variety of information to backend systems, which may enable manufacturers to collect far more information than would be necessary to provide IoT services and im-

---

208. Privacy harms can be discussed as *subjective or objective*, with one inherent to the individual and presumably not legally compensable, while the other is determined to merit some compensation or protection under the law. *See* M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1142–43 (2011). SPI largely reflects the first, except where specifically connected to adverse decisions or statutory protection. *See id.*

209. *See* R. Sathya & Annamma Abraham, *Comparison of Supervised and Unsupervised Learning Algorithms for Pattern Classification*, 2 INT'L. J. ADVANCED RES. ARTIFICIAL INTELLIGENCE, no. 2, 2013, at 34, 35.

210. The future of IoT includes AI, which means that AI technological implementations need to address cybersecurity issues, as do IoT infrastructures and devices. Although AI has been discussed in relation to automated attacks and cybersecurity attack prevention, the ability of cyberattackers (AI or non-AI) to change AI functions would likely cause substantial damage without human intervention. *Cf.* David Schatsky et al., *Intelligent IoT: Bringing the Power of AI to the Internet of Things*, DELOITTE INSIGHTS (Dec. 12, 2017), https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/intelligent-iot-internet-of-things-artificial-intelligence.html (identifying the potential value of AI to IoT, while not addressing potential cybersecurity issues in unsupervised device functionality).

211. *See supra* Section I.A and accompanying notes.

212. *See* Chen Han & Rituja Dongre, *Q&A. What Motivates Cyber-Attackers?*, TECH. INNOVATION MGMT. REV., Oct. 2014, at 40, 40–41 (2014).

213. Mark van Rijmenam, *The Re-Identification of Anonymous People with Big Data*, DATAFLOQ (Feb. 10, 2016), https://datafloq.com/read/re-identifying-anonymous-people-with-big-data/228.

prove such services over time.[214] Because manufacturers may configure IoT devices to connect to other IoT devices or mobile devices and associated apps, excessive data collection is highly probable, not just possible.[215]

In addition to data collection risks, IoT devices pose other risks to health, safety, and property. Although data collection can harm an individual via data loss, disclosure, or theft, IoT vulnerabilities may also endanger IoT device users, user homes, or a user's personal property.[216] State-sponsored hackers or rogue hacking organizations desiring to cause damage, interrupt service, or simply wreak havoc, would likely focus on infrastructure resources or application code to change or stop data transferred between a product cloud and connected IoT devices.[217]

Because of these risks, it is anticipated that IoT devices will impact not only privacy law but also questions of product liability and insurance coverage.[218] Examples of such impact include: simple IoT malfunction causing physical injury or property damage, outsider attacks causing physical injury or property damage, and hacking of devices or other systems resulting in personal information loss.[219]

IoT devices present new attack vectors and potential vulnerabilities specific to IoT technologies, increasing the probability of compromise.[220] Mohammad Abomhara and Geir M. Køien have identified three factors increasing the value of IoT to attackers: the automated nature of most devices without direction or involvement of humans, pervasive wireless connectivity, and limited resources to run traditional cybersecurity tech-

---

214. *Cf.* Rolf H. Weber, *Internet of Things—New Security and Privacy Challenges*, 26 COMPUTER L. & SECURITY REV. 23, 24 (2010).

215. One of the central pillars of privacy involves limiting data collection to business necessity; collection is within the bounds of what a reasonable person would expect, or data collection is proportionate to its use (rather than excessive). Ubiquitous computing turns this privacy pillar on its head by pre-supposing that this data is needed, and the value of AI combined with big data sets illustrates the value of collecting more than a business needs or a customer knows to be shared.

216. Lucy L. Thomson, *Insecurity of the Internet of Things*, ABA SCITECH LAW., Summer 2016, at 32, 34 (2016).

217. *See, e.g.*, Stephen Cobb, *10 Things to Know About the October 21 IoT DDoS Attacks*, WELIVESECURITY (Oct. 24, 2016, 7:16 PM) http://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks (describing a botnet that caused a distributed denial of service attack that stopped service for IoT devices).

218. Ellen MacDonald Farrell & Rachel P. Raphael, *Insurance Coverage Issues Created by the Internet*, LEXIS PRAC. ADVISOR J. (Feb. 28, 2018), https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/archive/2018/02/28/insurance-coverage-issues-created-by-the-internet.aspx; H. Michael O'Brien, *3 Ways Internet of Things Will Impact Product Liability*, LAW360 (Apr. 30, 2015, 9:26 AM), https://www.law360.com/articles/646492/3-ways-internet-of-things-will-impact-product-liability.

219. O'Brien, *supra* note 218. These impacts could lead to further attacks, such as distributed denial of service attacks (DDoS), which result in wide-scale outage. *See* Nat'l Cybersecurity Ctr. of Excellence, *Mitigating IoT-Based DDoS*, NAT'L INST. STANDARDS & TECH., https://nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos (last visited Oct. 7, 2018).

220. Thomson, *supra* note 216, at 33.

nologies.[221] A short-hand of these factors might include: *automation*, *connectivity*, and *resource constraints*. It is useful to consider how these devices might function to understand these factors in more detail:

> A home thermostat controls heating and cooling according to user-programmed specifications and is connected to a home wireless network, where it sends and receives real-time data to a product cloud, while receiving direction both from the product cloud and from the home owner, who has a mobile app to control the home temperature. The manufacturer has also implemented a ML utility to analyze data points from across devices and propose new schedules that might save the home owner on energy costs.

In this example, the home thermostat runs in the background, sending near real-time data back to the product cloud and receiving instructions both from the product cloud and from the home owner. The ability to send data is supported by a pervasive network connection with the home network. The homeowner decided to purchase a low-cost model, which does not include cybersecurity features. This example is not unusual: IoT devices are currently manufactured for low cost and speed, often resulting in few cybersecurity features.[222] Where devices have cybersecurity features, most do not include regular cybersecurity updates, critical for responding to changing cybersecurity vulnerabilities.[223]

Cybersecurity researchers, or ethical hackers, have recently completed vulnerability analyses on smart home products, and these analyses have brought personal-safety and property-damage risks, rather than privacy risks, to the forefront of IoT conversations.[224] Attackers could unlock IoT doors and padlocks, control connected wheelchairs remotely, and change smart thermostat temperatures past their factory maximums, posing risk of substantial damage to property and bodily harm.[225] In some cases IoT might require privacy measures under the law, but most IoT will not receive the same consideration for potential safety issues posed by poor cybersecurity.[226]

Connected toys have also caused significant concern over potential injury or exposure of children's information. Since 2007, manufacturers

---

221. Mohamed Abomhara & Geir M. Køien, *Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks*, 4 J. CYBER SECURITY & MOBILITY 65, 68 (2015).

222. *See generally* Tanuj Mohan, *IoT Security: Let's Not Forget the 'Thing*,*'* FORBES TECH. COUNCIL (May 2, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/05/02/iot-security-lets-not-forget-the-thing.

223. *See* Abomhara & Køien, *supra* note 221, at 71.

224. *See* Lucian Constantin, *Hackers Found 47 New Vulnerabilities in 23 IoT Devices at DEF CON*, CSO (Sept. 13, 2016, 9:32 AM), http://www.csoonline.com/article/3119765/cybersecurity/hackers-found-47-new-vulnerabilities-in-23-iot-devices-at-def-con.html.

225. *Id.* It is important to understand that although these particular devices were compromised, only twenty-three devices were reviewed, of many more devices currently manufactured.

226. *See* Hartzog & Selinger, *supra* note 185, at 589.

have invested in connected toys, and many of these toys include communication, messaging, or multiplayer features.[227] Such features could be manipulated by a cyberattacker, including attackers impersonating another child; communicating with children; collecting video, images or sound; or identifying a child's physical location.[228] Due to the potential for an alternative, unauthorized entity to communicate with a child through a toy, one Google toy patent was dubbed "IoT Chucky," referring to the ubiquitous possessed doll in a string of horror movies.[229]

Many cybersecurity and privacy concerns for connected toys have not become a reality yet, but some IoT devices used for children have already been compromised. Baby monitors are often manufactured today with internet-enabled capabilities to facilitate remote baby monitoring on mobile devices, and hackers have used poor cybersecurity on such devices to communicate directly with children.[230] Several disturbing accounts have been publicized, including one account where a hacker communicated disturbing messages to a child through the monitor.[231] Surely, even if the United States does not want to regulate IoT product cybersecurity generally, the potential for injury to children or other vulnerable populations resulting from poor cybersecurity measures should raise questions regarding appropriate IoT regulation.

The examples articulated in this Section are not comprehensive; rather, they illustrate substantial risks to consumers regarding discriminatory data-use practices, evolving privacy obligations, and emerging cybersecurity issues. Because potential IoT device compromise includes not only unauthorized disclosure but also potential physical-safety and property-damage risks, a sufficiently broad legal framework must be established or modified to prevent some discrimination, privacy, and cybersecurity IoT risks.

III. IOT REGULATORY FRAMEWORKS

The United States has not yet developed a comprehensive regulatory framework for IoT, big data, or AI. Although existing privacy and cybersecurity laws may provide minimal privacy or cybersecurity protection for IoT in specific, high-risk sectors, these laws focus on outdated

227. Marie-Helen Maras, *4 Ways 'Internet of Things' Toys Endanger Children*, CONVERSATION (May 10, 2018, 6:47 AM), https://theconversation.com/4-ways-internet-of-things-toys-endanger-children-94092.

228. Danelle L. Dobbins, Analysis of Security Concerns and Privacy Risks of Children's Smart Toys 1–4 (Sept. 28, 2015) (unpublished Ph.D. thesis, Washington University in St. Louis), https://sever.wustl.edu/degreeprograms/cybersecurity-management/SiteAssets/Dobbins%20-%20SmartToy_security_Final%20Revised%209-28-15.pdf.

229. *Id.* at 1.

230. Anthony Cuthbertson, *How to Protect Baby Monitors from Hackers*, NEWSWEEK (Jan. 29, 2016, 12:07 PM), http://www.newsweek.com/how-protect-baby-monitors-hackers-421104.

231. Chante Owens, *Stranger Hacks Family's Baby Monitor and Talks to Child at Night*, S.F. GLOBE (Dec. 17, 2017), http://sfglobe.com/2016/01/06/stranger-hacks-familys-baby-monitor-and-talks-to-child-at-night.

models for privacy and fail to account for increased risk presented by big data use and AI.[232] Congress has historically developed models that improve ease of compliance for a particular industry. Laws, such as HIPAA, are narrowly tailored to the most sensitive data consumers create or provide within a particular sector: data most vulnerable to exposure resulting in fraud or other harms, a risk-management model for regulation directly tied to data classification.[233] Although most of these laws focus only on privacy obligations, a few laws, such as HIPAA and GLBA, have also incorporated cybersecurity requirements.[234]

The EU's GDPR and the Network Information Cybersecurity Directive (NIS Directive) more comprehensively address these issues, offering potential models for IoT regulation. If the United States can appropriately sample key aspects of the GDPR and NIS Directive, the United States will benefit from a specifically defined regulatory framework focused on reducing discrimination, privacy, and cybersecurity risks to consumers while simultaneously protecting market interests related to data transfer and product efficacy.[235]

A. Healthcare IoT (IoHT)

For healthcare services and medical devices, two primary laws regulate the privacy, cybersecurity, and safety of services and devices for consumers: HIPAA and the Food, Drug, and Cosmetic Act (FDCA).[236] These divisions of the Department of Health and Human Services and the Food and Drug Administration (FDA) are tasked with regulating medical device manufacturing, while the Office for Civil Rights (OCR) manages healthcare compliance for CEs and BAs.[237] CEs often form the

---

232. Even for the most regulated of industries, privacy laws do not meet existing challenges around advanced and complex algorithm usage. Ford and Price explain that the dichotomy between algorithm accountability and privacy pose unique challenges for black-box medicine, or opaque algorithm usage in the medical context. Ford & Price, *supra* note 5, 12–31. Similarly, IoT applications of such algorithmic decision-making necessarily require navigating this dichotomy because similar infrastructures and goals apply to effective IoT functionality. *See* Hon et al., *supra* note 6, at 25. Privacy laws, such as HIPAA, are designed with a core focus of data minimization and reduction of identifiable data elements. *See id.* at 23.

233. This assertion is self-evident upon reading HIPAA, GLBA, COPPA, or the FCRA. *See infra* Sections III.A–III.C and accompanying notes. Each of these laws narrowly tailors its ambits to specific data classification (in the case of HIPAA the classification is wide, whereas the safe harbor for de-identification is specific, rendering certain data elements protected or not protected in relief) and organizations to be regulated (i.e., financial institutions for GLBA, CEs and BAs for HIPAA). Presumably, such an approach is purposeful and intended to focus on specific risks while offering organizational flexibility for lower risk activities.

234. *See* Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. § 6802 (2018); Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. §§ 160.103, 164.514 (2018).

235. *See infra* Part IV and accompanying notes.

236. *See* Federal Food, Drug, and Cosmetic Act (FDCA), 21 U.S.C. §§ 351–360 (2018); 45 C.F.R. §§ 160.103, 164.514.

237. 21 U.S.C. §§ 351–360; 45 C.F.R. §§ 160.103, 164.514; U.S. Dep't of Health & Human Servs., *Summary of the HIPAA Privacy Rule*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html?language=en (content last reviewed July 26, 2013).

primary relationship with a consumer, such as a healthcare provider, a group health plan, or a health insurance provider; while a BA works on behalf of and at the direction of a CE, for example providing technical services, billing services, or medical devices used at CE facilities or as part of insurance billing.[238]

The FDA, following concerns regarding connected devices, created off-the-shelf, pre- and post-market cybersecurity guidance for organizations manufacturing medical devices.[239] This guidance illustrates improved agency awareness of potential medical-device vulnerabilities on connected devices, but relying solely on guidance, rather than legal requirements, may not communicate the stringency needed to protect public health.[240] Although guidance may be instructive, guidance does not create binding obligations as administrative rules or law might establish, especially for manufacturers new to the medical-device sector or for devices not requiring FDA clearance review.

Since 2015 and continuing through the 21st Century Cures Act, the FDA has communicated self-imposed limitations on review of some medical IoT devices, presumably those without pervasive connectivity to the body (e.g., Class III implantable devices).[241] The FDA has, in review guidance, specified its intention to focus on limited Class II and Class III devices, yet these devices often are directly connected to the body, rather than decisional support systems or sensor-based systems, which nevertheless could impact privacy and cybersecurity.[242] Unfortunately, this likely means that many devices storing and transmitting highly sensitive data, such as those from sensor technologies or other health-tracking devices, may not be reviewed by the FDA.

IoT devices that are not regulated by the FDA may not be regulated under HIPAA. Because HIPAA applies to ePHI when an individual's data is handled by a CE or BA, typically the HIPAA Privacy Rule and Cybersecurity Rule will apply under the following conditions: when insurance is reimbursing or billing for IoT device use at the direction of a

238. U.S. Dep't of Health & Human Servs., *Business Associates*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html (July 26, 2013); U.S. Dep't of Health & Human Servs., *Covered Entities and Business Associates*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (content last reviewed June 16, 2017).

239. *Cybersecurity*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm (last updated Oct. 1, 2018).

240. *See* Charlotte A. Tschider, *Enhancing Cybersecurity for the Digital Health Marketplace*, ANNALS HEALTH L., Winter 2017, at 1, 10, 16, 29.

241. *Id.* at 25–26. The FDA has disclosed its intention to reduce oversight for Tier 1 devices, which may include Internet of Health Things (IoHT) sold to consumers. *See id.*

242. *See* U.S. FOOD & DRUG ADMIN., MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 13–15 (2015), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf. Further, the 21st Century Cures Act has subsequently eliminated some tools from the definition of medical device, further narrowing the scope of what the FDA will actually review. *Id.*

CE (IoT medical-device use) or IoT devices are provided as part of Group Health Plan or health insurance reimbursements.[243] Unfortunately, the narrow circumstances under which HIPAA requires IoT devices to employ cybersecurity protection leave many IoT devices handling health information unprotected.[244]

B. Children's Data

IoT devices affecting children's privacy, such as connected toys, are regulated by the FTC under COPPA.[245] COPPA applies to children under the age of thirteen and involves privacy (rather than cybersecurity) statutory requirements, such as the requirement to collect explicit, verifiable consent from a parent and a parent's right to stop processing of personal information.[246] COPPA regulates online activities that collect specific data elements, including: a child's image, screen name/avatar, location information, persistent online identifiers (such as an IP address), and other contact information, all likely data elements captured in IoT devices.[247] However, COPPA only provides privacy protections for children under the age of thirteen, and obligations appear to be tailored for an online web environment, rather than a device-centric environment with limited physical real estate for privacy notice display and agreement.[248] Further, it is unknown whether Congress will update COPPA to explicitly include IoT devices: devices are part of the online environment and

---

243. *See* Terry, *supra* note 203, at 339 (describing the function of HIPAA rules and their application to IoT entities, remarking that most mobile health hardware and software providers will not be subject to HIPAA).

244. *See generally* Tschider, *supra* note 240 (analyzing obligations for the digital health marketplace under both the FDCA and HIPAA, concluding that many devices will be left to general Federal Trade Commission oversight, rather than comparatively more restrictive and prescriptive regimes). Though related to device functionality rather than discrimination, algorithms in medical devices have received recent attention for their relative opacity and potential for safety issues. *See, e.g.*, W. Nicholson Price II, *Regulating Black-Box Medicine*, 116 MICH. L. REV. 421, 471 (investigating FDA processes and potential improvements as medical device functionality, including use of algorithms, is increasingly automated); Charlotte A. Tschider, *Deus Ex Machina: Regulating Cybersecurity and Artificial Intelligence for Patients of the Future*, 5 SAVANNAH L. REV. 177, 201–02 (2018) (describing the need to regulate AI due to potential AI safety and cybersecurity issues).

245. Press Release, FTC, Electronic Toy Maker VTech Settles FTC Allegations That It Violated Children's Privacy Law and the FTC Act (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated; *see* COPPA, 15 U.S.C. §§ 6501–06 (2018).

246. 15 U.S.C. § 6502.

247. *Id.* §§ 6501–02. COPPA will, to some extent, regulate children's IoT. *See id.* § 6502(b)(1)(A)(ii). Unfortunately, these protections do not include cybersecurity protections and do not apply to children thirteen and over. *See id.* § 6501(1).

248. Richard Chapo, *COPPA and the Internet of Things*, COPPA AND FERPA (June 10, 2016), http://web.archive.org/web/20161107194435/http://www.coppalawattorney.com/coppa-and-the-internet-of-things-2. Chapo describes a complaint rejected by the FTC, where the FTC appeared to narrowly define COPPA's "intentionally directed at children" requirement for broadly used devices, such as the Amazon Echo. *See id.* The FTC also stated that it did not believe new laws were needed at this time, due to the future evolution of IoT devices. *See id.* It should also be noted that California has extended COPPA's ability to delete data on request from under age thirteen to age eighteen. CAL. BUS. & PROF. CODE § 22580 (West 2018). A parent or individual after the age of eighteen may request deletion of data below age eighteen. *See id.*

the FTC has enforced actions against toy manufacturers.[249] However, it is still unclear whether Congress intended COPPA to apply to children's IoT devices, as it is not specifically noted within COPPA's text and legislative history.[250]

In addition to their relatively limited application across the IoT landscape and either nonexistent or insufficient cybersecurity controls, COPPA, HIPAA, and GLBA require adherence to a traditional privacy model. First, all require a traditional notice model, providing notice prior to any change in data-handling practices.[251] This model provides constructive notice, or an *opportunity* to read, but this notice does not necessarily result in meaningful choice. For IoT, product-specific constraints may limit the opportunity to display these details on an IoT device prior to data transmission and device communication in some IoT models.[252] As COPPA, GLBA, and HIPAA also reference specific data elements to which the laws apply, it is also unlikely that unspecified, personally identifiable IoT data or inferences would be regulated under any of these laws.[253]

C. Credit and Finance IoT

Although it is unlikely for consumer IoT to include credit reporting or be manufactured by financial institutions or investment companies, the Fair Credit Reporting Act (FCRA) and the GLBA could address some of the concerns raised by IoT devices. The GLBA specifically applies to financial institutions and NPI, requiring privacy notices and limiting third party data transfer.[254] The Office of the Comptroller of the Currency conducts annual and bi-annual examinations of GLBA-regulated organizations to assess privacy and cybersecurity protections.[255] Regulation S-P

---

249. FTC, *supra* note 196, at 5, 53. The FTC has since extended its guidance for COPPA to include connected toys, although COPPA itself does not specify application to IoT. *See Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, FTC (June 2017), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance [hereinafter FTC, *Compliance Plan*].

250. GINA STEVENS, CONG. RESEARCH SERV., LSB10051, SMART TOYS AND THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT OF 1998, at 2–3 (2018).

251. *See* Tschider, *supra* note 240, at 12–13. HIPAA (unlike COPPA) does not require *explicit* consent (consent is implied, except where express authorization is needed), but the vast majority of state laws do require explicit consent as well. *See id.* COPPA requires explicit notice followed by parental consent prior to data processing activities commencing. 15 U.S.C. § 6502(b)(1)(A).

252. *See supra* Section II.C and accompanying notes.

253. COPPA specifically lists children's data elements. *See* 15 U.S.C. § 6501(8); FTC, *Compliance Plan*, *supra* note 249. HIPAA has a broad definition of Protected Health Information (PHI). *See* 45 C.F.R. § 160.103. However, the presence of a HIPAA de-identification safe harbor effectively establishes these elements in relief: when these data elements have been removed, data may be transferred or processed without restriction. U.S. Dep't of Health & Human Servs., *supra* note 131.

254. 15 U.S.C. § 6802.

255. *See* OCC, OCC 2001-35, EXAMINATION PROCEDURES TO EVALUATE COMPLIANCE WITH THE GUIDELINES TO SAFEGUARD CUSTOMER INFORMATION, at 1 (2001), https://www.occ.gov/news-issuances/bulletins/2001/bulletin-2001-35a.pdf; *OCC Bulletin 2001-8, Guidelines Establishing Standards for Safeguarding Customer Information*, OCC.GOV, (Feb. 15, 2001), https://occ.gov/news-issuances/bulletins/2001/bulletin-2001-8.html.

mirrors GLBA requirements for investment institutions, regulated by the Securities and Exchange Commission with additional Financial Industry Regulatory Authority (FINRA) obligations and assessments.[256] Despite establishing privacy and cybersecurity expectations, few IoT manufacturers currently qualify as financial institutions or investment organizations.

Laws applicable to organizational decisions that could affect an individual's legal or similarly serious interests, such as antidiscrimination legislation or sectoral privacy laws, do not directly address potential discriminatory effects of automated technologies, with the exception of the FCRA.[257] The FCRA requires an organization making a decision based on legally reported credit data to inform the affected individual of the adverse action and agency providing the data, reasons for the adverse action, and responsive measures that may be taken if the information is incorrect.[258] Insurers might similarly use sensitive data for discriminatory reasons due to the insurance sector's ability to incorporate advanced analytics and reliance on data for decision-making.[259] These activities, along with those defined as producing results protected under due process interests, could introduce greater probability of individual injury.[260] A preliminary matter in FATE legal analysis should include defining or recognizing (as in due process matters) substantially impactful effects that require enhanced legal protection.[261]

D. FTC Actions and State Law

In addition to COPPA administration, the FTC also has broad rulemaking authority under Section 5 of the FTC Act to regulate unfair and deceptive trade practices.[262] FTC recognition of regulatory activity needed in the cybersecurity and privacy areas has translated to a flurry of activity in recent years to target organizations with insufficient cyberse-

256. 17 C.F.R. § 248.3(a)(1)–(2) (2018). In 2017, cybersecurity was identified by FINRA as an "Operational Risk" and a FINRA priority. *See* FIN. INDUS. REGULATION AUTH., 2017 ANNUAL REGULATORY AND EXAMINATION PRIORITIES LETTER (2017), http://www.finra.org/sites/default/files/2017-regulatory-and-examination-priorities-letter.pdf.

257. *See* Peppet, *supra* note 56, at 124–27. Peppet describes the broad loopholes in using data not directly implicating Title VII, the Americans with Disabilities Act (ADA), and the Genetic Information Non-Discrimination Act (GINA): for example, an employer not hiring a potential employee because of their poor exercise history (that might indicate a health condition) or indicia for race. *See id.* at 125.

258. 15 U.S.C. § 1681s-2(a)(1)(A)–(B). Despite these requirements, opportunities still exist for big data usage in credit activities. *See generally* Citron & Pasquale, *supra* note 101, at 24–28 (proposing additional safeguards for ensuring due process in credit monitoring).

259. Helveston, *supra* note 74, at 894. Insurers are permitted to overtly discriminate based on risk and loss calculations that directly tie to the identity and circumstances of the individual person. *See id.* at 893–94. However, discrimination may be difficult to tie to insurer decision-making when algorithms increasingly make decisions. *See id.* at 895.

260. *See* Crawford & Schultz, *supra* note 101, at 99–101. Crawford and Schultz address the risks of using automated decisioning for critical decisions, such as housing. *See id.* at 101–02.

261. *See FATE: Fairness, Accountability, Transparency, and Ethics in AI*, *supra* note 79.

262. *See* Terry, *supra* note 203, at 341.

curity controls following a data breach and organizations misrepresenting their privacy practices.[263] Despite recent success, IoT devices have not yet received a great deal of attention; and absent congressional intervention, the FTC plans to regulate IoT devices similarly to its historical Section 5 practices.[264] Despite Section 5's breadth, it also lacks specificity with regard to manufacturer programs and behavior, focusing heavily on *ex post* recovery rather than instructive upfront requirements.[265] Under Section 5, IoT manufacturers may only be held accountable for unfair or deceptive trade practices after products have already been developed, potentially impacting the privacy and safety of consumers.[266]

The FTC has developed several guides regarding broad privacy applications, suggesting that prior notice and clear disclosures should be used whenever possible.[267] Mobile devices, for example, should incorporate "just-in-time" contextual disclosures and obtain "express affirmative consent" before allowing apps to access sensitive device content.[268] In 2015, the FTC released a staff report discussing IoT privacy and cybersecurity from the perspective of workshop participants, including a discussion of functional and practical challenges in facilitating notice and consent on IoT devices, such as difficulties of managing device size and the degree of burden shifting to the device user in reviewing notices.[269] Still, the FTC has not proposed a reasonable solution for anticipated IoT vulnerabilities, such as cybersecurity issues and potential for discrimination.[270]

State laws have begun to anticipate general privacy and cybersecurity issues, with the 2017 New York Cybersecurity Act (NYCA) becoming

---

263. *Id.* (recounting the *FTC v. Wyndham Worldwide Corp*., 10 F. Supp. 3d 602 (D.N.J. 2014), and *In re LabMD, Inc.*, No. 9357, 2016 WL 4128215 (F.T.C. 2016), cases, establishing the role of the FTC in regulating unfair practices as they pertain to cybersecurity protections for consumers and establishing a co-extensive regulatory environment for the OCR and FTC with respect to healthcare activities). *See generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 589, 630 (2014) (describing the FTC's development of a parallel common law through its enforcement and other administrative actions).

264. Although the FTC has pushed for additional funding and more overt enforcement power, so far Congress has not agreed. *See* Terry, *supra* note 203, at 340–42.

265. *See id.* at 341–42. Despite the fact that the FTC's role has primarily consisted of guideline development and administrative action after the fact, government leaders have called on the FTC to take a more active role in IoT privacy and cybersecurity activities. *See* Press Release, Richard Blumenthal, Blumenthal to FTC: Internet of Things Manufacturers Must Implement Reasonable Security Standards to Prevent Cyber Attacks (Nov. 3, 2016), https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-to-ftc-internet-of-things-manufacturers-must-implement-reasonable-security-standards-to-prevent-cyber-attacks.

266. *See* Terry, *supra* note 203, at 341–42.

267. *See, e.g.*, FTC, *supra* note 196, at 22–23, 27 (describing challenges in the feasibility of facilitating traditional notice and consent).

268. *See* FTC, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 15, 19–20, 23 (2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

269. *See* FTC, *supra* note 196, at i–ii, 20–22.

270. Hartzog & Selinger, *supra* note 185.

the most comprehensive cybersecurity law to date.[271] The NYCA is applicable to financial institutions, investment organizations, and insurers licensed within the state of New York; it provides a comprehensive roadmap for strong cybersecurity practices.[272] Prior to passage of the NYCA, states had begun to pass specific cybersecurity requirements within state data-breach legislation, while states like California extended federal protection for children.[273] Washington state, Nevada, and Minnesota have statutes that attempt to regulate payment processing at retailers.[274] Although state regulators are increasingly aware of the challenges regarding privacy and cybersecurity, regulators have not directly addressed IoT, big data, or AI.[275]

E. Interest, Not Action, for IoT

With increased attention on IoT privacy, safety, and financial concerns, agencies traditionally less concerned with privacy and cybersecurity have begun considering future involvement in IoT regulation. In 2015, the U.S. Senate began reviewing questions regarding the dangers of IoT.[276] The initial hearing focused on concerns regarding connected cars and highlighted bipartisan apprehension about regulating a growing industry.[277] In 2017, Senators reintroduced the 2016 Developing Innovation and Growing the Internet of Things (DIGIT) Act, a bipartisan bill directing an IoT strategy by creating a commission to evaluate potential development, including consideration of user privacy and cybersecurity.[278]

In 2016, the Chairman of the Consumer Product Safety Commission (CPSC), Elliot Kaye, had communicated a desire for the CPSC to begin preparing for IoT safety concerns in 2016, including the role and efficacy

---

271. 23 N.Y. FIN. SERV. LAW § 500 (McKinney 2018).

272. *Id.* § 500–01.

273. *See* CAL. BUS. & PROF. CODE § 22580 (West 2018).

274. *FAQ on Washington State's PCI Law*, INFOLAWGROUP LLP (Mar. 24, 2010), https://www.infolawgroup.com/blog/2010/03/articles/payment-card-breach-laws/faq-on-washington-states-pci-law.

275. *See* Jacqueline Klosek, *Regulation of Big Data in the United States*, GLOBAL DATA HUB: TAYLOR WESSING (July 2014), https://united-kingdom.taylorwessing.com/globaldatahub/article_big_data_us_regs.html (describing applicable laws for financial institutions and specific health organizations, without any specific regulation applicable to big data); *see infra* Section III.E and accompanying notes (describing attempts at regulating U.S. IoT); *see, e.g.*, Matthew U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, 29 HARV. J.L. & TECH. 353, 393 (2016) (proposing a statutory approach to regulate AI); *see also* Calo, *supra* note 82, at 410 (identifying key policy questions related to potential AI regulation).

276. Jedidiah Bracy, *Senate Committee Explores Internet-of-Things Regulation*, IAPP (Feb. 12, 2015), https://iapp.org/news/a/senate-committee-explores-internet-of-things-regulation.

277. *Id.*

278. DIGIT Act, S. 88, 115th Cong. § 1–2 (as passed by Senate, Aug. 3, 2017); Press Release, Deb Fischer, Senators Introduce Bipartisan Internet of Things Bill (Mar. 1, 2016), https://www.fischer.senate.gov/public/index.cfm/2016/3/senators-introduce-bipartisan-internet-of-things-bill. The DIGIT Act was passed by the Senate. *S. 88: DIGIT Act*, GOVTRACK.US (Aug. 3, 2017), https://www.govtrack.us/congress/bills/115/s88.

of federal recall processes.[279] With the appointment of an acting Chairman, Ann Marie Buerkle, it is unclear how the CPSC's priorities might change.[280]

The Federal Communication Commission (FCC) briefly considered advancing IoT rules, aimed at risk reduction, but these considerations were put on hold indefinitely following a Donald Trump presidential victory.[281] The plan would have involved FCC Advisory Committees, Internet Service Provider-wide adoption of cybersecurity standards, a device certification process, and government/manufacturer collaboration to address risk-mitigation strategies.[282] Despite the FCC's interest in regulating IoT broadly, it appears that Congress would prefer to leverage existing frameworks to address the IoT concerns, rather than drafting new regulations for diverse IoT devices.[283]

The Department of Commerce's National Telecommunications and Information Administration (NTIA) sought public comment in 2016 on expected legal strategy for regulating IoT.[284] On January 12, 2017, the NTIA released a green paper entitled *Fostering the Advancement of the*

279. Emily Field, *CPSC Chair Kaye Eyes Safety Risks in New Technologies*, LAW360 (Aug. 8, 2016, 6:22 PM), https://www.law360.com/articles/824104/cpsc-chair-kaye-eyes-safety-risks-in-new-technologies.

280. Press Release, U.S. Consumer Prod. Safety Comm'n, Ann Marie Buerkle Elevated to Serve as Acting Chairman of U.S. Consumer Product Safety Commission (Feb. 10, 2017), https://www.cpsc.gov/content/ann-marie-buerkle-elevated-to-serve-as-acting-chairman-of-us-consumer-product-safety.

281. Shaun Waterman, *FCC Abandons Plans for Rules on IoT Cybersecurity*, CYBERSCOOP (Dec. 5, 2016), https://www.cyberscoop.com/iot-cybersecurity-fcc-donald-trump-mark-warner. Although the FCC may regulate aspects of IoT technology, the FCC has not characteristically enforced discriminatory impact, privacy, and cybersecurity, despite some regulation. *See* Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2018) (establishing requirements for communication transmissions and prohibiting unauthorized access to such communications).

282. Letter from Tom Wheeler, Chairman, FCC, to Senator Mark Warner (Dec. 2, 2016), https://www.scribd.com/document/333290070/FCC-Response-12-05-2016. Other industry leaders have proposed a third-party verification system, similar to the Fair Trade USA certification. *See* Amy Nordrum, *Which Path to IoT Security? Government Regulation, Third-Party Verification, or Market Forces*, IEEE SPECTRUM (Oct. 25, 2016, 1:00 PM), https://spectrum.ieee.org/tech-talk/telecom/internet/experts-discuss-3-paths-to-stronger-iot-device-security-government-regulation-thirdparty-verification-and-market-forces.

283. Mohana Ravindranath, *Who's in Charge of Regulating the Internet of Things*, NEXTGOV (Sept. 1, 2016), http://www.nextgov.com/emerging-tech/2016/09/internet-things-regulating-charge/131208. IoT devices may be highly diverse in function. Consider, for example, the differences between an implanted medical device, a distributed electrical grid management solution, a smart home, connected cars, and a connected set of army men. All of these devices are tremendously different in the data collected, the level of data sensitivity, the potential safety risks, and the overall computing power available to implement privacy or cybersecurity features. The National Institute of Standards and Technology (NIST) has developed a program, the Cybersecurity for IoT, which includes a variety of inputs from previously defined standards, frameworks, and functions. *See NIST Cybersecurity for IoT Program*, NIST (Sept. 25, 2018), https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program.

284. The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, 81 Fed. Reg. 19,956–60 (Apr. 6, 2016).

Internet of Things.[285] In this green paper, the NTIA reported on specific needs of the manufacturing community, including flexible standards not imposed by overly prescriptive regulations.[286] Some commenters emphasized the importance of cybersecurity by design and privacy by design, or building cybersecurity and privacy requirements into manufacturing and development processes.[287] Further, continuous updates and patching processes are required when new cybersecurity vulnerabilities are identified, a complex activity for consumer IoT devices.[288] Commenters also identified potential areas for increased scrutiny, such as devices used by children and connected, autonomous vehicles.[289]

From a privacy perspective, the NTIA green paper highlighted somewhat conflicting comments. Commenters acknowleged changing concerns with IoT for privacy, including the ubiquity of personal information, potential for collection of sensitive information, and transmission of data.[290] In contrast, commenters also argued that no new privacy issues applied to IoT, that it may be too early to define a regulatory privacy approach, and that it may be worth determining how existing regulation governs IoT.[291] Despite collection of commentary regarding IoT, commenters also communicated that the Department of Commerce is not well-positioned to regulate IoT as it does not currently have responsibility for privacy and cybersecurity compliance.[292]

The wide range of active administrative agencies determining the correct approach for regulating IoT demonstrates both the substantial benefits and risks associated with this technology. In August 2017, Democratic Senator Mark Warner introduced the Internet of Things Cybersecurity Improvement Act of 2017 (IoT-CIA), signaling some interest in reinvigorating discussion on IoT; but it is still unknown whether the IoT-CIA will receive serious consideration.[293]

F. The EU Model

The United States has not yet developed a comprehensive scheme for managing automated decision-making, but the EU has attempted to regulate these activities for organizations processing European residents' personal data, including U.S.-based multinational manufacturers. The GDPR has created one of the most comprehensive approaches to prevent

285. INTERNET POLICY TASK FORCE & DIG. ECON. LEADERSHIP TEAM, U.S. DEP'T OF COMMERCE, FOSTERING THE ADVANCEMENT OF THE INTERNET OF THINGS (2017), https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.
286. *Id.* at 25.
287. *Id.* at 27–28.
288. *Id.*
289. *Id.* at 26.
290. *Id.* at 32.
291. *Id.* at 31.
292. *Id.* at 33.
293. Internet of Things (IoT) Cybersecurity Improvement Act of 2017, S. 1691, 115th Cong. (2017).

unfair automated decision-making: notice prior to processing automated decisions, explicit consent requirements for automated decision-making impacting legal or similarly serious interests, an opportunity for an individual to object to such processing, and an opportunity to be heard via complaint.[294]

The GDPR regulates organizations within the EU region and any organization processing EU resident data via its long-arm provisions, including U.S. organizations.[295] The GDPR addresses these in three parts: (1) opportunity to consent (or not) to individual profiling, (2) notice of automated decision-making and potential consequences, and (3) opportunity to object to such automated decisions.[296] These activities ensure that people have the opportunity to know how their data will be automatically processed, to choose whether or not this model is desirable, and the ability to halt further activities or object and presumably receive an alternative (human) decision. The GDPR does not narrowly apply this requirement to activities involving special categories of personal information (more sensitive data), instead relying on application to those activities producing "legal effects" or "similarly significant effects."[297] The natural circumstances under which objection to automated processing would take place likely involves decisions implicating the

294. *See* GDPR, *supra* note 78, at 1, 45, 80.

295. *Id.* at 2–3. Article 22 directly establishes limits on profiling and automated decision-making, although these concepts are also weaved into Article 4(4) (definitions), Article 13 (Notice), and Article 15 (data subject rights). *Id.* at 33, 40, 43, 46. The application of these articles is quite broad, as personal information is broadly defined. Therefore, profiling and automated processing might pertain to newly created personal information resulting from processing or other insights derived from indirect or secondary identifiers. *See supra* Section II.B and accompanying notes. Many U.S. organizations make the mistake of thinking that Privacy Shield certification through the U.S. Department of Commerce effectively covers these organizations for GDPR compliance. However, Privacy Shield certification only covers data transfer to the United States when the recipient does not have a direct relationship with EU residents (e.g., suppliers of an EU company or a multinational company doing business with EU residents). When an organization does have a relationship with EU residents and is processing EU resident personal information, GDPR applies. *See* GDPR, *supra* note 78, at 32–33.

296. *See* GDPR, *supra* note 78, at 1, 6, 45, 80. Profiling and automated decision-making stem from the same foundation—data—and are linked within the GDPR: profiling is only restricted when it involves automated decision-making. Rita Heimes, *Top 10 Operational Impacts of the GDPR: Part 5—Profiling*, IAPP (Jan. 20, 2016), https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-5-profiling. It should be noted that these three activities illustrate how individuals might be owed disclosure or the ability to enforce their rights. The EU provides additional rights, such as the right to erasure, right to access and correct incorrect data, and ability to revoke previously given consent at any time. *See* GDPR, *supra* note 78, at 37, 43. These rights also support an individual's rights with respect to automated processing. *Id.* at 46. The GDPR also makes clear that coercive practices, for example not providing a service unless data unrelated to provisioning the service is provided (as is often seen in adhesive agreements in the United States), are not permitted. *Id.* at 8. This means that an individual may have the opportunity to still receive a service without providing additional personal information for profiling purposes.

297. *See* Article 29 Data Protection Working Party, *supra* note 163, at 9. Although the EU is still determining what is meant by "legal effects" or "similarly significant effects" in Article 22(1) of the GDPR, this is likely meant to apply to a portion of all automated processing and profiling activities, rather than all such activities.

rights and freedoms of natural persons: employment, government benefits, housing, and other financial opportunities.

The EU's Article 29 Working Party (WP), or the Data Protection Working Party, has written guidelines to further detail the meaning and application of GDPR. In its *Guidelines on Automated Individual Decision-making and Profiling for the Purpose of Regulation 2016/679*, the WP provides four examples of legal effects to illustrate when disclosure and due process-related activities apply: (1) entitlements or denial of social benefits granted by law (child or housing benefit), (2) refused border entry, (3) subjection to increased cybersecurity measures or surveillance activities, and (4) automatic disconnection from key services (e.g., phone service).[298]

Similar effects include those specifically included in the GDPR's Recital 71, such as discrimination through automated e-recruiting or automatic refusals of credit applications, as well as obtaining credit to purchase a product or obtaining a mortgage.[299] Specifically, marketing profiling is unlikely to trigger additional obligations, though this is dependent on the "characteristics of the case," including intrusiveness, expectations of individuals, method of advertising delivery, and whether individuals are especially vulnerable.[300] In all, the WP's guidelines provide useful ideas to appropriately tailor when automated processing activities should and should not receive enhanced process scrutiny.

Despite more advanced developments around automated decision-making and data-subject profiling, the GDPR has not evolved traditional notions of notice and consent to adapt to modern data processing and transfer themes. Rather, the GDPR has reinforced traditional, time-bound conceptions of notice prior to processing and explicit consent when other legal bases for processing cannot be met, many of which would be fundamentally incompatible with consumer IoT.[301] In addition to inflexibility around notice and consent conceptions, the WP has advanced an "impossibility" standard for anonymization, making data that is partially identifiable nearly impossible to use without explicit consent.[302] Even the act of anonymizing from identifiable personal data may require data-subject consent prior to anonymization.[303]

---

298. *Id.* at 10.
299. *Id.* at 11.
300. *Id.*
301. MICHAEL MORAN & TIM PANAGOS, MICROSHARE, IOT AND GDPR: A DATA CONVERGENCE THAT PITS THE BOLD AGAINST THE CAUTIOUS (2018), https://microshare.io/wp-content/uploads/2018/02/GDPRWhitepaperFeb2018.pdf.
302. *See* GDPR, *supra* note 78, at 37; *see also* Article 29 Data Protection Working Party, *supra* note 163 (establishing specific conditions for explicit consent).
303. *See* GDPR, *supra* note 78, at 4, 36. A variety of legal bases may be used, depending on the circumstance. When consent is the primary legal basis for processing under EU law, anonymization (a processing activity requiring a legal basis) will likely also require disclosure of intent to anonymize data and, therefore, consent.

The NIS Directive has additionally established, for critical infrastructure sectors, a robust cybersecurity framework. Critical infrastructure sectors include "essential services," such as: healthcare, banking, financial market infrastructures, energy, transportation, water, and digital infrastructures.[304] The NIS Directive requires more robust cybersecurity measures, as well as information cybersecurity protection for emergency preparedness and business continuity, which ensure continuous operation.[305] Despite these positive developments for privacy and cybersecurity generally, it is not yet clear to what extent these laws will translate effectively to IoT device manufacturing.

The EU legal framework for regulating algorithmic decision-making, privacy, and cybersecurity has established important expectations for organizations processing EU resident data. The United States could adapt some of these requirements, while creating a balanced IoT regulatory model that embraces a nontraditional privacy model and relies more heavily on due process considerations and additional opportunities for adjudicatory processes.

IV. DEVELOPING A LEGAL FRAMEWORK FOR IOT DEVICES

A comprehensive IoT legal framework could reduce potential consumer risk, ensure market consistency, and improve consumer trust. However, proposals for regulatory changes must consider how consumer and technology evolution may influence market development, what self-regulations an industry may choose to employ, and develop a legal framework that balances investment in preventative measures with adjudicatory relief.[306] As a variety of global studies have acknowledged, legal schemes must balance incentives to advance data-driven, efficient economic goals with appropriate consumer protection.[307]

---

304. *See* TSCHIDER, *supra* note 89, at 270.

305. Directive 2016/1148, of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 O.J. (L 194) 1, 6, 17, 19, 21–22.

306. *See, e.g.*, Glen Hepburn, Org. for Econ. Co-Operation & Dev. [OECD], *Alternatives to Traditional Regulation*, at 5–6, 33, https://www.oecd.org/gov/regulatory-policy/42245468.pdf (describing OECD models for market development and regulation outside of legal regulation).

307. *See generally* Gloria González Fuster & Amandine Scherrer, Directorate-General for Internal Policies, *Big Data and Smart Devices and Their Impact on Privacy*, PE 536.455, at 5 (Sept. 21, 2015), http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf (describing the market and legal considerations for the big data and device economy, as well as potential impacts on civil rights for EU residents). Although not explored in detail here, challenges regarding global trade with countries or regions that recognize privacy as a civil right and prioritize data collection, use, processing, and transfer transparency should be addressed in considering international trade, in particular cross-border sales of IoT devices with services provided from a variety of locations.

A. Policy and Regulation Timing

Adam D. Thierer has described policy models in relation to IoT, including the "permissionless innovation" principle and the "precautionary principle."[308] Thierer describes these principles as satisfying different positive policy benefits: the permissionless innovation principle encourages technology growth, in particular for the market to experiment before establishing limitations on technology use.[309] Conversely, the precautionary principle requires slowing down innovation to appropriately manage and limit risk to the public.[310] The rapid evolution of IoT in recent years has pushed towards a permissionless policy default; however, academics have cautioned against this model.[311] An ideal model for early-state IoT where risks are sufficiently understood, yet innovation is most desirable, should adopt a position between permissionless and precautionary states.

In addition to regulatory timing, regulations may impact IoT market development. Because many manufacturers have embarked on a new development effort in IoT devices and still must determine needed infrastructure and implementation details, barriers to market entry are still unknown. If a precautionary regulatory framework discourages entry into a market that could result in significant growth potential, higher barriers to entry could diminish competition, especially from small businesses or start-ups, which ultimately benefit consumers with high-value or low-cost goods.[312]

Consumers should also have some choice in relation to IoT devices, depending on the risk posed. While free market conditions may be appropriate for circumstances when the consumer can distinguish product differences and understand service details, other circumstances could require additional transparency. Indeed, privacy law should avoid paternalistic tendencies when consumers can effectively bargain to make noncoercive decisions.[313] However, hidden data practices, confusing features, and latent issues that *do* introduce substantial risk may require le-

---

308. *See* Thierer, *supra* note 14, at 42–45.

309. *See id.* at 44.

310. *Id.* at 43.

311. *Id.* at 48. Thierer describes Professor Scott R. Peppet's article, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, arguing for urgency in regulating IoT. *Id.* (quoting Peppet, *supra* note 56, at 165). Professor Ryan Calo has similarly criticized a lack of regulation due to digital market manipulation, or power asymmetries between consumers and manufacturers, which over time lead to consumer irrationality. Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 999 (2014).

312. *See* Leora Klapper et. al., *Entry Regulation as a Barrier to Entrepreneurship*, 82 J. FIN. ECON. 591, 593–94 (2006) (analyzing market conditions in Europe and concluding that higher regulation at business entry results in market participation from larger entities to the disadvantage of smaller entities).

313. *See* Solove, *supra* note 156, at 1881–82. Daniel Solove has noted the tendency towards overregulation in the EU by assuming consumers cannot make decisions with respect to their own information. *Id.* at 1897–98.

gal intervention, either through statutory requirements or adjudicatory processes.

B. Statutory Considerations

Statutory requirements, whether federal or state, should apply to regulatory topics where self-regulation and market forces do not effectively address risk.[314] Market forces may not drive change when consumers do not fully appreciate the risk or do not have the expertise to determine whether a product offering provides adequate protection. For IoT technologies, privacy concerns may fit this description because manufacturers currently do not standardize privacy requirements across industries for technology implementations in the United States.[315] IoT devices may pose substantial risk to consumers and their property, often risk that may be difficult to anticipate or understand prior to a significant compromise.[316] Discrimination, privacy, and cybersecurity risks will likely require different processes for effectively balancing beneficial market conditions with protecting consumers.

1. Discrimination

Legally protected interests should narrowly define discrimination rather than deferring to general fairness principles. These interests for protected groups might include statutory protection from discriminatory behavior coupled with an ability to civilly recover for statutory violations. For IoT, regulatory approaches should require extreme scrutiny when soliciting, collecting, or including SPI data elements in infrastructure and results of IoT features, including AI utilities. Restricted use applicable to SPI should extend to proxies for SPI with high risk of misuse, as with algorithmic decision-making directly affecting availability of public services or negatively impacting economic prospects. These interests must also afford appropriate due process transparency and recovery for legally protected rights, such as deprivation of property interests like public or government benefits, availability of housing, or real-property interests.

Risks resulting from discriminatory decision-making and potential deprivation of due process rights could be addressed by restricting sensitive data solicitation and additional data management activities, such as

314. It should be noted that, as we have observed in data breach notification statutes, states have often responded first to develop statutory requirements where state residents are affected. *See, e.g.*, Jessica Davis, *Colorado Passes Data Protection Law Requiring Breach Notification Within 30 Days*, HEALTHCARE IT NEWS (June. 7, 2018, 1:08 PM), https://www.healthcareitnews.com/news/colorado-passes-data-protection-law-requiring-breach-notification-within-30-days (noting that Colorado is one of several states passing data privacy laws "in the wake of" data breaches such as those affecting Verizon and Equifax).

315. *See supra* Part II and accompanying notes. A variety of highly specialized laws apply to specific relationships and data types within a particular sector. However, no omnibus law currently establishes a foundational baseline for IoT device data as a whole.

316. *See supra* Part II and accompanying notes.

transfer, data set recombination, or sales. Data solicitation of this type could be subject to use restrictions, wherein these data may only be collected when strictly necessary for the service provided. If highly sensitive data uses are restricted, yet the data collected is clearly necessary to the service provided, notifying consumers may be less critical to privacy interests. SPI data elements (and their proxies) could be specifically enumerated, starting with the most popular data elements listed in state data breach notification laws and antidiscrimination statutes.

Scholars have proposed algorithmic transparency, presumably communicated via a privacy notice model or upon inquiry, as one option for improving algorithmic fairness.[317] Transparency, however, could include transparency about automated processing or transparency about the algorithm. Legal frameworks applicable to consumer IoT devices should balance market interests, including harms of trade secret or other confidential disclosures and the difficulty of disclosure (as in ML algorithmic explanation), with consumer fairness interests.[318]

When IoT device infrastructures leverage algorithmic decision-making, algorithms may be incapable of human explanation because AI created them from big data stores without human training or intervention.[319] These unsupervised learning models, a learning type that does not involve human algorithmic creation at all, will likely adopt machine shorthand languages that are unreadable or unintelligible to humans.[320] If organizations cannot communicate algorithms effectively, privacy notices describing algorithmic calculation would be unlikely to improve transparency goals.

Automated processing activities posing "high risk" to consumers due to potential for discriminatory or unfair results should be disclosed by manufacturers prior to collecting data via IoT devices and require IoT users to explicitly consent to processing activities. For example, activities collecting SPI like a consumer's race and sexual orientation while using automated processing could present high risk to a consumer. However, automated processing activities, including the algorithms them-

317. *See* Crawford & Schultz, *supra* note 101, at 125–26. Crawford and Schultz advocate for algorithmic transparency and ability to intervene, albeit for more serious matters involving due process, rather than consumer IoT products that presumably do not pose as much risk to an individual's economic prospects. *See id.* at 124.

318. *See* W. Nicholson Price II, *Regulating Black-Box Medicine*, 116 MICH. L. REV. 421, 471–72. Price describes the potential harms of revealing secret and proprietary data, which could harm innovation. Price focuses on FDA operations and disclosure to the FDA, and presumably the same principle could apply to detailed consumer disclosures, assuming that manufacturers could effectively communicate algorithm functionality in accessible terms. *See id.*

319. *See* Adrienne LaFrance, *What an AI's Non-Human Language Actually Looks Like*, ATLANTIC (June 20, 2017), http://www.theatlantic.com/technology/archive/2017/06/what-an-ais-non-human-language-actually-looks-like/530934.

320. *See id.*

selves, need not be disclosed in detail to alert a consumer to their presence.

As a tradeoff for some opacity, consumers could control manufacturer rights with respect to algorithmic decision-making, such as the ability to receive information about automated decisions taken, the ability to object to automated processing, and the ability to correct information that may lead to an unfair result.[321] Where disclosure is clear and not entangled in privacy notice language that is easily ignored and consumers have opportunities to enforce their rights in a timely manner to prevent harm, downstream recovery may be less necessary. Self-help mechanisms, such as reviewing automated decision information or objecting to automated processing, improve efficiency for the system by reducing time, effort, and expense in the courts.

These approaches do increase transparency and consumer control, which are beneficial both for historically marginalized groups and for consumers who might individually suffer an injurious result due to inaccurate algorithmic decision-making. Consumers benefit from objection and correction as a form of procedural self-help, but objections and corrections improve algorithm-based IoT systems. Objections and corrections address the common criticism of automated decision-making "throughput," or the ability to correct and tune data sets and algorithms over time to increase accuracy.[322] When users interact to improve algorithmic accuracy, accuracy should improve.

When automated processing does implicate recognized legal rights, such as deprivation of property interests or criminal sanctions, effective due process procedures that consider technological deprivations become incredibly important. Crawford, Schultz, and Citron have proposed complementary techniques for enforcing due process rights.[323] These models, collectively, provide a clear direction for technological due process that applies to algorithmic decision-making. However, many of the algorithmic decisions that feed IoT functionality will likely serve general consumer interests rather than the type of decisions resulting in deprivation

---

321. This model offers an algorithmic accountability via disclosure of algorithm use. This approach could balance trade secret interests of a manufacturer while also enabling individuals to advocate for their own interests. Trade secret protection, an intellectual property interest which could be destroyed when details are shared, limits what can be shared with third parties, including consumers. *See* Price, *supra* note 318, at 472. Providing information about the presence of algorithmic decision-making and offering opportunities for meaningful response retains trade secret protection while improving transparency.

322. *See generally* Chérif Mballo & Vladimir Makarenkov, *Assessing the Performance of Machine Learning Methods in High-Throughput Screening* (2010) (conference paper), https://www.researchgate.net/profile/Cherif_Mballo/publication/268149301_Assessing_the_performance_of_machine_learning_methods_in_high-throughput_screening/links/54b561ac0cf28ebe92e56d92/Assessing-the-performance-of-machine-learning-methods-in-high-throughput-screening.pdf (proposing appropriate methodologies to increase throughput and improve accuracy in ML).

323. *See* Crawford & Schultz, *supra* note 101, at 121–28.

of property interests or criminal sanctions. For example, algorithms used in children's toys might benefit from transparency-enabling processes, but will not likely result in deprivation of property interests.

Manufacturers will also benefit from self-monitoring activities, which would provide ample best-practice evidence in the event of a legal action. Manufacturers should consider developing models and testing procedures specific to protected data elements and their proxies using ongoing computational verification.[324] Computational verification could run potential IoT device behavior based on these data to anticipate where discriminatory impacts might result. Manufacturers should also record legitimate justifications when collecting SPI for these purposes or using proxies for these data.

2. Privacy

As with automated processing, a regulation restricting data use should balance consumer interests with market maturity and interests. IoT devices will likely produce and consume large data volumes, yet most data should not be highly sensitive or identifiable. SPI could be restricted to necessary use, but statutory protection should permit flexible, free use of nonsensitive personal data to allow for statutory evolution over time and enhance market development. Broad data use could be checked by cybersecurity requirements protecting data to reduce the risk of injury. Like discrimination prevention activities, manufacturers should evaluate data sets as a whole not only to communicate specific SPI collected but also to evaluate data sets that could serve as proxies for SPI.

Regulations could incentivize use of PET, such as differential privacy methodologies, pseudonymization, de-identification, or encryption, which would reduce high-cost obligations, such as data breach notification.[325] Similar to HIPAA's encryption safe harbor, which absolves CEs from having to notify individuals in the event of a data breach, may reduce risk to such an extent that additional privacy obligations may be less necessary.[326] While PET might not dramatically reduce risk to consumers in all circumstances, when appropriately applied to holistic data sets rather than specific data elements, PET will likely reduce privacy and cybersecurity risks. However, encryption and other PETs may come

---

324. *See* Ford & Price, *supra* note 5, at 18. Although computational verification is presented by Ford and Price as a method for clinical trials performed by a third-party regulator, the same method could be used to reduce proxy-based discrimination when applied by an auditing capacity at a manufacturer.

325. *See generally* MARIT HANSEN ET AL., EUROPEAN UNION AGENCY FOR NETWORK AND INFO. SEC. (ENISA), READINESS ANALYSIS FOR THE ADOPTION AND EVOLUTION OF PRIVACY ENHANCING TECHNOLOGIES 7, 10 (2015), https://www.enisa.europa.eu/publications/pets (describing various technologies used to enhance privacy).

326. *See* U.S. Dep't of Health & Human Servs., *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, HHS.gov, https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html (content last reviewed July 26, 2013).

in a variety of different protection levels depending on how they are implemented.[327] For example, one encryption protocol may be easily broken, whereas other encryption protocols may take hundreds of years to break. For an IoT manufacturer to enjoy any potential reduction of other privacy obligations, qualifying PET should meet threshold requirements established by the National Institute of Standards and Technology (NIST).[328]

The FTC also has an opportunity to consider and certify alternative models that operationalize dynamic user preferences across IoT manufacturers. For example, user controls on mobile devices, such as on/off slide settings for sharing specific information (access to photos or contacts) or specific actions (connect to mobile network), could be implemented easily from a common portal or on devices with limited screen real estate.[329] The benefit to user-managed preferences includes the ability to change preferences at any time. With a shared interface, users could potentially change granular preferences across products simultaneously for secondary uses like third-party data sharing, data transfer restrictions, and data sales. This type of preference management could potentially serve as a vehicle for enhanced features or other value propositions if manufacturers seek to collect additional data.[330]

Another IoT market-based solution, the use of personal data stores, shows some promise. A personal data store houses data from a variety of devices and origins for an individual. Benefits include standardized data storage, identified data points of origin, records of data requests, and overall data captured. Having a central, common repository not only could improve access needs and streamline data requests but also could allow users or data subjects to make decisions regarding their data, such as limitations on data sharing to particular third parties (e.g., data brokers).[331] User-selected limitations could include rule sets, including re-

327. *Guide to Cryptography*, OWASP FOUND., http://www.owasp.org/index.php/Guide_to_Cryptography (last modified June 13, 2018).

328. *See, e.g.*, *Privacy-Enhancing Cryptography*, NAT'L INST. STANDARDS & TECH. (Feb. 7, 2017), https://csrc.nist.gov/Projects/Privacy-Enhancing-Cryptography (defining one technology currently under discussion by NIST).

329. Increased control or perception of control might also have the positive market result of increased data sharing and, following, improved products (and IoT devices and associated infrastructure will depend on quality data and substantial data volume). *See* Laura Brandimarte et al., *Misplaced Confidences: Privacy and the Control Paradox*, 4 SOC. PSYCHOL. & PERSONALITY SCI. 340, 341, 345 (2012) (concluding that voluntary data sharing or publication results in greater data sharing volume, regardless of the quality of disclosure).

330. It should be noted that IoT devices typically exhibit a different value proposition by providing a *thing*, an item of value. Data processing for primary purposes seeks to facilitate device functionality. Additional personal data collection, therefore, does not figure into the value proposition as heavily as with mobile apps or similar "free" models. For this reason, it is unlikely that markets would suffer substantially from restricting SPI processing somewhat and permitting user-controlled preference management.

331. In part, for-profit organizations already have leveraged the concept of big data storage via a third-party provider. Big data providers including Google, Amazon, and others provide cloud

quiring data shared to follow an anonymization or de-identification procedure, which could be certified by an accreditation body. Rules could also force additional consent when requests exceed predetermined settings. A user or data subject who prefers stricter control over data use limitations could require notification and explicit consent prior to expanded data use.

3. Cybersecurity

The problematic state of cybersecurity has led to more frequent data breaches across industries and products. However, too much technical specificity could lead to less mature cybersecurity implementations for more mature organizations. The FTC could develop guidelines that explicitly incorporate or reference appropriately rigorous NIST technical requirements to describe administrative and technical measures necessary for protecting information.[332] The FTC could also incentivize compliance with these guidelines by providing immunity from civil action when a manufacturer can prove it meets NIST requirements at the time of alleged consumer injury or data breach.

Any regulation should also address specially required cybersecurity measures, which might merit enhanced cybersecurity application. A regulation should require manufacturers to increase cybersecurity on high-risk data processing or high-risk devices, including: when collecting SPI or proxies for SPI; designing devices for children or other vulnerable populations; selling devices with substantial inherent product safety concerns (thermostats, connected locks, or ovens); and implementing unsupervised learning systems.

A high-risk data and device model reduces legal obligations for some manufacturers while preventing more substantial harms, a risk management regulatory model. IoT devices that collect SPI will be more likely overall to experience a cyberattack and children or other vulnerable populations may be less able to engage in self-help. For these reasons, manufactures could adopt a sliding-scale model that requires extensive cybersecurity requirements for high-risk environments, yet permits the market to regulate IoT devices posing substantially less risk to consumers.

4. Working Towards a Proposed Regulatory Model

The pervasive nature of connected technology across a wide variety of devices, including home applications, personal wearables, children's toys, and any host of other technologies; requires a broad-stroke regula-

---

services to customers today via massive data centers, albeit in logically or physically segregated cloud services.

332. *See Publications*, NAT'L INST. STANDARDS & TECH., https://www.nist.gov/publications (last visited Oct. 8, 2018).

tory approach applicable to all commercial entities manufacturing IoT devices. Where such manufacturers do not have a substantial business presence in the United States, a regulation could alternatively establish requirements for distributors to sell products in the United States. A regulatory model should similarly require manufacturers to ensure third-party suppliers working as subcontractors adhere to the same requirements.[333] For IoT devices more generally, an IoT regulation should establish a base, floor level of requirements, while specifying the administrative oversight needed for higher safety and sensitivity devices, such as medical devices or connected cars.

When regulating a large manufacturing base, regulatory authorities should address and develop new requirements while maintaining current, useful regulatory frameworks, while maintaining existing regulatory frameworks where useful. Although several government agencies have exhibited interest in regulating IoT, the FTC should be responsible for IoT regulation because it has the most experience in regulating privacy and cybersecurity across industries.[334] Still, the development of consumer products might benefit from engagement of the CPSC, especially in developing guidelines for manufacturers.[335] Manufacturers might benefit from a combined approach for investigatory and enforcement models: the FTC could develop guidelines and rules, while the CPSC fields complaints and conducts investigations. The collaboration of two large administrative agencies could anticipate potential privacy and cybersecurity issues while simultaneously leveraging a longstanding products liability regulatory framework.

Despite the unavailability of civil recovery via a private right of action under most privacy laws, the physicality of IoT and potential for safety issues makes a strong argument for available civil recovery and administrative fines when noncompliance is not likely to result in recovery. Available civil recovery actions could include breach of contract actions related to data processing and failure to disclose SPI collection or

---

333. The EU has created frameworks for third party enforcement, such as standard or model contractual clauses, and HIPAA requires use of a Business Associate Agreement (BAA). *See* Commission Decision 2010/87, of 5 Feb. 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries Under Directive 95/46/EC of the European Parliament and of the Council, 2010 O.J. (L 39) 6, 8, 10; U.S. Dep't of Health & Human Servs., *Business Associate Contracts*, HHS.GOV (Jan. 25, 2013), https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html. Despite existing models for more rigid third-party management, direct liability for the actions of third parties on behalf of the principal might effectively push downstream enforcement in the United States in products liability.

334. *See* Solove & Hartzog, *supra* note 263, at 586 (describing the development of FTC common law through privacy-focused cases).

335. The CPSC has communicated a desire to work with experts and attorneys in furtherance of developing appropriate policy and addressing potential hazards. *See Consumer Product Safety Administration Seeks Collaboration in Managing Internet of Things*, ABA, (May 12, 2017, 2:34 PM), https://www.americanbar.org/news/abanews/aba-news-archives/2017/05/consumer_productsaf.html.

use, negligence per se actions illustrating poor cybersecurity practices, and products liability actions for circumstances leading to personal injuries or property damage.[336] Indeed, these bodies of common law will need further exploration and, potentially, evolution of common law and code. Manufacturer actions, in limited cases, could also trigger other due process procedures, discrimination suits, or constitutional actions. Administrative agencies, such as the FTC or CPSC, might be congressionally mandated to investigate complaints of potential injury that pose challenges for the courts though nevertheless posing risk to consumers. For example, actions related to inappropriate data handling or SPI disclosure might be difficult to prove within current understandings of the common law, such as known torts, but might be investigated by an agency.

Despite rather broad opportunities for adjudication, a regulation could include incentives for earning a complete defense to civil liability with respect to specific claims. For example, if a manufacturer meets NIST requirements, the manufacturer could have a complete defense against claims of unreasonable technical and administrative controls. Similarly, manufacturers using a common preference management system might avoid general privacy liability, so long as they honor preference settings in a preference management system.

CONCLUSION

Modern IoT present more than a prospective concern for consumers: IoT now dominate connected devices worldwide and will only continue to grow in volume. IoT devices now incorporate advanced algorithms and ML utilities, while relying on big data infrastructures. The ubiquity of IoT devices paired with the ubiquity of data present more substantial issues than previously explored. Concerns regarding discrimination, privacy, and cybersecurity demonstrate the multifaceted nature of providing reliable and useful service: a need for safeguarding individuals rights, protecting consumer safety, and ensuring appropriate mechanisms exist for consumer self-help.

The United States does not, today, have an effective legal approach for addressing IoT concerns. However, regulating IoT requires much more than passing a federal law. Architecting an appropriate IoT risk management solution demands baseline legal requirements, industry self-regulation, and market interests. To ensure the IoT market flourishes, it is

336. *See, e.g.*, Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, 50 MICH. J. L. REFORM 913, 917–18 (2018) (describing factors influencing whether manufacturers should reasonably be held liable for cyberattacks on IoT); Stacy-Ann Elvy, *Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond*, 44 HOFSTRA L. REV. 839, 844–45 (2016) (proposing changes to UCC Article 2 provisions, such as revisiting unconscionability provisions in light of information asymmetry).

critical to develop a workable solution that addresses implicit IoT risks yet allows enough flexibility to enhance IoT growth.