2018

Commodifying Consumer Data in the Era of the Internet of Things

Stacy-Ann Elvy
New York Law School, selvy@nyls.edu

Recommended Citation
Boston College Law Review, Vol. 59, Issue 2 (February 2018), pp. 423-522

COMMODIFYING CONSUMER DATA IN THE ERA OF THE INTERNET OF THINGS

STACY-ANN ELVY

COMMODIFYING CONSUMER DATA IN THE ERA OF THE INTERNET OF THINGS

STACY-ANN ELVY*

Abstract: Internet of Things ("IoT") products generate a wealth of data about consumers that was never before widely and easily accessible to companies. Examples include biometric and health-related data, such as fingerprint patterns, heart rates, and calories burned. This Article explores the connection between the types of data generated by the IoT and the financial frameworks of Article 9 of the Uniform Commercial Code and the Bankruptcy Code. It critiques these regimes, which enable the commodification of consumer data, as well as laws aimed at protecting consumer data, such as the Bankruptcy Abuse Prevention and Consumer Protection Act, various state biometric data statutes, and the Health Insurance Portability and Accountability Act. This Article contends that in addition to privacy policies, financial frameworks can also play a critical role in facilitating the transfer and disclosure of consumer data in a manner that is opaque and potentially harmful to consumers. Furthermore, existing privacy frameworks that rely heavily on a notice and choice model and the provisions of a company's privacy policy to determine the level of protection given to consumers, and which may not always apply to IoT companies, do not effectively safeguard consumers in the IoT setting. This Article proposes several solutions to engender movement away from an overreliance on the notice and choice model and the terms of privacy policies, and to reduce the various moments of data disclosure authorized by financial frameworks. It also offers ways to preserve the value of IoT data as a source of financing for companies while simultaneously protecting the privacy of consumers.

INTRODUCTION

The Internet of Things ("IoT") has been described as "the next evolution of the Internet" and it is expected to usher in a new economic age with "changes rivaling the industrial revolution."[1] However, the rapid "digitali-

* Professor of Law, New York Law School (J.D., Harvard Law School; B.S., Cornell University). For helpful feedback, comments or insights, I am grateful to Paul Schwartz, Xuan-Thao Nguyen, Pamela Foohey, Edward Janger, Sharona Hoffman, Stephen Sepinuck, Heather Hughes, Juliet Moringiello, Jim Hawkins, Lucy Thomson, Cedric Powell, Sudha Setty, Audrey McFarlane, Nordia Elvy, Euklyn Elvy, Richard Chused, Gerald Korngold, Robert Blecker, and participants at the 2017 Property Implications of the Sharing Economy Conference at Penn State Law School.

[1] DAVE EVANS, THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 2 (Apr. 2011), https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf [https://perma.cc/CMR6-5KS7]; Kenie Ho, *Protecting the Revo-*

zation of our physical world" raises significant concerns for consumers.[2] In 2016, researchers at the University of California, Berkeley Center for Long-Term Cybersecurity ("Berkeley Center") published a report that evaluated five cybersecurity scenarios that could potentially occur in 2020.[3] Two of the most alarming scenarios involve: (1) a financial crisis in which companies sell their customer "data assets" to third parties (including unwittingly selling to parties that would use consumer data for perverse purposes), while companies become increasingly vulnerable to cyberattacks, and (2) the ubiquitous use of wearable devices that collect and monitor "real-time" biometric and health-related data, including emotional state and hormone levels, and the widespread use of these data to control and manipulate consumers.[4]

Consumers are already experiencing the effects of the "new normal" of 2020 identified by the Berkeley Center, in which companies routinely suffer from cyberattacks.[5] In 2016, Dyn, a business that "manages crucial parts of the [I]nternet's infrastructure," reported a serious attack on its systems that disrupted access to various websites, such as Twitter, Netflix, and the New York Times.[6] The hackers manipulated vulnerable IoT devices to initiate the

---

lution: Internet of Things Trade Secrets, LAW.COM: INSIDE COUNSEL (Oct. 6, 2016, 6:04 AM), http://www.law.com/insidecounsel/2016/10/06/protecting-the-revolution-internet-of-things-trade/ [https://web.archive.org/web/20180103172900/https://www.law.com/insidecounsel/2016/10/06/protecting-the-revolution-internet-of-things-trade/?slreturn=20180003122859]. The Internet of Things ("IoT") has been described as a network of connected products that accumulate and transfer data over the Internet. AIG, THE INTERNET OF THINGS: EVOLUTION OR REVOLUTION? 6–7 (2015), http://www.aig.com/content/dam/aig/america-canada/us/documents/business/casualty/aigiot-english-report.pdf [https://perma.cc/BA7X-Y9VV].

[2] JESSICA GROOPMAN & SUSAN ETLINGER, CONSUMER PERCEPTIONS OF PRIVACY IN THE INTERNET OF THINGS: WHAT BRANDS CAN LEARN FROM A CONCERNED CITIZENRY, ALTIMETER 2 (June 2015), http://www.altimetergroup.com/pdf/reports/Consumer-Perceptions-Privacy-IoT-Altimeter-Group.pdf [https://perma.cc/KP7V-H9LF]. Business Insider reports that "[n]early $6 trillion will be spent on IoT solutions over the next five years." John Greenough & Jonathan Camhi, *Here Are IoT Trends That Will Change the Way Businesses, Governments, and Consumers Interact with the World*, BUS. INSIDER (Aug. 29, 2016, 10:18 AM), http://www.businessinsider.com/top-internet-of-things-trends-2016-1 [https://perma.cc/73LE-LQY3].

[3] U.C. BERKELEY CTR. FOR LONG-TERM CYBERSECURITY, CYBERSECURITY FUTURES 2020, at 1 (2016), https://cltc.berkeley.edu/wp-content/uploads/2016/04/cltcReport_04-27-04a_pages.pdf [https://perma.cc/M523-YEZE].

[4] *Id.* at 6–7. As used in this Article, the term "health-related data" refers to data associated with the mental, emotional, or physical well-being and health of individuals, such as calories burned, sleep patterns, glucose levels, and the like. As used in this Article, the term "biometric data" refers to biometric identifiers, such as voice and face prints; scans and images of biometrics, such as fingerprint scans; other data related to and that can be transformed into biometric identifiers, such as a recording of an individual's voice or a photograph of an individual; and the authentication codes, templates, text, or mathematical representations associated with any such data.

[5] *Id.* at 9–10.

[6] Nicole Perlroth, *Hackers Used New Weapons to Disrupt Major Websites Across U.S.*, N.Y. TIMES (Oct. 21, 2016), https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html [https://perma.cc/N95B-H2FX].

attack.[7] Similarly, in 2017, Equifax reported that a breach of its servers revealed the sensitive data, including "social security numbers and birth dates," of millions of consumers.[8]

Customer information generated from consumer purchase and use of goods and services is a prized asset.[9] Companies' "use of customer databases has become a critical strategy to successful business."[10] The brisk expansion of the IoT will increase the consumer data contained in existing customer databases exponentially. The vulnerabilities associated with IoT devices and the speed at which companies can collect, analyze, and distribute consumer data in the IoT setting exacerbates concerns about privacy and security.[11] In the IoT context, data generation and collection does not end after the consumer purchases a device online or in a store, but instead increases once the consumer begins to use the IoT device, as well as the websites and mobile applications that are frequently required to access and operate the device. Not only will consumers' use of IoT devices and related services generate information, such as credit card numbers, names, dates of birth, and physical and email addresses, but also a wealth of new information. IoT devices can collect biometric and health-related data, such as

---

[7] *Id.*; *see also* Samuel Burke, *Massive Cyberattack Turned Ordinary Devices into Weapons*, CNN: TECH (Oct. 22, 2016, 10:37 AM), http://money.cnn.com/2016/10/22/technology/cyberattack-dyn-ddos/ [https://perma.cc/2YA9-KYCZ] (noting that the hackers used malware to control the IoT devices of consumers).

[8] Paresh Dave, *Credit Giant Equifax Says Social Security Numbers, Birth Dates of 143 Million Consumers May Have Been Exposed*, L.A. TIMES (Sept. 7, 2017, 5:25 PM), http://www.latimes.com/business/technology/la-fi-tn-equifax-data-breach-20170907-story.html [https://perma.cc/VP54-BBCF].

[9] Julia Alpert Gladstone, *Data Mines and Battlefields: Looking at Financial Aggregators to Understand the Legal Boundaries and Ownership Rights in the Use of Personal Data*, 19 J. MARSHALL J. COMPUTER & INFO. L. 313, 329 (2001) ("[C]onsumer profiles are a valuable intangible asset."); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056, 2056–57 (2004) ("The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from this trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.").

[10] Gladstone, *supra* note 9, at 329; *see also* Xuan-Thao N. Nguyen, *Commercial Law Collides with Cyberspace: The Trouble with Perfection—Insecurity Interests in the New Corporate Asset*, 59 WASH. & LEE L. REV. 37, 41 (2002) (noting that "due to the cyberspace nature" of Internet companies, their most important assets are intangibles); *Privacy*, E-COMMERCE L. REP., Aug. 2000, at 33, 33 ("For many dot coms, one of their most valuable assets, if not their most valuable asset, is their customer database.").

[11] Commentators frequently note the differences between the concepts of privacy and security. JOANNA LYN GRAMA, LEGAL ISSUES IN INFORMATION SECURITY 37 (2011) ("Information security and privacy are closely related. However, they're not the same."). Other commentators note that privacy scholars have varying definitions of the concept of privacy. Alan Rubel, *Claims to Privacy and the Distributed Value View*, 44 SAN DIEGO L. REV. 921, 923 (2007) (discussing "what is privacy"); Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1092 (2002) (delineating six different "conceptions" of privacy).

fingerprint scans, facial scans, heart rates, fitness levels, temperature, and blood sugar levels, among other things.[12] In fact, because of the IoT, "90 percent of the world's data has been generated over the past two years. Every second, over 205,000 new gigabytes are created, which is the equivalent of 150 million books."[13]

Prior to the technological advancements of the IoT, access to a consumer's health-related data was typically limited to healthcare and insurance providers. Similarly, biometric data, such as fingerprint scans, could previously be regularly accessed only by governmental entities or perhaps some employers and the banking and payments industry.[14] Today, companies, such as Apple, use biometrics in connection with their products.[15] In the IoT setting, biometric and health-related data are no longer being held primarily by a select group of traditional entities and providers. Instead, these types of data are now more ubiquitously dispersed and available to various entities—including retailers, manufacturers, and software and online companies—because of consumers' use of IoT devices, fitness applications, and other mobile applications.[16] Unlike financial information, biometric and health-related data are "more vulnerable in general as a data set

---

[12] Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 88, 98–99 (2014); Sharon Roberg-Perez, *The Future Is Now: Biometric Information and Data Privacy*, ANTITRUST, Summer 2017, at 60, 60.

[13] *See* AIG, *supra* note 1, at 2.

[14] Business Wire, *With Voice Biometrics from Nuance, Banco Santander México Customers Say "Goodbye" to PINs and Passwords, and "Hello" to a Better Banking Experience*, THESTREET (May 14, 2014, 8:00 AM), https://www.thestreet.com/story/12708042/2/with-voice-biometrics-from-nuance-banco-santander-m233xico-customers-say-8220goodbye8221-to-pins-and-passwords-and-8220hello8221-to-a-better-banking-experience.html [https://perma.cc/8B34-N7AJ]; Michele Masterson, *Barclays Deploys Nuance Voice Biometrics Solution*, SPEECH TECH. (May 8, 2013), http://www.speechtechmag.com/Articles/News/Speech-Technology-News-Features/Barclays-Deploys-Nuance-Voice-Biometrics-Solution-89506.aspx [https://perma.cc/RVG7-EZB6]; *Fingerprints and Other Biometrics*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics [https://perma.cc/3CYP-3LKZ] ("The FBI has long been a leader in biometrics. It has used various forms of biometric identification since our earliest days, including assuming responsibility for managing the national fingerprint collection in 1924."); *Street Level Surveillance*, ELEC. FRONTIER FOUND., https://www.eff.org/my/sls [https://web.archive.org/web/20170313045046/https://www.eff.org/my/sls] [hereinafter *Street Level Surveillance*] ("Fingerprints are the most commonly known biometric, and they have been used regularly by criminal justice agencies . . . .").

[15] *Street Level Surveillance*, *supra* note 14.

[16] Helen Nissenbaum & Heather Patterson, *Biosensing in Context: Health Privacy in a Connected World*, *in* QUANTIFIED: BIOSENSING TECHNOLOGIES IN EVERYDAY LIFE, 79, 83–84 (Dawn Nafus ed., 2016) (discussing examples of health-related data in the employment setting and contending that "[l]eading fitness tracking companies may cultivate new markets not only by selling their products and services directly to the public via retailers, but also by embedding them into existing health and wellness infrastructural ecosystems").

[because you can't] replace [them] like you can a credit card."[17] For data miners, advertisers, and hackers, health-related and biometric data are the "missing piece in consumer profiles."[18]

In light of the nature of Internet commerce, the most treasured asset of many businesses is "in the form of intangibles [and] [w]hen in need of capital, these companies must turn to these intangible assets, including consumer databases, to serve as collateral in secured transactions."[19] A significant source of financing for IoT start-ups comes from venture capital deals.[20] Rather than primarily obtaining equity financing, IoT companies may increasingly need to depend on traditional secured financing transactions in order to meet demands for their products and avoid potential delays associated with obtaining equity financing.[21] Traditional lenders may also insist on secured financing schemes when providing financing to new and established IoT companies. Jawbone, an IoT maker of wearable devices, raised $50 million in secured financing deals in 2013 and $300 million in 2015.[22]

---

[17] Sarah Kellogg, *Every Breath You Take: Data Privacy and Your Wearable Fitness Device*, 72 J. MO. B. 76, 76 (2016).

[18] *See id.* at 76–77.

[19] Xuan-Thao N. Nguyen, *Collateralizing Privacy*, 78 TUL. L. REV. 553, 576–77 (2004) [hereinafter Nguyen, *Collateralizing*].

[20] Lindsey O'Donnell, *The 10 Most Active VC Investors in the Internet of Things*, CRN (July 30, 2016, 10:00 AM), http://www.crn.com/slide-shows/networking/300081526/the-10-most-active-vc-investors-in-the-internet-of-things.htm [https://perma.cc/BWX7-89CB] ("Hype around the Internet of Things is growing, and venture capital investors are increasingly getting into the game as more IoT-based startups emerge with innovative technology."); *Funding to IoT Startups Has More Than Doubled in Six Years*, CB INSIGHTS (Nov. 10, 2015), https://www.cbinsights.com/research/internet-of-things-startup-funding/ [https://perma.cc/GEG5-SFUT] [hereinafter *Funding to IoT Start-ups*] (describing investments in IoT start-ups and noting the most "active" venture capital investors); VERSIZON, STATE OF THE MARKET: INTERNET OF THINGS 2016, at 5 (Apr. 2016), https://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf [https://perma.cc/H8KL-ZLL8] ("According to analysis conducted by our venture capital (VC) arm, Verizon Ventures, we estimate that consumer IoT startups raised 15% more VC funding than enterprise-focused startups in 2014.").

[21] Dan Primack, *Exclusive: Jawbone Raises More Than $100 Million*, FORTUNE (Sept. 12, 2013), http://fortune.com/2013/09/12/exclusive-jawbone-raises-more-than-100-million/ [https://perma.cc/8AG2-LKWB] (discussing one IoT company's issues with meeting consumer demands for its products and concerns about the length of time needed to acquire equity financing); *see also* Andrew M. Kaufman, *Counseling the Financially Distressed Technology Company: Finding and Preserving Value in E-Commerce Assets*, *in* UNDERSTANDING ELECTRONIC CONTRACTING 2002: THE IMPACT OF REGULATIONS, NEW LAWS & NEW AGREEMENTS 697 (PLI Intellectual Property Course Handbook Series No. G-697, 2002) (discussing technology companies' reliance on equity financing); *Funding to IoT Start-ups*, *supra* note 20 (discussing IoT funding).

[22] Katie Benner, *Jawbone Gets a Loan and a Leash*, BLOOMBERG (May 18, 2015, 7:46 PM), https://www.bloomberg.com/view/articles/2015-05-18/jawbone-s-latest-partner-is-a-lender-not-an-equity-investor [https://perma.cc/9A7X-L3VZ] (noting that the $300 million debt financing obtained by Jawbone "is secured by Jawbone's current and future licenses, intellectual property, royalties, accounts receivable and revenue from IP or licenses"); Rachel Metz, *Jawbone's New Wristband Adds You to the Internet of Things*, MIT TECH. REV. (Nov. 13, 2013), https://www.technologyreview.

IoT companies, such as I.D. Systems, have used their customer lists as collateral in asset based financing deals.[23] As IoT companies begin to discover the value of IoT data as an asset, it is only a matter of time before they begin to further exploit their customer databases, particularly when subsequent rounds of financing are needed beyond the start-up phase. However, any potential commodification of consumer generated data under Article 9 ("Article 9") of the Uniform Commercial Code ("UCC") may have significant consequences for consumers.

Consider an IoT company with a customer database that consists of names, phone numbers, addresses, fingerprint and retina scans, blood pressure levels, and other types of biometric and health-related data obtained from consumers' use of IoT devices, services, and related mobile applications. If the company uses its database as collateral to obtain financing from a lender, the secured financing rules contained in Article 9 permit the secured lender to sell the collateral to satisfy the company's debt in the event of a default.[24] Thus, consumers may find that with a simple purchase of an IoT device and use of the accompanying services and software, such as websites and mobile applications, their immutable biometric and health-related data, along with their names and addresses, will be offered for sale by a secured lender if the manufacturer of the device fails to pay back the loan. Of course, companies may also disclose the biometric data of consumers to third parties in non-Article 9 transactions.[25] For instance, Take-Two Interactive Software, a company that collects "facial scans of gamers," has been accused of distributing the facial data of its users.[26]

To date, three states have adopted statutes that broadly and definitively address companies' collection, transfer, and use of biometric data.[27] Alt-

---

com/s/521606/jawbones-new-wristband-adds-you-to-the-internet-of-things/ [https://perma.cc/774K-YPDK] (discussing Jawbone's production of a wearable IoT device that, along with the "associated smartphone software," can track "exercise, sleep patterns, and other activity"); Primack, *supra* note 21 (noting that the $50 million of funding raised by Jawbone "is an asset-based loan provided by J.P. Morgan and Wells Fargo, which is secured against assets like inventory").

[23] I.D. Sys., Inc., Current Report (Form 8-K) § 3.3.1 (Dec. 18, 2015) ("To secure the full payment and performance of all of the Obligations, each Loan Party Obligor hereby assigns to Lender and grants to Lender a continuing security interest in all property of each Loan Party Obligor, . . . all . . . General Intangibles (including [intellectual property rights and] customer lists . . . .").

[24] U.C.C. §§ 9-601, 9-610 (AM. LAW INST. & UNIF. LAW COMM'N 2017).

[25] Dune Lawrence, *Do You Own Your Own Fingerprints?*, BLOOMBERG (July 7, 2016, 7:00 AM), https://www.bloomberg.com/news/articles/2016-07-07/do-you-own-your-own-fingerprints [https://perma.cc/7PKP-RTHK] (discussing companies' various uses of biometric data).

[26] William Gorta, *Face Scan Storage Not Actual Injury, Video Game Maker Says*, LAW360 (Jan. 20, 2017, 8:12 PM), https://www.law360.com/articles/883480/face-scan-storage-not-actual-injury-video-game-maker-says [https://perma.cc/XA5D-MNDQ].

[27] 740 ILL. COMP. STAT. ANN. 14/15 (West 2018); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017); WASH. REV. CODE ANN. § 19.375.010 (West 2017); Roberg-Perez, *supra* note 12, at

hough some types of biometric data monetizations may be restricted under these statutes, it is not entirely clear whether the creation of a security interest encumbering a database containing biometric information would violate the terms of these statutes. If the laws of these states do not apply to a transaction or if other state privacy laws do not clearly cover biometric data, with the possible exception of federal and state unfair and deceptive practices statutes, companies may face few, if any, restrictions on their ability to monetize biometric data. This is particularly concerning for consumers given the generally permanent nature of biometric data.

In addition to potentially using their customer databases that contain IoT consumer data in secured financing transactions, companies may also transfer their databases to third parties during a bankruptcy proceeding. When Pay by Touch, "a biometric provider," filed for bankruptcy, the company's assets included its customer database which held the "biometric templates of over two million" consumers who supplied "their fingerprints to pay for gas and groceries."[28] Further, in what may be one of the first bankruptcy proceedings involving a business that focuses exclusively on the production and sale of IoT devices and services, FiLIP Technologies, Inc. ("FiLIP")—the manufacturer of wearable IoT devices that help parents "locate and track their children"—initiated bankruptcy proceedings in 2016.[29] The sale of the company's assets to a third party was eventually approved

---

61–63 (noting that in some instances, state data breach and privacy laws that generally address personal information could apply to the collection of biometric data, but in contrast the Illinois, Texas, and Washington statutes clearly address companies' use of biometric data); Justin Kay & Brendan McHugh, *The Next Steps for Biometrics Legislation Across the US*, LAW360 (May 25, 2017, 11:55 AM), https://www.law360.com/articles/928056/the-next-steps-for-biometrics-legislation-across-the-us [https://perma.cc/NK83-HSBD] ("Washington became just the third state [after Illinois and Texas] to enact its own legislation generally governing the collection, use and retention of biometric data."); *see also* WIS. STAT. ANN. § 134.98 (West 2017) (defining personal information to include non-biometric data and biometric data and imposing notice requirements for the "unauthorized acquisition of personal information"). This Article does not address various state laws that may apply to genetic information, but rather focuses on statutes that comprehensively, exclusively, and clearly regulate the collection, transfer, and use of biometric data by "private companies." 1-3 RAYMOND T. NIMMER & HOLLY K. TOWLE, DATA PRIVACY, PROTECTION, AND SECURITY LAW § 3.09 Lexis (2017) (discussing various state and federal statutes regulating genetic information); *Street Level Surveillance*, *supra* note 14 (discussing laws that address "the use of biometrics by private companies").

[28] Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 250 (2007); Report of Consumer Privacy Ombudsman at 5, *In re* Solidus Networks, Inc., No. 2:07-bk-20027-TD (Bankr. C.D. Cal. Mar. 26, 2008) [hereinafter Pay by Touch CPO Report] (discussing that the company held biometric data during bankruptcy proceedings).

[29] *In re* FiLIP Techs., Inc., No. 16-12192 (KG) (Bankr. D. Del. Oct. 5, 2016); Matt Chiappardi, *Child Tracking Device Maker Hits Ch. 11 Seeking a Buyer*, LAW360 (Oct. 5, 2016, 8:49 PM), https://www.law360.com/articles/848760/child-tracking-device-maker-hits-ch-11-seeking-a-buyer [https://perma.cc/WL6E-8Y7N].

by the bankruptcy court.[30] FiLIP's assets included data about the children and parents that used the company's products.[31] Consider the fact that retail toy giant Toys "R" Us recently filed for bankruptcy.[32] As of the date of writing, it is not yet entirely clear whether the data of millions of consumers will be disclosed or transferred.

In another example, in 2015 RadioShack filed for bankruptcy and among the company's assets were "117 million customer records" that included personally identifiable information, such as dates of birth, credit and debit card numbers, names, and physical and email addresses.[33] Standard General eventually acquired the company and its customer database.[34] Similarly, in 2016 Sports Authority filed for bankruptcy and sold its customer database for a winning bid of $15 million.[35]

---

[30] *FiLIP Techs.*, No. 16-12192 (KG); Jeff Montgomery, *Sale of Bankrupt Kid-Tracking Firm to Smartcom OK'd*, LAW360 (Nov. 8, 2016, 7:08 PM), https://www.law360.com/articles/860757/sale-of-bankrupt-kid-tracking-firm-to-smartcom-ok-d [https://perma.cc/JWZ6-8UQ2]; Vince Sullivan, *Kid-Tracker Co.'s Ch. 11 Liquidation Plan Gets Court Approval*, LAW360 (Jan. 12, 2017, 6:20 PM), https://www.law360.com/articles/880342/kid-tracker-co-s-ch-11-liquidation-plan-gets-court-approval [https://perma.cc/EL9E-FHK2]; *Terms of Service*, FILIP, http://www.myfilip.com/terms-of-service/ [https://perma.cc/K35G-TPVM].

[31] Order (I) Approving Asset Purchase Agreement; (II) Authorizing and Approving Sale of Acquired Assets Free and Clear of Liens, Claims and Encumbrances; (III) Authorizing the Assumption and Assignment of Certain Executory Contracts; and (IV) Granting Related Relief, *In re* FiLIP Technologies, Inc., No. 16-12192 (KG) (Bankr. D. Del. Nov. 9, 2016) [hereinafter FiLIP Sale Order]; Exhibit A to Sale Approval Order at 41, *In re* FiLIP Technologies, Inc., No. 16-12192 (KG) (Bankr. D. Del. Nov. 9, 2016) [hereinafter FiLIP Sale Exhibit A] ("[u]ser data of existing current and past customers").

[32] Voluntary Petition for Non-Individuals Filing for Bankruptcy, Toys "R" Us, Inc., No. 17-34665-KLP (E.D. Va. Sept. 9, 2017); Michael Corkery, *Toys 'R' Us Files for Bankruptcy, Crippled by Competition and Debt*, N.Y. TIMES: DEALBOOK (Sept. 19, 2017), https://www.nytimes.com/2017/09/19/business/dealbook/toys-r-us-bankruptcy.html [https://perma.cc/3CMA-TCHH].

[33] Chris Isidore, *RadioShack Sale Protects Most Customer Data*, CNN: MONEY (June 10, 2015, 4:16 PM), http://money.cnn.com/2015/06/10/news/companies/radioshack-customer-data-sale/index.html [https://perma.cc/6PC9-DVC3]; Brian Schaller, *RadioShack Bankruptcy Case Highlights Value of Consumer Data*, INFOLAWGROUP LLP (June 8, 2015), http://www.infolawgroup.com/2015/06/articles/privacy-law/radioshack-bankruptcy-case-highlights-value-of-consumer-data/ [https://perma.cc/X2VW-599G].

[34] Michael Hiltzik, *The RadioShack Bankruptcy Shows You Can't Trust a Company's Privacy Pledge*, L.A. TIMES (May 19, 2015, 12:09 PM), http://www.latimes.com/business/la-fi-mh-radioshack-you-have-no-privacy-left-20150519-column.html [https://perma.cc/7D4N-PPLF] (discussing the potential acquisition of RadioShack's customer database by Standard General for $26.2 million).

[35] Kathryn Rattigan, *Sports Authority Sells Its Customer Database to Dick's Sporting Goods for $15 Million*, DATA PRIV. & SECURITY INSIDER (July 7, 2016), https://www.dataprivacyandsecurityinsider.com/2016/07/sports-authority-sells-it-customer-database-to-dicks-sporting-goods-for-15-million/ [https://perma.cc/W7Z8-2GS9]; Alex Schiffer, *In Sports Authority Bankruptcy, Customer E-mail Data Commands Hefty Sum*, L.A. TIMES (June 30, 2016, 3:05 PM), http://www.latimes.com/business/la-fi-sports-authority-auction-20160629-snap-story.html [https://perma.cc/94Q3-XQ5K]; *see In re* Sports Authority Holdings, Inc., No. 16-10527 (Bankr. D. Del. Mar. 2, 2016).

Whether a consumer's information can be easily disclosed or transferred to a third party in connection with a monetization scheme, secured financing transaction, or bankruptcy proceeding depends significantly on the terms of a company's privacy policy. Thus, privacy policies, as well as financial frameworks, can play a critical role in obscurely commodifying consumer data in ways that are potentially detrimental to consumers. This Article demonstrates the prevalence of "data propertizations" and transfers by companies in the bankruptcy context and offers predictive arguments regarding the potential role of Article 9 in facilitating IoT data trade and disclosures.[36] Consider that prior to the company's bankruptcy, Pay by Touch's privacy policy provided that its "database of biometric identifiers . . . associated with consumer fingerprints" would not be transferred to unaffiliated parties without consumer consent.[37] A consumer privacy ombudsman was appointed to evaluate privacy concerns associated with the sale of consumer data during the bankruptcy proceeding.[38] Similarly, RadioShack's privacy policy did not include a carve out covering the sale or bankruptcy of the company, and the company's ability to sell much of the information con-

---

[36] One scholar has previously addressed the assignment of consumer data in transactions governed by Article 9 ("Article 9") of the Uniform Commercial Code ("UCC"), and others have evaluated the sale of consumer data in bankruptcy proceedings. Walter W. Miller, Jr. & Maureen A. O'Rourke, *Bankruptcy Law v. Privacy Rights: Which Holds the Trump Card?*, 38 HOUS. L. REV. 777, 807–33 (2001); Nguyen, *Collateralizing*, *supra* note 19, at 576–81. This Article builds on and expands the work of these scholars, but is distinct from previous scholarship in the following ways: (1) this Article analyzes consumer data disclosures and transfers in the IoT context in light of the new types of data being generated by consumer use of IoT products; (2) unlike previous scholarship that conducted separate and distinct evaluations of consumer data disclosures and transfers under Article 9 and the Bankruptcy Code, this Article conducts a simultaneous exploration of both commercial frameworks; (3) this Article highlights the inadequacies of existing privacy frameworks in remedying consumer harms that may occur as a result of data disclosures and transfers sanctioned by Article 9 and the Bankruptcy Code. Thus, this Article considers not only the privacy concerns raised by the creation of a security interest in IoT consumer data but also issues related to the monetization of biometric, health-related, and highly sensitive data in the IoT setting as well as the sale and transfer of such intimate data to third parties in bankruptcy.

[37] Pay by Touch CPO Report, *supra* note 28, at 3–4 (describing the company's privacy policy and noting that section 363(b)(1) of the U.S. Code applied in part because the company's privacy policy provided that it would "not rent, sell, license, or lend [personally identifiable information] to third parties for advertising or marketing without" obtaining consumer consent and would not share this information "with any third parties without" the consent of consumers); *TRUSTe Recommends Destruction of More Than 3.7 Million Fingerprint Records*, TRUSTARC BLOG (Apr. 2, 2008), http://www.truste.com/blog/2008/04/02/truste-recommends-destruction-of-more-than-37-million-fingerprint-records/ [https://perma.cc/87JS-NFVC] (describing Pay by Touch's privacy policy, which limited the sale of biometric identifiers, recommendations to the consumer privacy ombudsman ("CPO"), and the subsequent decision "to destroy all of the biometric identifiers and personally identifiable information associated with those identifiers").

[38] Order Appointing Consumer Privacy Ombudsman, *In re* Solidus Networks, Inc., No. 2:07-20027-TD (Bankr. C.D. Cal. Mar. 5, 2008).

tained in its customer database was restricted.[39] In contrast, Sports Authority's privacy policy authorized the transfer of consumer data in the event of a bankruptcy or the sale of the company.[40]

As will be shown below, IoT companies routinely make statements in their privacy policies that they will not transfer or disclose consumer data, and then subsequently retract that promise by including clauses that permit the monetization of consumer data and authorize the transfer of the data to unaffiliated parties in the event of bankruptcy or sale of the company or its assets.[41]

This Article takes the position that the vast types of highly sensitive data that will be easily accessible to companies because of consumers' use of IoT devices and related services, and the potential value of IoT data as a source of financing, combined with the recent slate of bankruptcy proceedings involving consumer data, and the potential resulting harms to consumers warrants changes to existing financial frameworks that permit companies to opaquely monetize, assign, and transfer consumer data to third parties.[42]

The Article further contends that various privacy frameworks that rely heavily on a notice and choice model and the provisions of a company's privacy policy to determine the level of protection given to consumers, and

---

[39] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 783 (2016) (noting that "RadioShack's privacy policy . . . [provided] that consumers' data would not be sold, or, alternatively, that RadioShack would obtain consumers' affirmative consent before transferring their personal data," and that, ultimately, RadioShack "agree[d] to destroy most of the data, including Social Security numbers, telephone numbers, and dates of birth, and to reduce the number of data points per customer available for sale from 170 to 7"); Allison Grande, *RadioShack Bankruptcy to Test Shelf Life of Privacy Vows*, LAW360 (Apr. 3, 2015, 8:58 PM), https://www.law360.com/articles/639460/radioshack-bankruptcy-to-test-shelf-life-of-privacy-vows [https://perma.cc/6F4C-P4KC]; Laura Northrup, *RadioShack Will Not Be Selling Your Phone Number to New Owners*, CONSUMERIST (May 20, 2015, 5:25 PM), https://consumerist.com/2015/05/20/radioshack-will-not-be-selling-your-phone-number-to-new-owners/ [https://perma.cc/W6RZ-XBYH].

[40] Kate Cox, *Sports Authority Bankruptcy Means Now Dick's Sporting Goods Owns 114M Customer Records*, CONSUMERIST (July 1, 2016, 2:51 PM), https://consumerist.com/2016/07/01/sports-authority-bankruptcy-means-now-dicks-sporting-goods-owns-114m-customer-records/ [https://perma.cc/76ZW-228S] ("Sports Authority's privacy policy was a little more forward-looking than RadioShack's, from an industry perspective. Their policy stated that any data they had could be sold along with other company assets, and so it has been.").

[41] *See infra* notes 77–129 and accompanying text.

[42] There are various financial frameworks and other transactions, such as mergers and acquisitions, in which consumer data may be transferred and disclosed to unaffiliated third parties. For instance, Verizon's acquisition of Yahoo could include a transfer of consumer data to Verizon. David Lazarus, *Your Privacy: Verizon's Takeover of Yahoo Is All About User Data*, L.A. TIMES (Feb. 24, 2017, 3:00 AM), http://www.latimes.com/business/lazarus/la-fi-lazarus-verizon-yahoo-privacy-20170224-story.html [https://perma.cc/U8BS-S3S7]. However, this Article focuses only on a specific set of data transfers and disclosures permitted by privacy policies, Article 9 and the Bankruptcy Code.

which may not always apply to IoT companies or transactions, do not consistently and effectively safeguard the data of consumers in the IoT setting. The Article proposes different solutions that can be used to reduce the excessive dependency on the notice and choice model and the terms of privacy policies, as well as decrease moments of data disclosure and ameliorate potential concerns related to the assignment and transfer of consumer data as part of a bankruptcy proceeding or Article 9 transaction.

These solutions include: (a) limiting the transferability and assignability of biometric and health-related data by companies in Article 9 transactions and bankruptcy proceedings. By focusing on biometric and health-related data—some of the most highly sensitive data of consumers—this solution attempts to strike an effective balance between protecting consumer privacy and permitting companies to use other types of data for secured financing transactions (such as customer names and addresses), and (b) requiring the appointment of a consumer privacy ombudsman ("CPO") in all Article 9 transactions in which the secured party seeks to enforce its rights after default when the collateral concerns consumer data, and in bankruptcy proceedings involving the transfer of consumer data to third parties.

The remainder of this Article proceeds as follows: Part I documents the proliferation of biometric, health-related, and other types of highly sensitive consumer data in the IoT setting, and emphasizes the importance of these data to IoT companies and other entities. This Part also highlights the central role of privacy policies in authorizing the monetization and transfer of consumer IoT data to third parties. Additionally, it exposes the dangers of relying primarily on consumer consent to privacy policies to validate data collection and transfer practices. Lastly, this Part forecasts potential harms to consumers, such as exclusion, once privacy policies sanction the collection, disclosure and transfer of highly sensitive consumer IoT data in various settings, including business transactions.[43]

Part II then argues that privacy policies are not alone in enabling the disclosure and transfer of consumer IoT data, as financial frameworks can also play an instrumental role in facilitating this process. This Part examines the provisions of Article 9 and the Bankruptcy Code that permit the assignment and transfer of biometric, health-related, and other types of highly sensitive data. It demonstrates that these frameworks provide numerous opportunities for consumer IoT data to be commodified and subsequently disclosed or transferred after the initial data collection.[44]

Part III critiques state and federal legislation that may be used to regulate the collection, disclosure, and transfer of consumer data, such as the

[43] *See infra* notes 47–162 and accompanying text.
[44] *See infra* notes 163–262 and accompanying text.

Bankruptcy Abuse Prevention and Consumer Protection Act, the Federal Trade Commission Act, state biometric data protection statutes, and the Health Insurance Portability and Accountability Act. This Part contends that these existing frameworks do not always effectively protect health-related, biometric, and highly sensitive consumer IoT data because they rely excessively on a notice and choice model and the terms of privacy policies, and in some instances these laws may not be applicable to IoT companies or transactions.[45]

Lastly, Part IV counsels movement away from the excessive overreliance on the terms of privacy policies and the notice and choice model. This Part proposes a framework that includes significant revisions to Article 9 and the Bankruptcy Code to reduce the transfer and disclosure of highly-sensitive consumer IoT data by companies. This Part also evaluates potential critiques of these proposals, including, but not limited to, competition, innovation and funding concerns and demonstrates the soundness of the proposed solutions.[46]

I. THE IOT DATA GOLD RUSH

It is estimated that by 2020 companies will be able to earn more profits transferring and disclosing IoT data than by selling IoT devices to consumers.[47] Biometric, health-related, and highly sensitive data are increasingly important in the IoT setting, and are frequently generated from consumers' use of IoT devices, and accompanying mobile applications and services. Privacy policies are the primary vehicle through which consumer data are disclosed and transferred. Consumer consent to privacy policies should not be used to vindicate data collection and disclosure practices that are harmful to consumers. The collection, use, and disclosure of biometric and health-related consumer data by companies can be detrimental to consumers' interests in several ways, which will be explored in detail below.[48]

A. Biometric, Health, and Highly Sensitive Data

The IoT has drastically increased "the volume, velocity, variety and value of data."[49] Companies can process and compile at record speeds data ob-

---

[45] *See infra* notes 263–390 and accompanying text.

[46] *See infra* notes 391–461 and accompanying text.

[47] Matt McFarland, *Your Car's Data May Soon Be More Valuable Than the Car Itself*, CNN: TECH (Feb. 7, 2017 9:05 AM), http://money.cnn.com/2017/02/07/technology/car-data-value/index.html [https://perma.cc/HM82-LPQR].

[48] *See infra* notes 131–162 and accompanying text.

[49] Terrell McSweeny, Comm'r, Fed. Trade Comm'n, Remarks at TecNation 2016 (Sept. 20, 2016) (transcript available at https://www.ftc.gov/system/files/documents/public_statements/985773/mcsweeny_-_tecnation_2016_9-20-16.pdf [https://perma.cc/P3V5-QPUX]).

tained from IoT devices and services, such as Wi-Fi enabled washing machines, refrigerators, cars, and other household appliances.[50] Fog computing allows companies to evaluate "time-sensitive . . . IoT data in milliseconds."[51]

It is estimated that about thirty percent of companies "use biometric authentication for mobile devices."[52] Biometrics, such as fingerprints and voice prints, are increasingly being used for identification purposes in the banking and payments industry.[53] With the rise of the IoT, however, the use of biometrics will not be limited to the payments industry, governmental entities, and smartphones. Biometric sensors and identifiers are expected to play a central role in Internet-connected devices in various industries.[54] In fact, by 2018 biometric sensors in IoT devices are projected to "total at least 500 million."[55]

Biometric data can be stored in various ways, including in central or decentralized systems or on a device in the possession of the consumer.[56] Some companies that currently use biometrics contend that they "do not store actual" biometric scans but rather the authentication codes or mathe-

---

[50] *Id.*

[51] CISCO, FOG COMPUTING AND THE INTERNET OF THINGS: EXTEND THE CLOUD TO WHERE THE THINGS ARE 1 (2015), https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf [https://perma.cc/Z59Z-MY2C] (noting that fog computing allows companies to analyze IoT data "at the network edge" while "send[ing] selected data to the cloud for historical analysis and longer-term storage").

[52] *See* Press Release, Gartner, Gartner Says 30 Percent of Organizations Will Use Biometric Authentication for Mobile Devices by 2016 (Feb. 4, 2014), http://www.gartner.com/newsroom/id/2661115 [https://perma.cc/2XUL-38AC].

[53] Jaime Toplin, *Biometrics in the Payment Industry: Why Biologically Based Authentication Is Becoming the Go-to Security Feature for Enabling Digital Commerce*, BUS. INSIDER (July 21, 2016, 1:42 PM), http://www.businessinsider.com/the-biometrics-report-2016-7 [https://perma.cc/3ZZ9-CEY6]; *Survey: Consumers Embrace Biometric Authentication*, MOBILE PAYMENTS TODAY (May 8, 2017), www.mobilepaymentstoday.com/news/survey-consumers-embrace-biometric-authentication/?utm_source=Email_marketing&utm_campaign=reviewMPT05132017144522&cmp=1&utm_medium=HTMLEmail [https://perma.cc/ZM32-QJSU] (discussing a study that suggests that consumers "would like to have more biometrics options for mobile banking").

[54] Narsimhmaswamy Badugu, *Biometrics in Internet of Things (IoT) Security*, LINKEDIN (Sept. 26, 2016), https://www.linkedin.com/pulse/biometrics-internet-things-iot-security-narsimhmaswamy-badugu/ [https://perma.cc/DQ5N-T4TX] (noting that biometrics will be used in the following areas: "Smart security[;] . . . Healthcare & Hospitals[;] Financials services[;] Automotive Industry[;] Endless applications wherever Identification and confirmation is required").

[55] *Id.*

[56] Tim De Chant, *The Boring and Exciting World of Biometrics*, PBS (June 18, 2013), http://www.pbs.org/wgbh/nova/next/tech/biometrics-and-the-future-of-identification [https://perma.cc/3EK7-Y5K2]; *see also* Andrew Patrick & Sabrina Mu, *Biometric Security Template Storage*, *in* USABILITY & ACCEPTABILITY OF BIOMETRIC SEC. DEVICES, http://www.andrewpatrick.ca/biometrics/templates/template.shtml [https://perma.cc/YM96-P8KG] (describing the storage of biometric data in a "central database," "individual workstation[]," "sensing device," or "portable token").

matical representations of the biometric identifiers.[57] As each individual's biometrics and the resulting authentication codes or templates are unique, biometric identifiers can be used to identify users and authenticate access to devices.[58] Biometric data may also be used for non-authentication purposes.[59] One commentator predicts that biometrics will "become the most widespread user interface for customers to interact with their various digital devices . . . ."[60] Consider that real estate developers are currently building "smart apartments" that utilize IoT devices and other "digital amenities, which are controlled by voice commands and smartphone apps . . . ."[61]

A report on IoT devices found that approximately 16% of consumers have smartwatches or fitness trackers, and between 8% to 12% of consumers indicated that they would be willing to purchase such devices.[62] Mobile applications, such as Runkeeper and Fitnet, that enable consumers to track their health and fitness goals are projected to generate more than $26 billion in revenues.[63] The health monitors and fitness device market is expected to "grow eight-fold from $5.1 billion in 2013 to $41.8 billion in 2023."[64] By 2020, companies will manufacture "[n]early 100 million wearable remote patient monitoring (RPM) devices," including blood pressure and glucose monitors.[65] It is estimated that "[b]y 2020, 40% of IoT-related technology

---

[57] Anna Myers, *Can the U.S. Legal System Adapt to Biometric Technology?*, INT'L ASS'N PRIVACY PROF'LS (Aug. 12, 2016), https://iapp.org/news/a/can-the-u-s-legal-system-can-adapt-to-biometric-technology/ [https://perma.cc/W4NK-4S35] (noting that companies use "authentication codes or templates" for biometric identifiers and "[t]he templates are coded as long, hard-to-predict numerical sequences"); Claire Gartland, *Biometrics Are a Grave Threat to Privacy*, N.Y. TIMES (July 5, 2016, 3:21 AM), http://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-are-a-grave-threat-to-privacy [https://perma.cc/R26T-2VDR]; *see also About Touch ID Advanced Security Technology*, APPLE SUPPORT (Sept. 11, 2017), https://support.apple.com/en-us/HT204587 [https://perma.cc/PZH4-J3BZ] (noting that Apple's Touch ID does not store scans of a user's fingerprint but rather a "mathematical representation" of the fingerprint).

[58] Gartland, *supra* note 57.

[59] *Id.*

[60] Paul Schaus, *Biometric Deployments Must Consider the 'Internet of Things,'* PAYMENTS SOURCE (Aug. 9, 2016, 12:01 AM), http://www.paymentssource.com/news/paythink/biometric-deployments-must-consider-the-internet-of-things-3024711-1.html [https://perma.cc/9674-84BL].

[61] C.J. Hughes, *The Latest in Apartment Technology: Fridge Cams and Robotic Valets*, N.Y. TIMES (Dec. 15, 2017), https://www.nytimes.com/2017/12/15/realestate/apartment-technology-fridge-cams-robotic-valets.html [https://perma.cc/NKU6-AVTT].

[62] Marketwired, *Kantar: Nearly 16% of US Consumers and 9% in EU4 Now Own Wearables*, YAHOO!: FINANCE (Jan. 25, 2017), https://finance.yahoo.com/news/kantar-nearly-16-us-consumers-125500338.html [https://perma.cc/6B6H-GFFD].

[63] Kellogg, *supra* note 17, at 77.

[64] Michael Essery, *Mobile Health Devices Market to Grow 8-fold to $41.8 Billion in 2023*, LUXRESEARCH (July 1, 2014), http://www.luxresearchinc.com/news-and-events/press-releases/read/mobile-health-devices-market-grow-8-fold-418-billion-2023 [https://perma.cc/5GDF-U9X9].

[65] Kellogg, *supra* note 17, at 78. Commentators contend that remote patient monitoring devices may be subject to the Health Insurance Portability and Accountability Act ("HIPAA"). *Id.*

will be health-related, more than any other category, making up a $117 billion market."[66]

IoT devices collect large amounts of health-related data about adults and children. For instance, a Fitbit device or app can track and collect data about a user's heart rate, calories burned, sleep patterns, and location.[67] Wi-Fi enabled blood sugar monitors can record blood sugar levels and alert consumers to changes in their levels.[68] The Apple Watch observes users' heart rates and daily health-related activities.[69] Mimo manufactures "a biometric-tracking onesie" for babies that monitors sleep patterns, among other things, and can connect to a parent's IoT thermostat and camera.[70] Pacif-i offers an IoT pacifier than can track an infant's temperature.[71]

IoT devices are frequently supported by mobile applications and websites that also collect additional data about consumers. The Propeller Health Inhaler uses "built-in sensors" that connect to a user's smartphone to "measur[e] where and when [users] have symptoms" of asthma attacks.[72] Of course, in some instances, mobile applications, such as Runkeeper, can be used as standalone items that allow users to monitor their health activities through their smartphones.[73] Health-related data garnered from IoT devices may also be useful for research purposes.[74]

---

[66] Dimiter V. Dimitrov, *Medical Internet of Things and Big Data in Healthcare*, 22 HEALTHCARE INFORMATICS RES. 156, 156 (2016), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4981575/ [https://perma.cc/54YR-8BMZ].

[67] *The Fitness App for Everyone*, FITBIT, https://www.Fitbit.com/app [https://perma.cc/DX5Z-L3W8].

[68] Emily Field, *Blood Sugar Monitor Maker Hit with Suit Over Car Crash*, LAW360 (Aug. 31, 2016, 4:59 PM), http://www.law360.com/articles/834866/blood-sugar-monitor-maker-hit-with-suit-over-car-crash [https://perma.cc/SD63-4ZA8].

[69] *Apple Watch Series 3*, APPLE, https://www.apple.com/apple-watch-series-3/ [https://perma.cc/6CXN-6AAS].

[70] Jacqueline Howard, *There Are Health-Tracking Wearables for Babies, Too*, CNN (Nov. 6, 2017, 7:11 AM), http://www.cnn.com/2017/11/06/health/baby-technology-products-teching/index.html [https://perma.cc/MW8S-E5BY]; *Mimo Works with Nest*, MIMO, http://mimobaby.com/nest [https://web.archive.org/web/20170107143735/https://www.mimobaby.com/nest] (describing how the product connects to Nest IoT devices); MIMO, http://mimobaby.com/ [https://perma.cc/TV2L-E6AJ] (describing the company's product as "[s]leep trackers for little ones").

[71] PACIF-I, https://www.pacif-i.io [https://perma.cc/7JT5-X47D] (discussing the capabilities of the company's connected Smart Pacifier).

[72] Kellogg, *supra* note 17, at 78 ("Propeller Health's inhaler, which has built-in sensors, connects through Bluetooth to smartphones, and lets individuals respond to asthma attacks while also tracking where those attacks occur."); PROPELLER, https://www.propellerhealth.com [https://perma.cc/3QDT-3CBB] ("Small sensor[,] Big difference").

[73] Kellogg, *supra* note 17, at 77.

[74] *Id.* (discussing research on asthma attacks); Alex Hutchinson, *The Power of Big (Fitness) Data*, RUNNER'S WORLD (Mar. 22, 2016, 9:32 AM), http://www.runnersworld.com/sweat-science/the-power-of-big-fitness-data [https://perma.cc/XHZ2-WQZK] (contending that "[i]t may be hard to extract meaning from any one individual's data—but collectively, the millions of peo-

In addition to simply collecting information about consumers, wearable IoT fitness devices can also "share their data with a multitude of applications and devices, with few if any restrictions."[75] Furthermore, in the future a device, such as a remote patient cardiac monitor, may be able to communicate and share data with a Fitbit wristband or potentially a Nest thermostat or security camera.

IoT devices may also collect potentially embarrassing and intimate information about consumers. An IoT sex-toy controlled by a mobile application collects and records real time data about how consumers use the device, including "the date and time of each use" and the selected "vibration intensity and pattern."[76]

B. IoT Privacy Policies

The provisions of a company's privacy policy primarily determine the extent to which a consumer's health-related, biometric, or highly sensitive data are disclosed to third parties. However, not all companies have privacy policies. It is estimated that approximately 26% of companies offering free mobile applications and 40% of businesses providing paid mobile applications or devices that monitor consumer health do not have privacy policies.[77] Mobile health devices and applications may also transmit consumer data, including "personally identifiable information," to third parties.[78] If an IoT company does not have a privacy policy, it is likely free to monetize consumer data without concern for potential privacy policy violation claims. Of course, in some instances, state law may require certain companies to post privacy policies.[79]

---

ple wearing self-monitoring devices amount to 'the largest and most comprehensive observational health trial ever conducted'").

[75] Kellogg, *supra* note 17, at 76.

[76] Shayna Posses, *Vibrator Gets Too Intimate by Tracking Usage Info, Suit Says*, LAW360 (Sept. 15, 2016, 3:57 PM), http://www.law360.com/articles/840299/vibrator-gets-too-intimate-by-tracking-usage-info-suit-says [https://perma.cc/R8JJ-TLCB].

[77] LINDA ACKERMAN, MOBILE HEALTH AND FITNESS APPLICATIONS AND INFORMATION PRIVACY, PRIVACY RTS. CLEARINGHOUSE 1, 5 (July 15, 2013), https://www.privacyrights.org/sites/default/files/mobile-medical-apps-privacy-consumer-report.pdf [https://perma.cc/AU3B-XW8E].

[78] *Id.* at 20.

[79] CAL. BUS. & PROF. CODE § 22575(a) (West 2017) ("An operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall conspicuously post its privacy policy on its Web site . . . ."); DEL. CODE ANN. tit. 6, § 1205C(a) (West 2017) ("An operator of a commercial internet website, online or cloud computing service, online application, or mobile application that collects personally identifiable information through the Internet about individual users residing in Delaware who use or visit the operator's commercial internet website, online or cloud computing service, online application, or mobile application shall make its privacy policy conspicuously available on its internet website, online or cloud computing service, online application, or mobile application."); *State Laws Relat-*

Privacy policies routinely authorize companies to disclose, sell, and transfer consumer data to third parties. Consider that the privacy policy of Clear, a company that provides a paid service that collects and uses consumers' biometric data ("digital images of fingerprints and irises") to allow them to authenticate their identity and by-pass airport and events security, provides that biometric data can be transferred to third parties in the event of a sale of the company or its assets.[80]

Not surprisingly, a report on privacy policies found that eighty-five of the "top 100 websites in the United States" had "terms of service or privacy policies" that authorize the sale of consumer data in the event of "a merger, acquisition, bankruptcy, asset sale or other [business] transaction."[81] In some instances, companies' privacy policies may expressly note that they "cannot guarantee the security of information provided over the Internet or stored in [their] databases."[82] Privacy and security can be drafted out of privacy policies. In the report on privacy policies mentioned above, only seventeen of these top websites had policies requiring the company to notify consumers of the transfer or sale of their information.[83] At least one non-IoT company's privacy policy includes a carve out for a "financing . . . of

---

ed to Internet Privacy, NAT'L CONF. STATE LEGISLATURES (June 20, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx [https://perma.cc/K492-XE9T] (noting that Nevada enacted a bill similar to the California statute in 2017). Such state law requirements may in some instances be preempted by federal legislation. People *ex rel.* Harris v. Delta Air Lines, Inc., 202 Cal. Rptr. 3d 395, 395 (Cal. Dist. Ct. App. 2016) (finding that a lawsuit brought by the State of California alleging violations of its Online Privacy Protection Act was preempted by the Airline Deregulation Act).

[80] *Privacy Policy*, CLEAR, https://www.clearme.com/privacy_policy [https://perma.cc/U9N8-LBL5] ("We reserve the right to transfer personal information we have about consumers in the event we sell or transfer all or a portion of our business or assets . . . .").

[81] Natasha Singer & Jeremy B. Merrill, *When a Company Is Put Up for Sale, in Many Cases, Your Personal Data Is, Too*, N.Y. TIMES (June 28, 2015), https://www.nytimes.com/2015/06/29/technology/when-a-company-goes-up-for-sale-in-many-cases-so-does-your-personal-data.html [https://perma.cc/7GKU-QQRF]; Kate Cox, *Your Personal Information Is Probably Going to Be for Sale When the Company You Gave It to Is*, CONSUMERIST (June 29, 2015, 9:54 AM), https://consumerist.com/2015/06/29/your-personal-information-is-probably-going-to-be-for-sale-when-the-company-you-gave-it-to-is/ [https://consumerist.com/2015/06/29/your-personal-information-is-probably-going-to-be-for-sale-when-the-company-you-gave-it-to-is/] (discussing the New York Times report on the provisions of privacy policies).

[82] Consumer Privacy Ombudsman Report to the Court at 25, *In re* Gander Mountain Co. Overton's Inc., No. 17-30673 (Bankr. D. Minn. May 3, 2017) [hereinafter Gander CPO Report]; *Privacy Policy*, FiLIP, http://www.myfilip.com/privacy-policy/ [https://perma.cc/XR8L-ZJL8] [hereinafter FiLIP Privacy Policy] ("[D]ue to the inherent open nature of the Internet and wireless communications, we cannot guarantee that your personal information will be completely free from unauthorized access by third parties . . . . Your use of our FiLIP Service demonstrates your assumption of this risk.").

[83] Singer & Merrill, *supra* note 81.

all or a portion of [the] business."[84] This may include secured financing transactions.

The privacy policy of Nest, a manufacturer of various IoT devices, including thermostats and smart security systems, provides that the company "do[es] not rent or sell [its] customer lists."[85] The privacy policy goes on to provide, however, that the company may sell or transfer consumer data in connection with a "business transition."[86] In the event of such a transition, the company promises to request that the buyer of its assets comply with whatever privacy policy is in place when the data is collected.[87] Amazon's privacy policy also authorizes the transfer of consumer data upon a "business transfer."[88] Amazon manufactures various IoT devices that utilize some degree of artificial intelligence, such as the Amazon Echo.[89] Apple's privacy policy states that "in the event of a reorganization, merger, or sale we may transfer any and all personal information we collect to the relevant third party."[90]

Privacy policies may also provide that consumers consent to the terms of the policy simply by using the IoT device.[91] Moreover, privacy policies change frequently and companies revise their privacy statements unilaterally in accordance with unilateral amendment provisions contained in their conditions of use or privacy policies. If a company's privacy policy in effect at the time of the sale or when the data was originally collected does not contain provisions that adequately protect consumer data, the purchaser of the company's assets may be free to use the data as it pleases. Even if a company promises to request that a buyer of the company's assets (including consumer data) complies with the company's existing privacy policy,

---

[84] *Nextio—Privacy Policy*, NEXTIO, https://www.nextio.com/n/privacy [https://perma.cc/NW38-ZLML] ("We may share information about you as follows or as otherwise described in this Privacy Policy: . . . In connection with, or during negotiations of, any merger, sale of company assets, financing or acquisition of all or a portion of our business by another company . . . .").

[85] *Privacy Statement for Nest Products and Services*, NEST, https://nest.com/legal/privacy-statement-for-nest-products-and-services [https://perma.cc/UZ2E-P98K] [hereinafter *Nest Product Privacy Policy*].

[86] *Id.*

[87] *Id.*

[88] *Amazon Privacy Notice*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=468496 [https://perma.cc/5KNB3RRM] [hereinafter *Amazon Privacy Policy*].

[89] Arjun Kharpal, *Amazon's Alexa Stole the Show at CES in a Bid to Become the Internet of Things Operating System*, CNBC (Jan. 6, 2017, 6:54 AM), https://www.cnbc.com/2017/01/06/ces-2017-amazon-alexa-stole-the-show-a-bid-to-become-the-iot-operating-system.html [https://perma.cc/24AK-7QQF].

[90] *Privacy Policy*, APPLE, http://www.apple.com/legal/privacy/en-ww/ [https://perma.cc/8ZFX-NFA6] [hereinafter *Apple Privacy Policy*].

[91] *Nest Product Privacy Policy*, *supra* note 85 ("By using Nest Products, you agree to allow us to collect and process information as described in this Privacy Statement.").

non-compliance with the privacy policy could be permissible if consumer consent is obtained.

The American Law Institute's proposed Restatement of the Law of Consumer Contracts, if finalized and adopted, could provide explicit guidance on whether privacy policies should be viewed as contracts.[92] Historically, however, there has been some dispute about whether privacy policies are indeed contracts or simply "broad statements of company policy."[93] Relying on consumer consent to authorize data use and collection practices is problematic for several reasons.

First, consumers frequently fail to read and understand contract terms and their implications.[94] Consumers may freely consent to the disclosure and transfer of their data without truly understanding the ramifications of this decision and may not always be aware that they are entering into data-trade agreements. Even after some consumers conduct detailed reviews of privacy policies, many "regard even highly ambiguous privacy policy language as authorizing controversial company practices that implicate their personal privacy."[95] Additionally, although some consumers may review privacy policies, consumer consent to privacy policies is "driven by social norms."[96]

---

[92] *Restatement of the Law, Consumer Contracts*, AM. LAW INST., https://www.ali.org/projects/show/consumer-contracts/ [https://perma.cc/HTW8-NZT9] (proposing a restatement that "will focus on aspects of the law unique to consumer contracts and on regulatory techniques . . . in consumer-protection law"); *see* Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1458 (2017) (discussing the proposed restatement); *Project Feature: Restatement of the Law, Consumer Contracts*, ALI ADVISOR, http://www.thealiadviser.org/consumer-contracts/ [https://perma.cc/2PK4-UMUF] (noting topics that may be addressed by the restatement).

[93] *In re* Am. Airlines, Inc., Privacy Litig., 370 F. Supp. 2d 552, 561 (N.D. Tex. 2005); Warren E. Agin, *The New Regime for Treatment of Customer Data in Bankruptcy Cases*, 10 J. BANKR. L. & PRAC. 365 (contending that privacy statements may be "executory or non-executory" contracts depending primarily on "whether it places continuing material obligations on each party" but a "privacy policy might not even qualify as an enforceable contract"); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 595–96, 628 (2014) (discussing whether privacy policies are contracts).

[94] Nancy S. Kim & D.A. Jeremy Telman, *Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent*, 80 MO. L. REV. 723, 732 (2015), (contending that "due to their size and market dominance . . . companies [such as, Google, Facebook and Yahoo] exercise quasi-governmental authority and monopoly power that makes consumer consent to data collection meaningless"); Aaron Perzanowski & Chris Jay Hoofnagle, *What We Buy When We Buy Now*, 165 U. PA. L. REV. 315, 320 (2017) ("The overwhelming majority of online shoppers ignore license terms."); Ari Ezra Waldman, Privacy, Notice, and Design 2 (July 25, 2016) (unpublished manuscript) (on file with the Federal Trade Commission) (contending that privacy policies are "difficult to understand" and are insufficient at providing notice).

[95] Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEGAL STUD. S69, S87 (2016). Strahilevitz & Kugler further contend that many e-mail and social network users view "the vague and imprecise policy language as authorizing Facebook, Yahoo, and Google to engage in [disturbing privacy] practices." *Id.* at S92–S93.

[96] *Id.* at S87.

Admittedly, the level of consumers' awareness and understanding of data-trade agreements may to some extent be context dependent. For instance, a consumer that uses a health mobile application is likely aware that the application is collecting some types of health-related data even if the consumer may not thoroughly grasp the implications of this type of data collection. In contrast, a consumer that uses an IoT refrigerator or toaster may not be aware of the types of, and extent to which, data are being collected and what can subsequently be done with such data. For example, the Roomba robotic vacuum not only self-cleans a consumer's home, but also collects "home layout data" including "the location of everything from [walls and] lamps to home security cameras and thermostats."[97] The company has suggested that it may sell this data to third parties.[98]

Second, consumers may consent to terms and conditions that do not adequately describe a company's biometric data collection and storage policies. Thus, even if all consumers were inclined to routinely attempt to review and understand a company's data collection policies and practices, consumers may not be provided with the information necessary to make informed decisions about data collection and disclosure before being required to consent (or deemed to have consented) to a company's conditions of use or privacy policy. In *Vigil v. Take-Two Interactive Software, Inc.*, a 2017 case involving a company that collects biometric data, the plaintiffs contended that the company collected and shared their biometric data without supplying them with sufficient information about the company's data collection, retention, and destruction policies.[99] The district court reasoned that although the company failed to disclose how long the data would be stored, at a minimum the plaintiffs understood that in order to use the company's products their face scans would be collected and stored "so long as those avatars existed."[100]

Third, "security fatigue" may also be exacerbated in the IoT setting and may lead consumers to make reckless choices, including consenting to

---

[97] Maggie Astor, *Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared*, N.Y. TIMES (July 25, 2017), https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html [https://perma.cc/3W6L-LAAP] (discussing the privacy implications of the Roomba vacuum); Natalie O'Neill, *Roomba Maker Wants to Sell Your Home's Floor Plan*, N.Y. POST (July 25, 2017, 1:04 PM), https://nypost.com/2017/07/25/roomba-maker-wants-to-sell-your-homes-floor-plan/ [https://perma.cc/V5BR-R4M7]; *iRobot® Roomba® 980*, IROBOT, http://store.irobot.com/default/roomba-vacuuming-robot-vacuum-irobot-roomba-980/R980020.html [https://perma.cc/VAC8-VY8K] (describing the self-cleaning capabilities of the Wi-Fi connected Roomba vacuum).

[98] O'Neill, *supra* note 97.

[99] 235 F. Supp. 3d 499, 506–07, 521–22 (S.D.N.Y. 2017) (granting defendant's motion to dismiss plaintiffs' amended complaint), *aff'd in part, vacated in part*, Santana v. Take-Two Interactive Software, Inc., No. 17-303, 2017 U.S. App. LEXIS 23446 (2d Cir. Nov. 21, 2017).

[100] *Id.* at 515.

dubious data collection practices.[101] Given that consumers have multiple IoT devices in their homes, consumers may become exhausted with having to implement or comply with numerous measures to ensure their privacy and security.[102]

Fourth, even when a consumer declines to consent to data collection, companies may be able to "draw probabilistic inferences" about non-consenting consumers from the data generated by consumers that do consent to data collection, once a "representative sample" is reached.[103] This may then render a consumer's decision to decline to consent to data collection meaningless.[104]

Fifth, the different companies that may be involved in manufacturing and operating the various components of IoT devices, services, and applications, including "hardware and software developers," may have contrasting privacy policies and data collection practices.[105] Even if a single company manufactures all components, and operates and provides all services and servers, related to the device, the company may have different privacy policies that govern different aspects of its interactions with consumers. For instance, Nest provides a separate privacy statement for its IoT devices and services and another for its websites.[106] Thus, portions of a consumer's data, collected and shared through IoT devices, services and related websites, may be subject to different privacy policies.

Sixth, both IoT and non-IoT privacy policies permit companies to share consumer data with various third parties. For instance, privacy policy provisions can authorize consumer data disclosures when consumers accept rewards programs or promotional offers provided by third parties that are recommended by device manufacturers.[107] In such an instance, data that is

---

[101] Belton Zeigler, *The Next Threat to Cybersecurity: Consumer Fatigue*, LAW360 (Nov. 9, 2016, 2:20 PM), https://www.law360.com/articles/861219/print?section=consumerprotection [https://perma.cc/3GJ2-2H2H].

[102] *Id. See generally* Brian Stanton et al., *Security Fatigue*, IT PROF., Sept./Oct. 2016, at 26 (discussing the potential impact of security fatigue).

[103] Solon Barocas & Helen Nissenbaum, *Big Data's End Run Around Procedural Privacy Protections*, COMM. ACM, Nov. 2014, at 31, 32.

[104] *Id.*

[105] Ronald Raether et al., *The Technology Lawyer and Connected Things*, LAW360 (July 28, 2016, 3:36 PM), http://www.law360.com/articles/822484/the-technology-lawyer-and-connected-things [https://perma.cc/ZV7U-QVBH].

[106] *Compare Privacy Policy for Nest Web Sites*, NEST, https://nest.com/legal/privacy-policy-for-nest-web-sites/ [https://perma.cc/WT85-F2VW], *with Privacy Statement for Nest Products and Services*, NEST, https://nest.com/legal/privacy-statement-for-nest-products-and-services/ [https://perma.cc/TT6Y-S9RZ].

[107] *Nest Product Privacy Policy*, *supra* note 85 (authorizing the disclosure of consumer information with consumer consent when a consumer "enrolls in third party reward programs such as rush hour rewards").

provided to the unaffiliated party is subject to that party's privacy policy.[108] Consider that a consumer may link their Fitbit account to their Facebook account to share fitness updates.[109] To the extent that a consumer authorizes this connection, the health-related data from the IoT device or mobile application could be shared with Facebook and the consumer's Facebook account information could be shared with Fitbit.[110] How the Fitbit health-related data will be used by Facebook depends on Facebook's privacy policy.[111]

Consumer data may also be disclosed to third-party service providers that help IoT companies process data and monitor their systems.[112] Some consumers may be aware that by using a company's IoT product they are authorizing the company to collect their data, but consumers are unlikely to obtain information about the third parties that the company contracts with to maintain, store, or process their data or be aware of how such third parties protect consumer-related data.[113] Additionally, as demonstrated in Part II below, the use of third-party service contractors provides several opportunities for consumer data to be disclosed and transferred under Article 9 and other state statutes.[114]

Aggregated and anonymized consumer data are also frequently sold or transferred to third parties. An animated short summary of Fitbit's privacy policy provides "[w]e don't sell data that could identify you to anyone, anywhere, anytime. Ever. Period. That's all folks."[115] The language prohibiting the sale of the data refers to data that is not anonymized. This implies that anonymized data may be sold. In fact, in the company's complete privacy statement, which is accessible only after clicking a separate link, the company acknowledges that it may monetize de-identified data.[116] Similarly, the privacy policy of FiLIP states that the company may share "non-personal or de-identified information with any number of parties, including data analytics companies, technology providers and other business part-

---

[108] *Id.*

[109] *Fitbit Privacy Policy*, FITBIT, https://www.fitbit.com/legal/privacy-policy#what-data [https://perma.cc/6YBV-MV32] [hereinafter *Fitbit Privacy Policy*].

[110] *Id.*

[111] *Id.*

[112] ACKERMAN, *supra* note 77, at 18, 20–22.

[113] *Id.* (noting that companies may not always disclose all third parties who may have access to consumer data in their privacy policies); Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 946 (2007) ("One set of difficulties with consumer shopping for data security follows from the frequent lack of any [business-to-customer] relationship between the individual whose data are stolen and the entities that play a major role in processing her information.").

[114] *See infra* notes 232–237 and accompanying text.

[115] *Let's Talk About Privacy, Publicly*, FITBIT, https://www.fitbit.com/legal/privacy [https://perma.cc/RX4W-QEJ6].

[116] *Fitbit Privacy Policy*, *supra* note 109 ("[Fitbit] may share or sell aggregated, de-identified data that does not identify you.").

ners."[117] The term "business partners" could very well mean data brokers that the company has entered into cooperative agreements with. IoT companies, such as Fitbit and Jawbone, have faced scrutiny in other countries for allegedly violating relevant laws by collecting more data than was needed for their products to function and for failing to disclose to consumers the parties with "whom they share consumer data."[118]

Data that has been anonymized could be de-anonymized or re-identified. [119] Promises by an IoT company to anonymize health-related, biometric, or any other type of consumer data before monetizing or providing third-party access to the data may be meaningless. As one scholar has emphasized, companies continue to disclose "information [that can be used to re-identify consumers and which is] connected to sensitive data in supposedly anonymized databases, with absolute impunity."[120] Consider that a study conducted by researchers at Carnegie Mellon University suggests that an individual's social security number can be predicted from various sources of data, including public information and data from social networking profiles.[121] Other researchers evaluating the robustness of anonymization and metadata conclude that it is possible to re-identify ninety percent of consumers from anonymized "credit card transactions for 1.1 million users."[122] Their study found that "even data sets that provide coarse infor-

---

[117] FiLIP Privacy Policy, *supra* note 82.

[118] Allison Grande, *Norwegian Watchdog Hits Fitbit, Others Over Privacy Missteps*, LAW360 (Nov. 3, 2016 10:56 PM), https://www.law360.com/articles/859337/norwegian-watchdog-hits-fitbit-others-over-privacy-misstep [https://perma.cc/3MSZ-33AX] (describing "formal complaints" filed by the Norwegian Consumer Council against Fitbit, Garmin, Jawbone, and Mio for alleged violations of Norwegian and "European privacy and marketing laws").

[119] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1703–05 (2010) (discussing how de-identified consumer data can be re-identified and contending that for eighty-seven percent of Americans, "[no] other people in the United States share [their] specific combination of ZIP code, birth date (including year), and sex" and this information could be used to de-identify anonymized data and correctly identify "more than 80 percent of" users).

[120] *Id.* at 1705.

[121] Alessandro Acquisti & Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106 PROC. NAT'L ACAD. SCI. 10,975, 10,975 (2009) (The study "observed a correlation between individuals' SSNs and their birth data and found that for younger cohorts the correlation allows statistical inference of private SSNs. The inferences are made possible by the public availability of the Social Security Administration's Death Master File and the widespread accessibility of personal information from multiple sources, such as data brokers or profiles on social networking sites.").

[122] Yves-Alexandre de Montjoye et al., *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, 347 SCIENCE 536, 537 (2015). *But see generally* Andrew Chin & Anne Klinefelter, *Differential Privacy as a Response to the Reidentification Threat: The Facebook Advertiser Case Study*, 90 N.C. L. REV. 1417 (2012) (objecting to criticisms of anonymization and contending that new technology may protect anonymity under a "differential privacy standard"); David Sánchez et al., *Comment on "Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata,"* 351 SCIENCE 1274-a (2016) (critiquing the Montjoye study and conclud-

mation at any or all of the dimensions provide little anonymity and that women are more reidentifiable than men."[123]

The monetization of children's biometric or health related-data is also concerning even if such data are anonymized. The privacy policy of Owlet, the manufacturer of an infant IoT monitoring sock device, provides that the company may freely transfer and disclose infants' anonymized health-related data, such as "heart rate and blood-oxygen level[s]."[124] The company's privacy policy also provides that the "personal information" of adults and babies may also be disclosed to third parties for marketing purposes and in connection with business transactions.[125] In the IoT setting, before minors come of age their immutable biometric or health-related data could be collected, stored, transferred, and resold to third parties for years. This may occur despite federal law aimed at protecting the information of children.[126]

Companies may also collect personally identifiable data that is mixed in with non-personally identifiable data. FiLIP's privacy policy provides that if

---

ing that "data owners and subjects can be reassured that sound anonymization methodologies exist to produce useful anonymized data that can be safely shared for research"); *see also* Yves-Alexandre de Montjoye & Alex "Sandy" Petland, *Response to Comment on "Unique in the Shopping Mall: On the Reidentifiability of Credit Card Data,"* 351 SCIENCE 1274-b (2016) (responding to the Sánchez critique noted above and contending that "Sánchez *et al.* . . . fundamentally misunderstand the size and dimensionality of modern big-data data sets and how they are being used in industry and research," and that "[t]he current deidentification model, where the data are anonymized and released, is obsolete and should not be used for policy").

[123] Montjoye et al., *supra* note 122, at 536.

[124] *Privacy*, OWLET, http://www.owletcare.com/privacy/ [https://perma.cc/QC68-QC5M] [hereinafter *Owlet Privacy Policy*].

[125] *Id.* The privacy policy also notes that consumers may opt-out of marketing. *Id.*

[126] *See, e.g.*, Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2012); Angela J. Campbell, *Rethinking Children's Advertising Policies for the Digital Age*, 29 LOY. CONSUMER L. REV. 1, 21–35 (2016) (discussing the limitations of the Children's Online Privacy Protection Act ("COPPA") framework); Ben Kochman, *Devices Can Collect Kids' Commands Without Consent: FTC*, LAW360 (Oct. 24, 2017, 5:54 PM), https://www.law360.com/articles/977168/devices-can-collect-kids-commands-without-consent-ftc [https://perma.cc/N9KW-BDVQ] (discussing the Federal Trade Commission (FTC) policy statement authorizing IoT companies "to collect audio files from kids without consent" and noting that at least one commentator has stated that the policy statement does "not solve the consent problem that lies at the heart of COPPA," because "[i]t is simply too easy for advertisers to obtain personal data of children for marketing purposes") (internal quotation marks omitted); *Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings*, FED. TRADE COMM'N, https://www.ftc.gov/system/files/documents/public_statements/1266473/coppa_policy_statement_audiorecordings.pdf [https://perma.cc/PL3R-RU37] (explaining that "when a covered operator collects an audio file containing a child's voice solely as a replacement for written words, such as to perform a search or fulfill a verbal instruction or request, but only maintains the file for the brief time necessary for that purpose, the FTC would not take an enforcement action against the operator on the basis that the operator collected the audio file without first obtaining verifiable parental consent. Such an operator, however, must provide the notice required by the COPPA Rule, including clear notice of its collection and use of audio files and its deletion policy, in its privacy policy," and noting that the operator may not monetize such audio files).

it accidentally obtains personal information along with non-personal data, it will not intentionally use the personal data as if it had obtained consumer consent.[127] The use of the word "intentional" suggests than an unintentional use of the personally identifiable data may be permissible under the policy.

Lastly, some IoT companies may allow consumers to delete their data.[128] However, IoT privacy policies can authorize companies to retain and store data on company servers even though the consumer may no longer have access to the data.[129] Thus, IoT companies could continue to monetize consumer data even if the data is no longer viewable to the consumer or if the consumer has requested that their data be deleted.

The foregoing discussion demonstrates that the first few statements of a company's privacy policy may lure consumers into believing that their data will be protected. However, there will likely be several exceptions to the company's initial promise not to sell, disclose or transfer consumer data.

C. Consumer Harms & Risks

Once a privacy policy authorizes the collection, disclosure, or transfer of consumer IoT data, it can be disclosed to third parties, with problematic consequences for consumers. Admittedly, there are benefits to the collection and use of biometric, health-related, and highly sensitive data, including convenience and the facilitation of seamless interactions with IoT devices. Although the collection of IoT data may be necessary to allow an owner to use certain aspects of IoT devices and services, whether interests in such data should be sold or assigned after collection should not depend primarily on the language in privacy policies. Given the rapid level at which technol-

---

[127] FiLIP Privacy Policy, *supra* note 82 ("It is possible at times when collecting non-personal information through automatic means that we may unintentionally collect or receive personal information that is mixed in with the non-personal information. While we will make reasonable efforts to prevent such incidental data collection, the possibility still exists. If we do inadvertently collect personal information, we will not intentionally use such personal information as if we had collected it with your consent.").

[128] *See Nest Product Privacy Policy*, *supra* note 85 ("Nest generally stores your personal information on Nest's servers until you delete or edit it, or for as long as you remain a Nest customer . . . . [But, due to] the way we maintain certain Services, after your information is deleted, backup copies may linger for some time before they are deleted, and we may retain certain data for a longer period of time . . . .").

[129] FiLIP Privacy Policy, *supra* note 82 ("We may retain your information for as long as we feel that there is a business need or benefit to do so. This will include retaining location-based information."); *Fitbit Privacy Pledge*, FITBIT, https://www.fitbit.com/no/legal/privacy [https://perma.cc/CJ9R-B98B] ("If you remove data from your [Fitbit] Account, it will no longer appear to you or others who use the Service. Backups of that data will remain in association with your [Fitbit] Account and in our archive servers."); *Nest Product Privacy Policy*, *supra* note 85 ("We may retain certain data for a longer period of time . . . ."); *Owlet Privacy Policy*, *supra* note 124 ("We will retain your information for our business purposes, and in connection with our legal obligations, and to resolve disputes and enforce our agreements.").

ogy is evolving, there may be risks associated with the collection and disclosure of consumer data that consumers may never become aware of or fully understand. This concern may remain true even for consumers that have some awareness of the value of their data. The harms and risks discussed below may arise whenever consumer data of any kind is collected. However, the uniqueness and highly-sensitive nature of biometric and health-related data, as well as the potential for the collection, disclosure or transfer of such IoT data under existing privacy policies and the financial frameworks discussed in Part II below,[130] are troublesome for several reasons, which the remainder of this section will explore.

1. Consensual Disclosures and Data Analytics

Privacy policies permit companies to use and analyze the data that they collect about consumers. Once consumers authorize data collection, data analytics allows businesses "to combine and jointly analyze more previously disparate sources of data than ever before" to paint a more complete and accurate picture of the lives and activities of consumers, individuals in their households, and communities.[131] Thus, combining existing data about consumers with biometric and health-related data opens new windows into, and generates new insights about, consumer preferences, behaviors, and activities.

---

[130] *See infra* notes 163–262 and accompanying text.

[131] Terrell McSweeny, Comm'r, Fed. Trade Comm'n, Keynote Remarks at the Taiwan International Conference on Competition Policy: A U.S. Enforcer's Perspective: Protecting Competition and Promoting Innovation 13 (June 29, 2016) (transcript on file with the Federal Trade Commission); *see* FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION?, at i, 1 (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf [https://perma.cc/4PD3-GARZ] [hereinafter FTC, BIG DATA] ("The analysis of this data is often valuable . . . as it can guide the development of new products and services, predict the preferences of individuals, help tailor services and opportunities, and guide individualized marketing."); Elvy, *supra* note 92, at 1379 (discussing companies' use of data analytics); Michelle De Mooy et al., *Should It Stay, or Should It Go?: The Legal Policy and Technical Landscape Around Data Deletion*, CTR. FOR DEMOCRACY & TECH. 5 (Feb. 2017), https://cdt.org/files/2017/02/2017-02-23-Data-Deletion-FNL2.pdf [https://perma.cc/RBF2-HT4R] ("The ability to conduct broader and deeper analysis of data holdings can help businesses develop a multi-faceted view of their customers . . . ."); *Marketers Gain Unified View of Customers Across All Channels and Devices with BlueConic and Acxiom*, BUS. WIRE (Oct. 4, 2017, 7:00 AM), http://www.businesswire.com/news/home/20171004005276/en/Marketers-Gain-Unified-View-Customers-Channels-Devices [https://perma.cc/6VBX-6G59] (announcing a recent partnership between Axciom, one of the largest data brokers, and BlueConic, a "customer data platform" to allow companies "to unify and enhance their first-party data in real-time by accessing Acxiom's premium third-party referential database intelligence and data enrichment services to create a complete view of their customer across the entire customer lifecycle, through all channels and devices").

Insights gleaned from IoT data and data analytics may be used to engender "new justifications [or methods] for exclusion," such as when biometric or health-related data are used to explain differences in the price of products, deny opportunities to certain individuals, and influence consumer consent to data collection practices.[132]

With respect to the potential for exclusion, Facebook's advertisement practices provide an example of the dangers of data collection and analytics even when consumer consent to data collection is received.[133] Facebook, a company that collects and processes personal data about consumers, including biometric data, allowed advertisers to "target users by their interests" and exclude certain groups with "Ethnic Affinities" from their advertisements.[134] The company assigned consumers to an "Ethnic Affinities" category (a demographic category) "based on pages and posts they have liked or engaged with on Facebook."[135] Companies could use the "Ethnic Affinities" category to exclude users based on their race, by for instance, advertising housing options to only specific groups.[136]

Today, companies are developing innovative facial "recognition technology" to correlate a person's name to their face in public "even if they are

---

[132] Peppet, *supra* note 12, at 117–40 (discussing concerns regarding exclusion, privacy, and security in the IoT setting); FTC, BIG DATA, *supra* note 131, at 9–12. In some instances, some organizations may be limited in their ability to discriminate based on, for instance, the health status of an individual. *See, e.g.*, 29 U.S.C. § 1182(a) (2012) ("[p]rohibiting discrimination against individual participants and beneficiaries based on health status"); *see also* Nondiscrimination and Wellness Programs in Health Coverage in the Group Market, Final Rules, 71 Fed. Reg. 75,014 (Dec. 13, 2006) (describing final rules governing the provisions prohibiting discrimination).

[133] *Statement of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/legal/terms/update [https://perma.cc/BGF5-B28X] [hereinafter *Facebook Statement of Rights*]. Facebook's statement of rights and responsibilities states that:

> [b]y using or accessing the Facebook Services, you agree to this Statement . . . . We designed our Data Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. . . . For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License).

Id.

[134] Julia Angwin & Terry Parris, Jr., *Facebook Lets Advertisers Exclude Users by Race*, PROPUBLICA (Oct. 28, 2016, 1:00 PM), https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race [https://perma.cc/P6U3-KP8D].

[135] *Id.*

[136] *Id.*; *see also* Sapna Maheshwari & Mike Isaac, *Facebook, After 'Fail' Over Ads Targeting Racists, Makes Changes*, N.Y. TIMES (Sept. 20, 2017), https://www.nytimes.com/2017/09/20/business/media/facebook-racist-ads.html [https://perma.cc/NCX6-TQBH] (discussing Facebook's use of "ethnic affinities" or "multicultural affinity" category in advertising and the company's attempts to remedy concerns associated with same) (internal quotation marks omitted).

obscured and identify people by their clothing and posture."[137] It may ultimately be possible for companies to exclude individuals with specific biometric identifiers or health-related markers (such as perceived emotional state and hormone levels) from specific offers. Consider that a recent peer reviewed study conducted by researchers at Stanford University suggests that artificial intelligence can be used to scan facial images and deduce sexual orientation more accurately than humans.[138] Unrestricted use of these types of data by companies for artificial intelligence and data analytics purposes can lead to the development of new proxy traits that can enable exclusion. By allowing consumer data to be easily transferred from one entity to another, financial frameworks can also facilitate exclusion. Commentators report that "Facebook has filed patents for" facial recognition technology that would permit it "to tailor ads based on users' facial expressions" and the company is developing physical IoT products that may utilize its biometric database and facial recognition technology.[139] In light of Facebook's previous inconsistent statements about its plans for the use of biometric data, in the future the company could find new ways to monetize its significantly large biometric database, including disclosing or transferring this information to other entities, such as IoT companies, thereby providing new opportunities for exclusion.[140]

---

[137] FACEBOOK INC: BIOMETRIC DATA CLASS ACTION ONGOING IN ILLINOIS, CLASS ACTION REPORTER (Beard Group, Inc., Washington, D.C.), Sept. 15, 2017, at 2 [hereinafter FACEBOOK BIOMETRIC DATA]; Kate Baggaley, *How Facial Recognition Systems Will Reshape Your Daily Life*, NBC NEWS: MACH (Sept. 14, 2017, 2:43 PM), https://www.nbcnews.com/mach/tech/how-facial-recognition-systems-will-reshape-your-daily-life-ncna801336 [https://perma.cc/6Q4Z-Z8CG] (discussing the expected widespread use of facial recognition technology across various industries, including "shopping, banking, travel, and more").

[138] *See generally* Yilun Wang & Michal Kosinski, *Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation from Facial Images*, J. PERSONALITY & SOC. PSYCHOL. (forthcoming 2018), https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/wang_kosinski.pdf [https://perma.cc/ZR2X-ECD8] (finding that human "faces contain more information about sexual orientation than can be perceived or interpreted by the human brain" and contending that the study "showed that the facial features extracted by a [deep neural network] can be used to accurately identify the sexual orientation of both men and women"). *But see Advances in AI Are Used to Spot Signs of Sexuality*, THE ECONOMIST (Sept. 9, 2017), https://www.economist.com/news/science-and-technology/21728614-machines-read-faces-are-coming-advances-ai-are-used-spot-signs [https://perma.cc/ZWE2-VDAP] (discussing the Wang and Kosinski study and its limitations).

[139] FACEBOOK BIOMETRIC DATA, *supra* note 137; Alex Heath, *Facebook Is Putting a Top Exec in Charge of All Hardware and Readying an 'Aloha' Video Chat Device*, BUS. INSIDER (Aug. 23, 2017, 4:52 PM), http://www.businessinsider.com/facebooks-andrew-bosworth-to-lead-oculus-building-8-aloha-video-chat-device-details-2017-8 [https://perma.cc/9VMF-NA7S] (describing Facebook's production of a video chat device that will use facial recognition technology to rival the Amazon Echo Show).

[140] *See* FACEBOOK BIOMETRIC DATA, *supra* note 137, at 4–5 (noting that "Facebook hasn't been consistent about what it plans to do with its facial data" and that in 2012 Facebook's privacy

2. Non-Consensual Disclosures and Data Breaches

The risk of data breaches has long been problematic for both consumers and companies. Yet, the unauthorized disclosure of IoT consumer data is even more alarming. For consumers, this concern is exacerbated when privacy policies are drafted to insulate companies from liability for third-party hacking and when financial frameworks permit consumer data to be continuously transferred from one party to another. As IoT data are moved from one party to another and from one network to another, data storage and transfer vulnerabilities may be exposed making unauthorized access much easier, particularly when the data are not encrypted.

Health-related data and biometric identifiers (as well as the source of biometric identifiers, such as voice recordings) can be stored on vulnerable IoT devices or in a company's database on a server and potentially "linked with [other] personal information about" consumers.[141] A company's servers or the IoT device storing this information could be easily hacked resulting in data exfiltration.[142] As one commentator has noted, although "you can reset a password . . . you can't replace your fingertips or eyeballs."[143] Furthermore, if health-related data are disclosed "there are few good remedies" for victims because "[t]hey are unprotected, and sometimes their whole families are unprotected."[144] The harms that consumers may face from regular data breaches that expose financial records, names, or addresses are well documented.[145] These consumer harms are likely to be magnified if a hack results in the release of biometric or health-related data. Consider that the database of IoT toy maker CloudPets which stores the "personal information, photos and recordings of children's voices" was hacked and the data was held for ransom.[146] With sufficient computing power, pho-

---

manager was unwilling to guarantee that "the company wouldn't share its faceprint database with third parties").

[141] WAYNE PENNY, SANS INST., BIOMETRICS: A DOUBLE EDGED SWORD—SECURITY AND PRIVACY 8 (2002), https://www.sans.org/reading-room/whitepapers/authentication/biometrics-double-edged-sword-security-privacy-137 [https://perma.cc/LCT9-MRHP].

[142] *Id.* at 6.

[143] De Chant, *supra* note 56.

[144] Kellogg, *supra* note 17, at 76.

[145] *See generally* M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011) (discussing various theories of privacy harm: "unwanted observation" and "unanticipated or coerced use of information concerning a person against that person"); Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. (forthcoming), https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2885638 [https://perma.cc/AC5J-XPHF] (discussing consumer harms from data breaches and contending that courts should be willing to recognize such harms although they are "intangible, risk-oriented, and diffuse").

[146] Selena Larson, *Stuffed Toys Leak Millions of Voice Recordings from Kids and Parents*, CNN: TECH (Feb. 27, 2017, 11:04 PM), http://money.cnn.com/2017/02/27/technology/cloudpets-data-leak-voices-photos/index.html [https://perma.cc/J83T-X8PM].

tographs and audio voice recordings can be easily transformed into biometric identifiers, such as voice or face prints, and enable facial recognition technology "to identify one face from millions in under one second."[147]

Even if biometric data are stored solely on a device, and a company promises that its implemented security measures ensure that the company, and other applications or software programs and servers do not have access to the data, it may be possible to breach the company's security measures. For instance, in connection with Apple's Touch-Id, which allegedly stores only a "mathematical representation" of scanned fingerprints, Apple's website states that "[i]t isn't possible for someone to reverse engineer your actual fingerprint image from" the mathematical representation.[148] Nevertheless, the company attempts to limit its potential liability for "damage to, compromise, or corruption of data" in the limited warranty it provides to consumers by expressly noting that Apple is not responsible in such instances.[149] The company's end user license agreement contains a similar provision.[150] There have been previous reports of Touch-Id hacks that allowed parties to unlock Apple devices and potentially gain access to data stored on the device.[151] The company's recent decision to use facial recognition technology in connection with its

---

[147] *Facial Recognition: Why 2018 Will Be a Landmark Year for Artificial Intelligence*, THE ECONOMIST: FILMS, http://films.economist.com/the-world-in-2018 [https://perma.cc/EPW2-EFJ3] (discussing the ease and speed with which software programs and machines can transform photographs into face prints that are used to identify individuals and the implications of same); *Biometrics*, PRIVACY INT'L, https://www.privacyinternational.org/node/70 [https://perma.cc/ST9K-N69L] ("If an individual's voice—an entirely unique sound—is recorded its frequency pattern and spectrum can be used to generate a voiceprint, a voice profile linked to their identity."); Jeff John Roberts, *Judge Says Customers Can Sue Over Face Scans*, FORTUNE (Sept. 19, 2017), http://fortune.com/2017/09/19/shutterfly-face-scan [https://perma.cc/4U55-Z4C9] (discussing how photographs can be used by companies to generate geometrical facial data); James Vincent, *Lyrebird Claims It Can Recreate Any Voice Using Just One Minute of Sample Audio*, THE VERGE (Apr. 24, 2017, 12:04 PM), https://www.theverge.com/2017/4/24/15406882/ai-voice-synthesis-copy-human-speech-lyrebird [https://perma.cc/7M3J-BQG2] (discussing the use of artificial intelligence to easily transform audio recordings into voice-prints).

[148] *Apple Privacy Policy*, *supra* note 90.

[149] *Apple One (1) Year Limited Warranty*, APPLE, http://www.apple.com/legal/warranty/products/ios-warranty-document-us.html [https://perma.cc/NPA3-BPDV] (warranty for "iPhone, iPad, iPod, and Apple TV"); *Apple One (1) Year Limited Warranty*, APPLE, http://www.apple.com/legal/warranty/products/warranty-us.html [https://perma.cc/D676-DRZ7] (warranty for "Apple Branded Products Only").

[150] *Apple Inc. iOS Software License Agreement: Single Use License*, APPLE, http://images.apple.com/legal/sla/docs/iOS11.pdf [https://perma.cc/327Q-986T] ("[I]n no event shall Apple . . . be liable for . . . corruption or loss of data.").

[151] Mathew J. Schwartz, *Apple iPhone 6 Touch ID Hacked*, BANK INFO. SECURITY (Sept. 23, 2014), http://www.bankinfosecurity.com/apple-iphone-6-touchid-hacked-a-7348 [https://perma.cc/25US-ETKA]; *see also* Seth Rosenblatt, *Apple's Touch ID Still Vulnerable to Hack, Security Researcher Finds*, CNET (Sept. 23, 2014, 6:14 PM), https://www.cnet.com/news/apples-touch-id-still-vulnerable-to-hack-security-researcher-finds [https://perma.cc/NWH3-DEAV] (noting that the Touch ID security was not significantly improved from the iPhone 5S to the iPhone 6).

newer devices evidences the extent to which companies are integrating various types of biometrics into their products and widens the breadth of potential harms to consumers.[152]

A company that stores mathematical representations of biometric images solely on a consumer's device could elect in the future to store or provide access to this information via the cloud. For instance, one commentator reports that a patent filing by Apple describes a "biometric sensor data synchronization" system in which biometric data on one device can be transferred to the cloud and synced with other devices.[153] Transferring biometric data to the cloud presents security concerns because cloud-based systems are not immune from intrusion.[154]

Since IoT devices frequently communicate and transmit data amongst various devices in a consumer's home, "the least secure device becomes the security level for all [of a consumer's] devices."[155] The home of the average

---

[152] *Does Apple's Facial Recognition Technology Compromise Security for Convenience?*, CBS NEWS (Sept. 16, 2017, 12:13 PM), https://www.cbsnews.com/news/how-apples-facial-recognition-technology-compromises-security/ [https://perma.cc/EMY6-VV2M] (discussing implications of the iPhone X's new facial recognition technology "which uses a 3-D scan of the user's face to unlock the phone").

[153] U.S. Patent Appl. No. 13/938392 (filed July 10, 2013); Lance Whitney, *Apple Eyes Way to Leave Fingerprints in the Cloud*, CNET (Jan. 15, 2015, 6:04 AM), https://www.cnet.com/news/apple-eyes-way-to-sync-your-touch-id-data-in-the-cloud/ [https://perma.cc/NKZ4-98HM].

[154] Thomas Barrabi, *Why Hackers Love the Cloud*, FOX BUS. (Dec. 16, 2016), http://www.foxbusiness.com/features/2016/12/16/why-hackers-love-cloud.html [https://perma.cc/8HY9-EFQP] ("The problem with the cloud is that it simply expands the systemic vulnerabilities that have existed since the Internet was developed.") (internal quotation marks omitted); Nina Cunningham & Altman Weil, *The Myth of the Secure Cloud*, LEGAL TECH NEWS (Oct. 4, 2017, 11:18 AM), https://www.law.com/legaltechnews/almID/1202799610449/ [https://perma.cc/TN8U-8AWT] (discussing security issues associated with the cloud).

[155] Kellogg, *supra* note 17, at 78. A potentially influential legislative response in this area may be forthcoming. *See* S. 1691, 115th Cong. (2017) (proposing the "Internet of Things (IoT) Cybersecurity Improvement Act of 2017" to impose "security requirements" on IoT companies for IoT devices provided to the U.S. government); Allison Grande, *Senate Bill Would Up Internet of Things Device Security*, LAW360 (Aug. 2, 2017, 8:57 PM), https://www.law360.com/articles/950047/senate-bill-would-up-internet-of-things-device-security [https://perma.cc/STF7-V4KW] (noting that although the proposed "bill is directed toward only those manufacturers that sell their devices to the government, [experts predict] . . . that 'if they can influence companies to meet those standards to win federal business, those companies will likely adopt those same best practices more broadly for developing products for people across the country to buy'"); *see also* Allison Grande, *Equifax Fallout Could Boost Consumers' Shaky Harm Claims*, LAW360 (Oct. 6, 2017, 11:29 PM), https://www.law360.com/articles/972241/equifax-fallout-could-boost-consumers-shaky-harm-claims [https://perma.cc/63XV-2UMC] (discussing proposals by various U.S. senators and representatives to impose on companies "fixed statutory damages" in favor of consumers in the event of a data breach and shift the burden "to companies to ensure that consumers are made whole, regardless of whether individuals have suffered identity theft or any other actual harm"). Lastly, a proposed bill in California would, if adopted, impose reasonable security standards on manufacturers that sell IoT devices to consumers. *See* S.B. 327, 2017–2018 Leg., Reg. Sess. (Cal. 2017) (proposing to require manufacturers of IoT devices "to equip the device with reasonable security features appropriate to the nature of the device and the information it may collect, con-

consumer contains thirteen IoT devices.[156] While the manufacturer of one IoT device may take steps to build security and privacy into its device, if one device in a consumer's home is susceptible to intrusion, all other devices are rendered vulnerable. Thus, because multiple devices are integrated in the IoT setting, foreign and domestic hackers are provided with multiple points of entry and chances to obtain highly sensitive consumer data.

3. Non-Consensual Disclosures and Initial Data Collectors

IoT companies could also disclose biometric and health-related data without obtaining consumer consent or providing notice of data collection or transfer. Manufacturers of children IoT toys, such as My Friend Cayla and i-Que Robot, have allegedly collected and shared with third parties audio files of children's voices and their private conversations without obtaining parental consent.[157] As noted earlier, companies and hackers can easily transform voice recordings into voice prints that can be used to identify consumers.[158] IoT toys also suffer from significant security vulnerabilities, and as a result, hackers may be able to communicate with children through the toys.[159] While consumer consent should not be used to justify data collection practices that are detrimental to consumers, the intentional unauthorized disclosure of consumer biometric data by IoT companies is particularly egregious given the immutable and singular nature of most biometric data.

Even when biometric and health-related data are not at issue, companies may also collect and transfer other types of consumer data without first obtaining consent. Vizio, Inc., a manufacturer of Internet-enabled televisions, covertly tracked consumers' viewing habits and disclosed and sold this information to unaffiliated parties without obtaining appropriate consumer consent.[160] Bose, a manufacturer of wireless headphones, has been

---

tain, or transmit, that protect it from unauthorized access, destruction, use, modification, or disclosure.").

[156] Rich Handley, *Cuebiq Database Offers IoT Device Usage Data to Marketers*, RFID J. (Aug. 4, 2017), http://www.rfidjournal.com/articles/view?16435 [https://perma.cc/9GEW-ERP4].

[157] Allison Grande, *Groups Say 'Spy Toys' Don't Play Well with Privacy Regs*, LAW360 (Dec. 7, 2016, 6:44 PM), https://www.law360.com/articles/870122 [https://perma.cc/EM5J-88KS] [hereinafter Grande, *Spy Toys*]; *see also* Press Release, Fed. Trade Comm'n, Electronic Toy Maker VTech Settles FTC Allegations that It Violated Children's Privacy Law and the FTC Act (Jan. 8, 2018) (on file with the Federal Trade Commission) (discussing the FTC's settlement agreement with IoT toy maker Vtech for allegedly collecting child data without obtaining parental consent and failing to implement adequate security measures with respect to such data).

[158] *See supra* note 147 and accompanying text.

[159] Grande, *Spy Toys*, *supra* note 157.

[160] Press Release, Fed. Trade Comm'n, Vizio to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions Without Users' Consent (Feb. 6, 2017) (on file with the Federal Trade Commission); Allison Grande, *Vizio's TV Snooping Flouts Privacy Laws, Consumers Say*, LAW360 (Nov. 7, 2016, 9:54 PM), https://www.

accused of surreptitiously collecting and disclosing to unaffiliated entities consumers' "listening habits" without acquiring consumer authorization.[161] Information about a consumer's audio listening habits "including music, radio broadcast, Podcast, and lecture choices—provide an incredible amount of insight into his or her personality, behavior, political views, and personal identity."[162] These examples suggest that companies are indeed willing to collect, transfer and disclose consumer data without obtaining consumer consent, and companies could very easily engage in similar practices with respect to biometric and health-related data despite the highly-sensitive and irreplaceable nature of such data.

II. DATA TRANSFERS & COMMERCIAL REGIMES

As the foregoing Part demonstrates, consumers may face significant harms when their IoT data are collected, monetized, and disclosed by companies, and existing privacy policies frequently authorize the collection, transfer, and disclosure of consumer data.[163] However, privacy policies are not alone in enabling this process. Commercial frameworks that permit the commodification of consumer data can also play a significant role in facilitating the transfer and disclosure of consumer data in ways that are non-transparent and potentially detrimental to consumer interests. The secured transactions rules of Article 9 and the Bankruptcy Code are examples of commercial frameworks that provide various avenues for the subsequent transfer, assignment, and disclosure of consumer data to third parties.

After IoT data are disclosed and transferred to third parties through these financial frameworks, many of the resulting harms to consumers forecasted in Part I above are likely to follow.[164] The databases and servers of transferees, debtors, and secured parties are not immune from hacking, and transferees may subsequently disclose IoT data to third parties. Transferees may also deploy data analytics to mine and monetize their newly acquired data assets and use the data in ways that are harmful to consumer interests. Transferees could also begin using online "pay-for-privacy" models to fur-

---

law360.com/articles/860311/vizio-s-tv-snooping-flouts-privacy-laws-consumers-say [https://perma.cc/93MY-KFV2].

[161] Jeff John Roberts, *These Popular Headphones Spy on Users, Lawsuit Says*, FORTUNE (Apr. 19, 2017), http://fortune.com/2017/04/19/bose-headphones-privacy/ [https://perma.cc/4P4G-KMKK] [hereinafter Roberts, *Headphones*]; *see also* Allison Grande, *Bose, Secret Messaging App Hit with Privacy Suits*, LAW360 (Apr. 19, 2017, 9:41 PM), https://www.law360.com/articles/914824/bose-secret-messaging-app-hit-with-privacy-suits [https://perma.cc/KK4F-MZWG] (noting that Bose shared "app users' listening habits" with a data mining company).

[162] Roberts, *Headphones*, *supra* note 161.

[163] *See supra* notes 77–129 and accompanying text (discussing privacy policies); *supra* notes 131–162 and accompanying text (discussing consumer harms).

[164] *See supra* notes 131–162 and accompanying text.

ther extract value from the data. As I have noted elsewhere, although the wealthy may have always had more privacy, use of pay-for-privacy models in the IoT and online settings may exacerbate concerns about unequal access to privacy for vulnerable consumers.[165] Most importantly, the possible disclosure and transfer of biometric and health-related data to a third party through these financial frameworks is a significant privacy harm given the highly sensitive nature of these types of data.

A. Article 9 of the UCC

To obtain financing from lenders, companies routinely offer their personal property as collateral to secure funds. With some exceptions, Article 9 governs transactions that "create[] a security interest in personal property or fixtures by contract."[166] Thus, Article 9 provides detailed rules for creating and perfecting a security interest.[167] Through the process of "attachment" the parties create a security interest that is "enforceable against the debtor and third parties," and through "perfection" a lender notifies third parties of its interest in the debtor's collateral.[168] If a lender is the first to file or properly perfect its security interest in the collateral using the various methods provided under Article 9, the lender will generally have priority over other third parties claiming a security interest in the same collateral, subject to the lender retaining its filing or perfection status and a few other exceptions.[169] Priority may become a hotly contested issue between competing lenders when the debtor files for bankruptcy.

Article 9 delineates numerous categories for different types of personal property that qualify as Article 9 collateral.[170] The type of collateral that is offered by a company to secure a loan from a lender impacts the specific rules that govern the creation and perfection of the lender's security interest in the collateral. For instance, a lender may typically perfect its security interest in a debtor's "inventory" or "equipment" by filing a financing statement or by effectuating a "possession" of the collateral.[171] On the other

---

[165] Elvy, *supra* note 92, at 1399–1411.

[166] U.C.C. § 9-109(a)(1) (AM. LAW INST. & UNIF. LAW COMM'N 2017).

[167] *See, e.g.*, *id.* §§ 9-201 to -206, 9-301 to -316; LINDA J. RUSCH & STEPHEN L. SEPINUCK, PROBLEMS AND MATERIALS ON SECURED TRANSACTIONS 49 (3d ed. 2014) (noting that Article 9 created a "simple and unified structure within which the immense variety of modern secured financing transactions involving personal property could occur").

[168] U.C.C. §§ 9-203(a), 9-308; RUSCH & SEPINUCK, *supra* note 167, at 223–24 ("[A]ttachment is all a secured party needs to have a security interest that is enforceable against the debtor . . . [and] a perfection method—is, in many instances, the provision of some form of notice to the commercial world of the secured party's interest in the collateral.").

[169] U.C.C. §§ 9-110, 9-322, 9-324, 9-328.

[170] *Id.* § 9-102(a) (defining various forms of personal property).

[171] U.C.C. §§ 9-310, 9-313; RUSCH & SEPINUCK, *supra* note 167, at 249.

hand, if the collateral provided to secure the loan is "investment property," the lender can generally perfect either by filing a financing statement or by obtaining "control" of the collateral.[172]

Under Article 9, a company's customer database, "the modern version of the customer list," is likely a general intangible.[173] Customer databases can include very detailed data about consumers.[174] Recall that in the IoT era, the customer databases of today's companies could potentially expand to include biometric, health-related, and other highly sensitive data about consumers.[175] Thus, new types of data that were not previously accessible to companies on a wide scale or seen in customer databases could become part of a company's assets. Although some companies may store only voice recordings or photographs in their databases, businesses can convert these data into biometric identifiers, such as voice or face prints, at any time.[176]

To the extent that biometric data are stored only on a device and are not accessible to IoT companies, the information is unlikely to be part of the company's customer database. However, as noted, IoT manufacturers of children's products have allegedly disclosed audio files of children's voices to third parties that could be used to generate voice prints that can identify individuals.[177] Consider that the Amazon Echo—an IoT device—records and stores consumers' "voice requests."[178] These recordings are retained on the company's servers (even after consumers delete their voice recordings from the IoT device) and can be transformed into voice prints.[179] Thus, bi-

---

[172] U.C.C. §§ 9-310, 9-314 (AM. LAW INST. & UNIF. LAW COMM'N 2017); RUSCH & SEPINUCK, *supra* note 167, at 249.

[173] Jonathan C. Lipson, *Financing Information Technologies: Fairness and Function*, 2001 WIS. L. REV. 1067, 1081; *see* U.C.C. § 9-102(a)(42) (defining general intangible as "any personal property, including things in action, other than accounts, chattel paper, commercial tort claims, deposit accounts, documents, goods, instruments, investment property, letter-of-credit rights, letters of credit, money, and oil, gas, or other minerals before extraction," including "payment intangibles and software"); *In re* Emergency Beacon Corp., 23 U.C.C. Rep. Serv. 766, 769–70 (S.D.N.Y. 1977) (finding that customer lists are general intangibles under Article 9); Miller & O'Rourke, *supra* note 36, at 788–89 (noting that customer lists are viewed as general intangibles under Article 9); Nguyen, *Collateralizing*, *supra* note 19, at 580 (asserting that customer databases are general intangibles).

[174] Miller & O'Rourke, *supra* note 36, at 782 (noting that customer lists can include "simply basic information like names and addresses, or exhaustive data on a customer's financial position and shopping preferences").

[175] *See supra* notes 49–76 and accompanying text.

[176] *See infra* note 178 and accompanying text.

[177] *See supra* note 147, 157 and accompanying text.

[178] Tim Moynihan, *Alexa and Google Home Record What You Say. But What Happens to That Data?*, WIRED (Dec. 5, 2016, 9:00 AM), https://www.wired.com/2016/12/alexa-and-google-record-your-voice/ [https://perma.cc/S4T7-ELDL].

[179] *Id.*; *see also* Jing Cao & Dina Bass, *Why Google, Microsoft and Amazon Love the Sound of Your Voice*, BLOOMBERG (Dec. 13, 2016, 6:00 AM), https://www.bloomberg.com/news/articles/2016-12-13/why-google-microsoft-and-amazon-love-the-sound-of-your-voice [https://perma.cc/

ometric related data may not always be stored solely on an IoT device, and in many instances, may be part of a company's customer database and subject to assignment. Moreover, regardless of how or where the data are stored or processed, "most of the means of online production (in terms of hardware, software, content or data) are . . . . increasingly owned or at least *de facto* controlled by large companies."[180]

Companies have long offered their customer databases or lists (along with other types of assets) as collateral to obtain financing.[181] Article 9's framework facilitates this process.[182] As these databases and the data become even more valuable in the IoT setting, this practice may continue and possibly become more widespread.

A lender may create an enforceable security interest in a company's customer database or list by having the debtor authenticate a security agreement that contains a sufficient "description of the collateral."[183] The debtor should also have "rights in the collateral or the power to transfer rights in the collateral" to the lender, and value must be exchanged in the transaction, which typically occurs through the lender's provision of funds.[184] To preserve its priority status and provide notice of its interest in the company's customer list or database the lender may perfect by filing a financing statement in the appropriate filing office.[185] Lenders and debtors are not required to describe in detail in their agreement the type of collateral

---

K98B-F32D] ("Every hour, Amazon uploads Alexa queries to a vast digital warehouse."); Lisa Eadicicco, *Exclusive: Amazon Developing Advanced Voice-Recognition for Alexa*, TIME (Feb. 27, 2017), http://time.com/4683981/amazon-echo-voice-id-feature-2017/ [https://perma.cc/5RLM-LG4M] (discussing Amazon's expected use of "'voice print' to verify a person's identity" in connection with its IoT products); Kim Komando, *How to Listen to Everything Amazon Echo Has Ever Heard*, FOX NEWS (Apr. 15, 2017), http://www.foxnews.com/tech/2017/04/15/how-to-listen-to-everything-amazon-echo-has-ever-heard.print.html [https://perma.cc/9KWX-RB7E] ("The downside is that Amazon stores a recording of every voice command you've issued to Alexa—not just in the device itself, but on Amazon's servers."); Vincent, *supra* note 147 ("[A] Canadian AI startup named Lyrebird . . . claims [it] can clone anyone's voice by listening to just a single minute of sample audio."); *Biometrics*, *supra* note 147 (discussing the use of audio recordings to identify individuals).

[180] Primavera De Filippi & Smari McCarthy, *Cloud Computing: Centralization and Data Sovereignty*, 3 EUR. J.L. & TECH. 1, 1 (2012).

[181] Nguyen, *Collateralizing*, *supra* note 19, at 577.

[182] *See infra* notes 183–249 and accompanying text.

[183] U.C.C. §§ 9-108, 9-203(b)(3)(A) (AM. LAW INST. & UNIF. LAW COMM'N 2017) (providing the requirements for "reasonably identify[ing]" collateral).

[184] *Id.* § 9-203(b)(2).

[185] Nguyen, *Collateralizing*, *supra* note 19, at 579 ("If a consumer database is not protected under copyright law and not registered by the Copyright Office, the security interest in the consumer database is perfected by filing a financing statement with the Office of the Secretary of State.").

that is subject to the security interest.[186] With some exceptions, the parties can simply use the applicable Article 9 collateral label.[187] Further, the financing statement may list the collateral as a general intangible or when appropriate "all assets or all personal property" of the debtor.[188]

As one scholar has noted, because Article 9 does not require the lender to clearly specify that it has obtained a security interest in a company's customer database or list, "the public will not know whether 'general intangible' means trademarks, patents, . . . payment intangibles, . . . or consumer databases."[189] Thus, consumers will be unable to determine whether their biometric, health-related, or other types of highly sensitive data have been assigned by a company that has obtained the data as a result of the consumer's use of an IoT device.

Once the lender creates an effective security interest in a company's customer database or list through the process of attachment, Article 9 provides the lender with several rights when the company is in default.[190] Article 9 does not contain a definition of the term "default."[191] As such, the provisions of the parties' security agreement regarding an event of default typically govern.[192] In some instances, state statutes may limit the permissible events of

---

[186] *Id.* at 586 ("[A]rticle 9 does not require the parties to the security agreement to have a detailed description of the 'type of the collateral'; as long as the collateral is identified as a type of collateral, no detailed description is necessary."); RUSCH & SEPINUCK, *supra* note 167, at 63 ("[A]lthough the UCC authorizes parties to describe collateral—in their private agreements and in certain public notices—by its classification, it does not require that they do so.").

[187] U.C.C. § 9-108(a)–(b) ("[A] description of collateral reasonably identifies the collateral if it identifies the collateral by (1) specific listing; (2) category . . . ."). *But see id.* § 9-108(c) (prohibiting a description of collateral as "all the debtors' assets or all the debtor's personal property" in the agreement); *id.* § 9-108(e) (listing instances in which "description only by collateral type is insufficient").

[188] *Id.* § 9-504 ("A financing statement sufficiently indicates the collateral that it covers if the financing statement provides: (1) a description of the collateral pursuant to section 9-108 or (2) an indication that the financing statement covers all assets or all personal property."); RUSCH & SEPINUCK, *supra* note 167, at 234 ("[U]nlike a security agreement, a financing statement may describe the collateral it covers as 'all assets' or 'all personal property.' If it does not use such a broad description, the standard for the description is the same standard as for the security agreement.").

[189] Nguyen, *Collateralizing*, *supra* note 19, at 586.

[190] *See, e.g.*, U.C.C. § 9-601 (AM. LAW INST. & UNIF. LAW COMM'N 2017); RUSCH & SEPINUCK, *supra* note 167, at 140 ("Article 9 conditions many of the secured party's enforcement rights upon the existence of a 'default.'").

[191] RUSCH & SEPINUCK, *supra* note 167, at 140 ("Article 9 does not define 'default.' Instead, what constitutes a default is governed by the parties' security agreement or lending agreement.").

[192] *Id.*; *But see In re* Eastep, 562 B.R. 783, 788 n.3 (Bankr. W.D. Okla. 2017) (noting that although the "term 'default' is not defined in the UCC," Section 9-201(b) authorizes the use of state consumer protection statutes to define an event of default in transactions involving consumers and the state statute at issue provided that "a default exists in a consumer credit transaction only if 'the consumer fails to make a payment as required by the agreement,' or 'the prospect of payment, performance, or realization of collateral is significantly impaired'") (internal quotation marks and citations omitted); *In re* Visnicky, 401 B.R. 61, 66 (Bankr. D. R.I. 2009) ("A current

default in consumer credit transactions.[193] Various events may qualify as a default under a security agreement, including the IoT company's failure to make timely payments on the loan provided in connection with the Article 9 transaction.[194] Because not all security agreements are publicly distributed, consumers may be unable to determine what events may trigger an event of default under the agreement. Further, even if these contracts were routinely made public and widely distributed by companies and lenders, it is unlikely that consumers would be able to understand the terms of the agreement and its data disclosure implications.

One could contend that consumers simply do not care about privacy or security. Yet, recent research suggests that consumers are indeed concerned about their lack of control over their data.[195]

Another potential critique regarding concerns about security interests in customer databases is that much of the data may be anonymized and aggregated or such databases could primarily contain metadata.[196] However, as one scholar has noted, anonymized electronic health records and data can be re-identified through various means which could impact "tens of thousands or even hundreds of thousands of records."[197] In some instances, "simple code[s] could unlock patients'" identifying information.[198] Moreover, "metadata of all sorts can reveal much about an individual."[199] Consumers

---

trend in the consumer credit area is that '[b]oth legislatures and courts are chipping away at the open-ended concept of default in consumer credit transactions,' by defining default objectively . . . .") (brackets in original).

[193] UNIF. CONSUMER CREDIT CODE § 5.109 (UNIF. LAW COMM'N 1974) (limiting an event of default to failure to make payment or the possibility of "significant impairment"); 10A HAWKLAND UCC SERIES § 6:39, Westlaw (database updated Dec. 2017) ("The Uniform Consumer Credit Code (U3C), either the 1968, 1974 or a modified version, is the law in ten states . . . .").

[194] RUSCH & SEPINUCK, *supra* note 167, at 140.

[195] Lee Rainie & Maeve Duggan, *Privacy and Information Sharing*, PEW RES. CTR. (Jan. 14, 2016), http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf [https://perma.cc/8B5B-2ZD8].

[196] Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 873 (2016) (contending that "[c]ourts have not resolved the question of whether metadata deserves lesser protection than other data"); Schwartz, *supra* note 9, at 2070 (defining metadata as "information about information").

[197] SHARONA HOFFMAN, ELECTRONIC HEALTH RECORDS AND MEDICAL BIG DATA: LAW AND POLICY 137 (2016); *see also* Frederik Zuiderveen Borgesius et al., *Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework*, 30 BERKELEY TECH. L.J. 2073, 2121 (2015) ("Irreversible anonymization is difficult—perhaps impossible."); Marc A. Rodwin, *Patient Data: Property, Privacy & the Public Interest*, 36 AM. J.L. & MED. 586, 613–14 (2010) (discussing companies' sale of patient data and the use of anonymization to vindicate the practice).

[198] Adam Tanner, *The Hidden Global Trade in Patient Medical Data*, YALEGLOBAL ONLINE (Jan. 24, 2017), http://yaleglobal.yale.edu/content/hidden-global-trade-patient-medical-data [https://perma.cc/9WVM-PNTU].

[199] Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 556 (2017). Donohue further contends that:

can also be re-identified from metadata.[200] Thus, even if anonymized data is used in secured transactions and even if one contends that consumers have no property interest in anonymized data, the risk of re-identification remains.

If an IoT company is in default the lender has the ability to exercise its rights as set forth in its agreement with the IoT company (subject to some exceptions) as well as specific rights provided in Article 9.[201] Upon default, the lender "may sell, lease, license or otherwise dispose" of the collateral.[202] The disposition of the collateral by the lender must be "commercially reasonable."[203] In many instances, the lender may also retain the collateral "in full or partial satisfaction" of the debt upon receiving the debtor's consent.[204] Thus, when an IoT company has used its customer database as security and has defaulted under the security agreement, the lender can generally do what it pleases with the customer database to satisfy the debtor's obligations.

Many privacy policies do not specifically address the creation of a security interest in consumer data but rather contain generic language described in Part I.B authorizing the sale or transfer of customer data in certain business transactions.[205] A secured financing transaction under Article 9 may qualify as a business transaction depending on the specific language of the privacy policy. For instance, as discussed above, Nest's privacy policy authorizes the disclosure and transfer of consumer data upon the "sale or transfer of the company and/or all or part of its assets."[206] Since customer databases or lists could be viewed as company assets, once a security interest is created in the database, it could be sold when the IoT company fails to pay the loan, and the sale could arguably be in accordance with the company's privacy policy. Unless the IoT company files for bankruptcy or it pro-

---

> [L]aw enforcement regularly uses search terms to bring criminal charges against individuals. The reason is simple: patterns in phone calls, text messages, instant messaging, emails, or even URL visits demonstrate beliefs, relationships, and social networks—yet the form of that data (metadata) has not historically been considered content. The same is true of consumer metadata and financial records. Sophisticated pattern analytics mean that non-content morphs into content, making any formal distinction meaningless.

Id.

[200] Ferguson, *supra* note 196, at 873 ("[T]he line between data and metadata in the context of billions of connected things becomes vanishingly thin. Metadata can reveal personal information just like content."); Montjoye et al., *supra* note 122, at 536 (contending that metadata "contain sensitive information," discussing the use of metadata by large companies, such as Netflix and Google, and finding that individuals can be re-identified from "credit card metadata").

[201] U.C.C. §§ 9-601, 9-602 (AM. LAW INST. & UNIF. LAW COMM'N 2017).

[202] *Id.* § 9-610(a).

[203] *Id.* § 9-610(b).

[204] *Id.* § 9-620.

[205] *See supra* notes 77–129 and accompanying text.

[206] *Nest Product Privacy Policy*, *supra* note 85; *see supra* note 86 and accompanying text.

vides notice (assuming that its privacy policy requires it to do so), consumers may be unaware that their data will be transferred to a third party once the IoT company is in default.[207] Thus, not only are consumers unaware of the various events that may trigger a default under the security agreement between the lender and the IoT company, but they may also not be informed when the event of default or subsequent data transfer and disclosure occurs. Many of the privacy frameworks discussed in Part III below rely on a notice and choice model to protect consumers.[208] Yet, in this area consumers are unlikely to receive sufficient notice.

B. Data Ownership vs. Rights in the Data

The question of who owns the data or who has rights in the data generated by IoT devices is a vexing one.[209] One could contend that consumers, and not IoT companies, are the true owners of consumer data particularly because consumers generate the data by using IoT devices, mobile applications, and websites.[210]

Commentators have adopted contrasting positions on questions of data ownership, rights in data and the legal regimes that should govern related issues. Indeed, "[t]he idea that personal information is property has been

---

[207] Nguyen, *Collateralizing*, *supra* note 19, at 592–93.

[208] *See infra* notes 263–390 and accompanying text.

[209] Mark A. Hall, *Property, Privacy, and the Pursuit of Interconnected Electronic Medical Records*, 95 IOWA L. REV. 631, 631 (2010) ("Who owns a patient's medical information? The patient, the provider, or the insurer? All of the above? None of the above? In the emerging era of electronic medical records, no legal question is more critical, more contested, or more poorly understood."); Mauricio Paez & Mike La Marca, *The Internet of Things: Emerging Legal Issues for Businesses*, 43 N. KY. L. REV. 29, 65 (2016) (discussing the lack of clarity regarding whether consumers or merchants own IoT data and contending that "the consumer owns the physical media where the data is stored," but different merchants "along the data processing chain can assert valid ownership of such data"); Peppet, *supra* note 12, at 95 (discussing IoT devices and contending that privacy policies do not clearly indicate who owns the data collected by such devices); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1130–31 (2000) ("[T]he traditional view in American law has been that information as such cannot be owned by any person.").

[210] Plaintiffs' Opposition to Defendants' Motion to Dismiss Consolidated Class Action Complaint at 29, *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., No. 11MD02258 (S.D. Cal. May 14, 2012), 2012 WL 2339054 (contending that "[p]ersonal [i]nformation is property just as much as website domains . . . and [p]laintiffs gave the[ir] [p]ersonal [i]nformation to [the defendant] for use for a limited period of time"); Vera Bergelson, *It's Personal but Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 384 (2003) (advocating for a property approach to personal information prior to the rise of IoT and contending that "individuals have a stronger moral claim to personal information than collectors"). *But see In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 974 (S.D. Cal. 2012) (stating that "the Court is hard pressed to conceive of how [p]laintiffs' [p]ersonal [i]nformation could be construed to be personal property so that [p]laintiffs somehow 'delivered' this property to Sony and then expected it be returned").

widely debated."[211] Some scholars argue that personal data should be viewed as property.[212] One commentator posits that "privacy as property has taken hold in the courts."[213] On the other hand, some case law suggests and several privacy law scholars contend that individuals do not have a property interest in their personal information.[214] At least one court has been reluctant to extend the holding in such cases to all claims involving consumer data.[215] Courts appear to be unwilling to find that "it is categorically impossible for [consumers] to allege some property interest that [is] compromised

---

[211] Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 MD. L. REV. 335, 373 (2013).

[212] *E.g.*, ALAN F. WESTIN, PRIVACY AND FREEDOM 324–25 (1967) ("[P]ersonal information, thought of as the right of decision over one's private personality, should be defined as a property right, with all the restraints on interference by public or private authorities and due-process guarantees that our law of property has been so skillful in devising."); Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 63–65 (1999) ("A property regime gives the holder of the property right the power to hold out—until the buyer is willing to pay what the seller demands.").

[213] Lauren Henry Scholz, *Privacy as Quasi-Property*, 101 IOWA L. REV. 1113, 1121 (2016).

[214] Order Granting Defendant's Motions to Dismiss for Lack of Article III Standing with Leave to Amend, *In re* iPhone Application Litig., No. 11-MD-02250-LHK, 2011 WL 4403963, at *14 (N.D. Cal. Sept. 20, 2011) (stating that to "assert a [California Unfair Competition Law] claim, a private plaintiff needs to have 'suffered injury in fact and lost money or property as a result of the unfair competition' [and] [n]umerous courts have held that a plaintiff's 'personal information' does not constitute money or property under" California's Unfair Competition Law) (internal modifications omitted); Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1030 (N.D. Cal 2012) ("[T]he weight of authority holds that a plaintiff's 'personal information' does not constitute property."); *In re* Facebook Privacy Litig., 791 F. Supp. 2d 705, 714 (N.D. Cal. May 12, 2011), *aff'd in part*, 572 Fed. App'x 494 (9th Cir. 2014) (holding that "personal information does not constitute property for purposes of" a claim under California's Unfair Competition Law); Ruiz v. Gap, Inc., 540 F. Supp. 2d 1121, 1126–27 (N.D. Cal. 2008), *aff'd*, 380 Fed. Appx. 689 (9th Cir. 2010) (finding that plaintiff did not present "any authority to support the contention that unauthorized release of personal information constitutes a loss of property"); Moore v. Regents of the Univ. of Cal., 793 P.2d 479, 487 (Cal. 1990) (holding no property interest exists in genetic data); Miller & O'Rourke, *supra* note 36, at 813 ("Even if the law were to put aside its usual focus on property interests under section 363 and hold that a customer has an 'interest' in her own information, it is unlikely also to hold that the customer has an interest in the aggregate list constituting the 'property' that the trustee seeks to sell."); John M. Newman, *Anti-Trust in Zero-Price Markets: Applications*, 94 WASH. U. L. REV. 49, 55 (2016) ("[C]ourts have been uniformly reluctant to treat personal information as property for general legal purposes."); Samuelson, *supra* note 209, at 1132 ("[H]owever intuitively powerful the notion of property rights in one's data may be, it is clear that in the United States the existence of some legally protectable interests in personal data in certain circumstances is not equivalent to a legal rule that a person has a property interest in one's personal data.").

[215] Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 811 (N.D. Cal 2011) (distinguishing the holdings in *In Re Facebook Privacy Litigation* and *In Re Iphone Application Litigation*, and stating "the [c]ourt finds the reasoning in this line of cases inapplicable to Plaintiffs' misappropriation claim, which, as previously discussed, is of an entirely different nature than a privacy tort claim. Plaintiffs here do not assert that their personal information has inherent economic value and that the mere disclosure of such data constitutes a loss of money or property"). In *Fraley*, the plaintiffs contended that Facebook "unlawfully misappropriated [their] names, photographs, likenesses, and identities for use in paid advertisements without obtaining [their] consent." *Id.* at 790.

by [a company's] alleged practices" with respect to their information.[216] Yet, some courts have also suggested that personal information has no value for which consumers can expect compensation.[217] Whether this perplexing view will continue in the emerging personal data economy ("PDE") setting in which various companies purport to provide platforms that allow individuals to monetize (and be directly compensated for) consumer-generated data and "take ownership of their information," remains to be seen.[218] In fact, in *In re Google Inc. Cookie Placement Consumer Privacy Litigation*—a class action alleging inappropriate collection of consumer data—the Third Circuit suggested that the plaintiffs needed to allege that they intended to monetize their data or "store[] their information with a future sale in mind."[219] The burgeoning PDE provides consumers with opportunities to sell, aggregate, store, and mine their personal information.[220] Lastly, other scholars contend that a property approach to personal data facilitates the

[216] LaCourt v. Specific Media, Inc., No. SACV 10-1256-GW(JCGx), 2011 WL 1661532, at *4 (C.D. Cal. Apr. 28, 2011). In *LaCourt*, the court indicated that it was willing to "recognize the viability in the abstract of such concepts as 'opportunity costs,' 'value-for-value exchanges,' [and] 'consumer choice' . . . ." *Id.*; *see also Fraley*, 830 F. Supp. 2d at 799 (discussing the *LaCourt* court's recognition of these concepts and suggesting that the court's decision *In re iPhone Application Litigation* acknowledged same).

[217] *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 327 (E.D.N.Y. 2005) ("[T]here is absolutely no support for the proposition that the personal information of an individual JetBlue passenger had any value for which that passenger could have expected to be compensated."); Stayart v. Google Inc., 783 F. Supp. 2d 1055, 1057 (E.D. Wis. 2011) ("[P]laintiff alleges no facts which suggest that her name has any commercial value . . . ."); Thomas B. Norton, *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model*, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 181, 194 (2016) ("Courts have also held that personally identifiable information is not considered property and thus has no compensable value, despite concrete evidence to the contrary.").

[218] MOBILE ECOSYSTEM FORUM, UNDERSTANDING THE PERSONAL DATA ECONOMY: THE EMERGENCE OF A NEW DATA VALUE-EXCHANGE 3, https://mobileecosystemforum.com//wp-content/uploads/2016/11/Understanding-the-Personal-Data-Economy-Whitepaper.pdf [https://perma.cc/CW3S-T4NT]; Elvy, *supra* note 92, at 1393–1400 (discussing personal data economy models). In *Fraley*, the court reasoned that the *In re iPhone Application Litigation* and *Low* decisions "found that the plaintiffs were unable to articulate how they were economically injured by the use of their own information to advertise to themselves and unable to articulate how the collection of demographic information was an economic loss to them." *Fraley*, 830 F. Supp. 2d at 798–99. In the personal data economy setting, consumers may be able to more easily establish economic value and loss of their information.

[219] 806 F.3d 125, 149 (3d Cir. 2015) (affirming district court's dismissal of plaintiff's California Unfair Competition Law and Computer Fraud and Abuse Act claims and reasoning that "the plaintiffs [did] not allege that they [participated in the 'market for internet history information' or] incurred costs, lost opportunities to sell, or lost the value of their data as a result of their data having been collected by others").

[220] Elvy, *supra* note 92, at 1393–1400 (discussing personal data economy models).

commodification of consumer data, while some commentators advocate for a contractual approach.[221]

Despite this scholarly debate, companies are currently commodifying consumer data as it has significant value for such entities and various legal frameworks may impact a company's rights in consumer related data. Further, although one may posit that consumers own or have rights in the data they generate, consumers frequently consent to the use of their information by IoT companies. Recall that Nest's privacy policy provides that by using the company's IoT products, consumers will be deemed to have consented to data collection, storage, and processing not only by Nest but also by the company's third-party service providers.[222] The policy also notes that consumer data may be "collected, stored and processed" on servers (and by parties) located in the "United States or in other countries."[223] Thus, consumers are potentially consenting to the international transfer of their data. Through this consent, consumers could be said to grant or authorize IoT companies to obtain rights in the data they generate, including the right to process, aggregate, anonymize, and transform the data. These rights can include a grant of a royalty-free license to use consumer data, the provisions of which may be contained in a company's privacy policy or terms of service.[224] Thus, through privacy

---

[221] Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POL'Y 591, 592 (1994) (calling for a contractual approach to privacy that "give[s] individuals the power to choose privacy or not without requiring privacy for everybody or nobody," and that allows companies to offer deals to consumers to prevent them from opting out of data collection and transfers); Barbara J. Evans, *Much Ado About Data Ownership*, 25 HARV. J.L. & TECH. 69, 77–108 (2011) (critiquing "data propertization" arguments in the healthcare context); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1301 (2000) (contending that a "property rights approach" to protecting data privacy in which individuals "own information about themselves . . . would tend to encourage the market in personal data rather than constrain[] it"). Some scholars have suggested that First Amendment concerns can be avoided by grounding privacy rights and regulation in contract law. *See, e.g.*, Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1204 (2005) [hereinafter Richards, *First Amendment*] (contending that "the regime of contract law grants policymakers a wide variety of regulatory tools, including the power to supply both default and mandatory terms to" regulate consumer privacy while simultaneously avoiding First Amendment challenges); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1050–51 (2000) ("While privacy protection secured by contract is constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law."). Richards suggests that a state could adopt legislation prohibiting the waiver of consumer privacy rights and such legislation would be evaluated "under the rational basis review reserved for economic regulation generally." Richards, *First Amendment*, *supra*, at 1204. However, several of the federal and state statutes evaluated in this Article continue to rely on consumer consent and the notice and choice model.

[222] *Nest Product Privacy Policy*, *supra* note 85.

[223] *Id.*

[224] *Facebook Statement of Rights*, *supra* note 133; *Terms of Service*, NEST, https://nest.com/legal/terms-of-service/ [https://perma.cc/84HD-RWB2] ("You hereby grant us with a nonexclusive, worldwide, royalty-free, perpetual, irrevocable, sublicenseable and transferable right to ac-

policies, IoT companies are arguably obtaining rights or interests in consumer generated data, and as one scholar notes "although privacy policies are principally creatures of contract, there are nascent elements of property that pervade the relationship."[225]

The "rights in data" versus "ownership of data" issue is an important distinction under Article 9. Customer databases and lists could be viewed as belonging to companies and subject to assignment.[226] Recall that to create an enforceable security interest against the debtor, the lender must ensure that the debtor has "rights in the collateral or the power to transfer rights in the collateral."[227] In *First National Bank v. Temple*, the court stated "all or some of [an] owner's rights can be transferred by way of a sale, lease or license [and] [a] person with transferable rights can grant an enforceable security interest in those rights."[228] In order for an IoT company to grant a security interest in its customer list or database, which contains biometric, health-related, or other types of highly sensitive data, full ownership of and title to the data by the company is likely not required.[229] However, if an IoT company has only limited rights in the data, the lender's security interest will normally attach only to those rights.[230] If a debtor has the power to

---

cess, display, or otherwise use your User Submissions," such as "text, graphics, articles, photographs, video, images, and illustrations," and "all related intellectual property rights . . . .").

[225] Edward J. Janger, *Muddy Property: Generating and Protecting Information Privacy Norms in Bankruptcy*, 44 WM. & MARY L. REV. 1801, 1818 (2003) (calling for the adoption of "muddy property rules" to regulate consumer data and contending that "if privacy norms for e-commerce transactions are to be enforced in bankruptcy, they need to be protected by property rights").

[226] CHARLENE BROWNLEE & BLAZE D. WALESKI, PRIVACY LAW § 7.08 (2017) ("It is fairly common practice for a business to consider and treat customer lists and the personal information collected from consumers as the property of the business."); Lipson, *supra* note 173, at 1082–83 ("[C]ustomer databases have become an important asset for both 'bricks and mortar' and Internet businesses, which increasingly capture valuable information about consumers . . . ."); Nguyen, *Collateralizing*, *supra* note 19, at 854.

[227] U.C.C. § 9-203(b)(2) (AM. LAW INST. & UNIF. LAW COMM'N 2017). A debtor is defined as "(A) a person having an interest, other than a security interest or other lien, in the collateral, whether or not the person is an obligor; (B) a seller of accounts, chattel paper, payment intangibles, or promissory notes; or (C) a consignee." *Id.* § 9-102(a)(28).

[228] 642 N.W.2d 197, 204 (S.D. 2002).

[229] State Bank of Young Am. v. Vidmar Iron Works, Inc., 292 N.W.2d 244, 249 (Minn. 1980) (noting that the UCC "does not require that collateral be owned by the debtor"); Border State Bank of Greenbush v. Bagley Livestock Exch., Inc., 690 N.W.2d 326, 332 (Minn. Ct. App. 2004) (noting that "[r]ights in the collateral, as the term is used in Article 9, include full ownership and limited rights that fall short of full ownership"); Greenbush State Bank v. Stephens, 463 N.W.2d 303, 306 (Minn. Ct. App. 1990) (noting that "'ownership' under the UCC can be shared, with each party possessing its own bundle of interests"); RUSCH & SEPINUCK, *supra* note 167, at 96 ("Article 9 does tell us that 'title' to the property is not particularly relevant."). *See generally* Heather Hughes, *Counterintuitive Thoughts on Legal Scholarship and Secured Transactions*, 55 BUFF. L. REV. 863, 878–81 (2007) (discussing debtor's rights in collateral under Article 9).

[230] U.C.C. § 9-203(b) cmt. 6 ("A debtor's limited rights in collateral, short of full ownership, are sufficient for a security interest to attach. However, in accordance with basic personal property

convey "another person's rights [in the collateral] only to a class of transferees that excludes secured parties," it is unlikely that a security interest can effectively encumber the collateral.[231]

An IoT company's use of a third-party technology service provider may muddle the question of rights in the collateral. As discussed earlier, IoT privacy policies may authorize IoT companies to share consumer data with third-party vendors and service providers. Depending on the terms of the service agreement, companies that provide data storage and analytics services could claim an interest in the data that they process on behalf of IoT companies.

If an IoT company elects to monetize its customer database by for instance licensing it to a third party or enters into an agreement with a third-party service vendor that processes the data, this third party could be viewed as having rights in the customer database or the data product derived from the database or list. To the extent that the third-party provider has rights in the customer database, list, or derived data product, and a secured party (lender) qualifies as a person to whom such rights can be transferred, the third-party provider could use the database or data product as collateral to obtain financing from the secured party. Consumer data (or the data product derived from such data) may then be at risk for foreclosure by another lender in addition to the lender of the IoT company that manufactures and sells the device to consumers. Consumers will likely be unaware of any such secondary assignment of rights in their data. IoT companies could attempt to avoid this problem by clearly limiting the ability of third-party service providers to encumber customer databases, lists, or data products derived from those sources in their agreements with such entities. However, various provisions in Article 9 address the impact of anti-assignment restrictions and, when applicable, these code sections may negate contractual terms that would impair the "creation, attachment or perfection of a security interest" in certain collateral. [232] Thus, in some instances "even if the source of [a] prohibition on transfer is . . . a contractual promise . . a debtor will generally still have the ability to grant" a security interest in the collateral under Article 9.[233]

Statutory liens in favor of service providers highlight another potential problem for IoT companies in this area and provide an additional avenue for

---

conveyancing principles, the baseline rule is that a security interest attaches only to whatever rights a debtor may have, broad or limited as those rights may be."). The comments section also notes that "certain exceptions to the baseline rule [mentioned above may] enable a debtor to transfer, and a security interest to attach to, greater rights than the debtor has." *Id.*

[231] *Id.* (describing as an example the concept of entrustment under section 2-403(2)).

[232] *Id.* § 9-408.

[233] RUSCH & SEPINUCK, *supra* note 167, at 96.

the transfer and disclosure of consumer IoT data. A state statute may grant service providers a lien on personal property for services or materials rendered in "making, repairing, improving or enhancing the value of" personal property.[234] Technology providers can be hired by companies to mine, manage, store and improve their IoT data by transforming raw data into readable or usable data.[235] These technology companies may have a lien arising under state law on the company's customer data (or derived product) for unpaid services and materials. If service providers remain unpaid and all state statutory requirements are satisfied, they may be able to foreclose on the data which could result in consumer data being transferred and disclosed to third parties.[236] In *Chemical Bank v. Communications Data Services, Inc.*, the court concluded that a service provider that was hired by the debtor to compile, update, maintain and transform raw data, enhanced the value of the data for the benefit of the debtor and therefore had an enforceable lien pursuant to the applicable state statute.[237]

Additionally, companies have been sued for allowing service providers and other third parties to have access to consumer data. For instance, in *Yershov v. Gannett Satellite Information Network, Inc.*, a consumer class action, the plaintiff contended that Gannett violated the Video Privacy Protection Act ("VPPA") by collecting and sharing with Adobe, Gannett's data analysis service provider, the location and video viewing data of application users, among other things.[238] The court held that the consumer had "plausibly plead[ed] a case that the VPPA's prohibition on disclosure applie[d]" to the transaction.[239] Whether consumers will ultimately be successful in such cases in the IoT setting is questionable. Consumers in *Yershov* were not re-

---

[234] *E.g.*, IOWA CODE ANN. § 577.1 (West 2017).

[235] *See, e.g.*, Chem. Bank v. Commc'ns Data Servs., Inc., 765 F. Supp. 1401, 1404 (S.D. Iowa 1991).

[236] *E.g.*, IOWA CODE ANN. § 577.2 ("Said lien may be foreclosed in the manner provided in the uniform commercial code . . . .").

[237] *Chem. Bank*, 765 F. Supp. at 1405 (denying secured creditor's motion for a preliminary injunction to prevent the artisan lien holder from foreclosing by sale on the debtor's data that was subject to the secured creditor's security interest on the debtor's general intangibles). *But see In re* S.M. Acquisition Co., 296 B.R. 452, 470 (Bankr. N.D. Ill. 2003). In *In re S.M. Acquisition Co.*, the court reasoned that:

> *Chemical Bank* represented a break with the common law rules governing possessory liens . . . . [because] a common law artisan's lien attaches to specific chattels under a bailment, and cannot be extended into the indefinite future. The court in *Chemical Bank* failed to discuss the common law artisan's lien and thereby violated the rule of construction that requires courts to consider the common law when construing the meaning of a statute.

Id.

[238] 820 F.3d 482, 484 (1st Cir. 2016).

[239] *Id.* at 489.

quired to consent to the disclosure of their data to third parties prior to using the mobile application.[240] As noted, IoT companies are increasingly including provisions in their privacy policies which provide that consumers will be deemed to have consented to third parties accessing their data simply by using an IoT device.[241] Even if IoT companies required consumers to give explicit consent to the disclosure of their data to third parties for monetization or service provider purposes, health-related and biometric data are highly sensitive and potentially personally identifiable. The extent to which such data are disclosed and transferred should not depend primarily on the terms of the company's privacy policy, which are generally provided on a "take-it-or-leave-it" basis.

Lastly, intellectual property law may also be relevant in evaluating rights related to customer databases or lists. IoT companies may assert that they have various intellectual property rights in the consumer data generated from the use of IoT devices and related websites and mobile applications.[242] If the customer database contains "a modest quantum of originality" and is "fixed in any tangible medium of expression" it may receive copyright protection.[243] One scholar suggests that "[m]ost commentators believe that there is no copyright protection for consumer databases."[244] If, however, IoT companies contract with technology providers to transform and manipulate raw data into useable data to obtain insights into business

---

[240] *Id.* at 484 ("[T]he App does not seek or obtain the user's consent to disclose anything about the user to third parties.").

[241] *See supra* note 91 and accompanying text.

[242] Ferguson, *supra* note 196, at 872 ("[I]nformation about my heartbeat recorded in a Fitbit is my personal data, but it is also being shared with the company that sold me the device. It is my heartbeat information, but a company's intellectual property.").

[243] 17 U.S.C. § 102(a) (2012) (stating that "copyright protection subsists . . . in original works of authorship fixed in any tangible medium of expression"); Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 345, 355 (1991) ("The two fundamental criteria of copyright protection [are] originality and fixation in tangible form [and finding that originality means] only that the work was independently created by the author . . . and that it possesses at least some minimal degree of creativity."); 1 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 2.08, Lexis (database updated Nov. 2017) ("[A] very modest quantum of originality will suffice [to support a copyright]."); Nguyen, *Collateralizing*, *supra* note 19, at 579 ("The arrangement of the database is entitled to copyright protection only if the arrangement is original and fixed in a tangible medium."). As to the tangible medium requirement, one scholar suggests the work "must be sufficiently stable to permit it to be perceived, reproduced, or otherwise communicated for 'more than a transitory' period." Lipson, *supra* note 173, at 1075.

[244] Nguyen, *Collateralizing*, *supra* note 19, at 579; *see also* 3-31 ASSET BASED FINANCING: A TRANSACTIONAL GUIDE § 31.06, Lexis (database updated Sept. 2017) ("Computer programs and computer databases are copyrightable. However, there is controversy about the extent of copyrightability of computer programs."); Lipson, *supra* note 173, at 1081–82 ("Databases are generally not subject to copyright, as lacking the 'originality' required by *Feist*."); Paez & Marca, *supra* note 209, at 65 ("[B]ecause data collected by IoT sensors is often compiled automatically through a standard set of selection criteria rather than any human involvement, it could be difficult to establish a valid copyright in many IoT-related data compilations.").

practices or make predictions about consumer preferences, activities or behaviors the compilation of the data could be viewed as original.[245]

Trade secret law may also provide protections for the customer database of IoT companies when the database is kept confidential.[246] Courts have found that "customer databases, customer lists, and detailed information are trade secrets."[247] Intellectual property rights can be assigned under Article 9 and are viewed as general intangibles.[248] Thus, even if a customer database qualifies for trade secret or copyright protection, the intellectual property rights associated with the customer database may be used as collateral for secured financing transactions under Article 9, although in some instances perfection requirements may be governed by federal rules depending on the type of intellectual property at issue.[249] As such, the con-

---

[245] CCC Info. Servs., Inc. v. MacLean Hunter Mkt. Reports, Inc., 44 F.3d 61, 67 (2d Cir. 1994) (finding that the "selection and arrangement of data in [a valuation book] displayed amply sufficient originality to pass the low threshold requirement to earn copyright protection" because it contained more than "pre-existing facts" and instead included predictions "based not only on a multitude of data sources, but also on professional judgment and expertise" unlike the "telephone numbers in *Fiest*"); Paven Malhotra, *How Big Data and IP Intersect: Big Data Is Big Business—But Who Owns It?*, INTELL. PROP. (Fall 2016), http://www.kvn.com/Templates/media/files/Articles/How%20Big%20Data%20and%20IP%20Intersect_Malhotra.pdf [https://perma.cc/M2XH-FZY3] ("[C]opyrights are also available for data compilations . . . . Under the framework of copyright, the compilation of data into a format that reflects the judgment and efforts of a corporation may be copyrightable. Importantly, though, the individual pieces of data that form the compilation are not—a significant shortcoming of copyright law.").

[246] Jane Kaufman Winn & James R. Wrathall, *Who Owns the Customer? The Emerging Law of Commercial Transactions in Electronic Customer Data*, 56 BUS. LAW. 213, 243 (2000) ("The common law trade secret doctrine can provide an alternative source of protection for databases. The doctrine generally protects valuable, confidential business information from misappropriation where the holder takes reasonable measures to maintain its secrecy."); Lipson, *supra* note 173, at 1081 ("A common form of trade secret will be the customer list."); Malhotra, *supra* note 245 ("[M]any states and the federal government define trade secrets as information and compilations of information that are not generally known, that confer a competitive advantage, and that have been the subject of efforts to maintain their confidentiality . . . . Because trade secret laws protect not only the compilation of data but also the underlying data itself, it offers companies a potent tool."); Nguyen, *Collateralizing*, *supra* note 19, at 578 ("Under trade secret law, the consumer database is entitled to trade secret protection if the consumer database is not publicly available information and is kept in secrecy.").

[247] Avery Dennison Corp. v. Kitsonas, 118 F. Supp. 2d 848, 854 (S.D. Ohio 2000) (finding that "customer lists, pricing information, [and] sales strategies" were trade secrets under state law); Nguyen, *Collateralizing*, *supra* note 19, at 578.

[248] *See* U.C.C. § 9-102(a)(42) cmt. 5(d) (AM. LAW INST. & UNIF. LAW COMM'N 2017) ("'General intangible' is the residual category of personal property, including things in action, that is not included in the other defined types of collateral. Examples are various categories of intellectual property . . . .").

[249] RUSCH & SEPINUCK, *supra* note 167, at 251 ("A federal filing is necessary to perfect a security interest in a registered copyright [but federal filings] are not needed to perfect a security interest in patents."); CLARA RUYAN MARTIN & DAVID B. OSHINKSY, INTERNET LAW AND PRACTICE IN CALIFORNIA: 2017 UPDATE § 16.31 (Suzanne L. Weakly ed., Continuing Education of the Bar of California 2017) ("Because there are no federal laws governing trade secrets, the

cerns discussed in this Article regarding the transfer and disclosure of consumer data under Article 9 remain present although a company may have intellectual property rights in consumer data.

C. Bankruptcy Implications

Once the debtor files for bankruptcy, attempts by secured parties to enforce their Article 9 rights as to collateral are normally enjoined.[250] In bankruptcy proceedings, secured creditors are typically in a better position than unsecured creditors.[251] During bankruptcy, a secured party will attempt to prevent avoidance of its security interest. The secured party may file a claim in connection with the bankruptcy proceeding[252] and may be involved in approving the debtor's plan to compensate creditors, depending on the type of bankruptcy sought by the debtor.[253]

UCC requirements for perfection of security interests are not preempted. To perfect a security interest in a trade secret, a lender must file a UCC1 financing statement with the applicable state."); Lipson, *supra* note 173, at 1081 ("Since trade secrets are creatures of state law, security interests in trade secrets should be governed by state law, including state contract and commercial law (i.e., the UCC)."); Nguyen, *Collateralizing*, *supra* note 19, at 579–80. Nguyen states that:

> [i]f a consumer database is entitled to copyright protection and is registered by the Copyright Office, perfection of the database occurs under the federal regime, not article 9. . . . [But,] [i]f a consumer database is not protected under copyright law and not registered by the Copyright Office, the security interest in the consumer database is perfected by filing a financing statement with the Office of the Secretary of State. The same method of perfection is applied if the consumer database is protected under trade secret law.

Id.

[250] 11 U.S.C. § 362 (2012) (discussing automatic stays); CHARLES JORDAN TABB, THE LAW OF BANKRUPTCY 136 (4th ed. 2016) ("[U]pon the filing of a bankruptcy petition an 'automatic stay' is effectuated" and "[a]ll collection efforts on pre-bankruptcy debts are halted immediately and automatically."). *But see* 11 U.S.C. § 362(d) (discussing relief from an automatic stay); TABB, *supra*, at 285 ("[A] creditor may ask the bankruptcy court for earlier relief from the automatic stay upon proof of one of the grounds specified in § 362(d).").

[251] RUSCH & SEPINUCK, *supra* note 167, at 131 ("[T]he bankruptcy process favors secured claims . . . ."); TABB, *supra* note 250, at 724 ("Holders of secured claims are preferred over unsecured creditors in a bankruptcy distribution."); *see* 11 U.S.C. § 363(k) (discussing credit bidding); TABB, *supra* note 250, at 446 ("If property of the estate is being sold, a creditor who has a lien on that property is entitled to 'credit bid' at the sale."); Marshall Tracht, *Can a Secured Creditor Be Denied the Right to Credit Bid When the Creditor's Collateral Is Sold Pursuant to a Chapter 11 Plan of Reorganization?*, ABA PREVIEW U.S. SUP. CT. CASES, Apr. 16, 2012, at 248, 248–49 (discussing secured creditors' right to credit bid).

[252] 11 U.S.C.§§ 501–502; TABB, *supra* note 250, at 726 ("To participate in the bankruptcy case as an 'allowed secured claim,' the holder of the secured claim must have its claim 'allowed' under § 501 and § 502" but "[n]ote, however, that a secured creditor does *not* necessarily forfeit its rights in the collateral if it chooses to forgo filing a proof of claim, instead opting to stand aloof from the bankruptcy case.").

[253] 11 U.S.C.§ 1126; TABB, *supra* note 250, at 1097 (discussing reorganization plans and noting that in such cases "[c]reditors and interest holders are dealt with in a plan by classes" and

Customer databases and lists can be part of the debtor's estate in bankruptcy.[254] After bankruptcy proceedings are initiated, an IoT company in possession of the collateral may be able to continue using its customer database and lists in the "ordinary course of business."[255] In theory, this could mean that disclosures, transfers, and uses of consumer data authorized by the debtor's privacy policy may continue even after the bankruptcy petition is filed, to the extent that such activities are within "the ordinary course of business."[256]

Since the customer database, which may include IoT biometric, health-related, and other types of highly sensitive consumer data, is part of the bankruptcy estate, it may be transferred to third parties.[257] If rights in the database

---

"[a]ll impaired classes will vote on whether to accept the plan[] . . . after receiving a court-approved disclosure statement," but "[c]lasses that are not impaired[] . . . are deemed to accept the plan").

[254] Miller & O'Rourke, *supra* note 36, at 789 ("[B]ankruptcy cases decided under the federal Bankruptcy Code . . . include "customer lists" in the debtor's estate, which is itself comprised of property."); *see also In re* Levitz Ins. Agency, 152 B.R. 693, 697 (Bankr. D. Mass. 1992) (suggesting that customer lists are general intangibles).

[255] 11 U.S.C. § 363(b)–(c) (noting that "notice and a hearing" are needed for uses, sales and leases "outside of the ordinary course of business"); RUSCH & SEPINUCK, *supra* note 167, at 133 ("After a bankruptcy petition is filed, the debtor is entitled to use property subject to a security interest without court approval if such use is in the ordinary course of business . . . ."); TABB, *supra* note 250, at 443–44 ("Section 363 governs the use, sale, or lease of property of the estate by the trustee (or debtor in possession)," and if the use, sale or lease "is *not* in the ordinary course, then the trustee may use, sell, or lease the property only 'after notice and a hearing.'"). To the extent that the activity is within the "ordinary course of business," a notice and hearing is unnecessary with the exception of "'cash collateral,' which the trustee may use, sell, or lease only in accordance with the strict requirements of § 363(c)(2)–(4)." TABB, *supra* note 250, at 444.

[256] *See* TABB, *supra* note 250, at 445 (discussing the tests established by courts to determine whether an activity is within the "ordinary course of business" and concluding that "[d]efining the 'ordinary course of business,' then, appears to turn largely on the question of whether the transaction is one as to which creditors presumably would want prior notice and the opportunity to be heard").

[257] *See* 11 U.S.C. § 363 (2012) ("[u]se, sale, or lease of property"); *id.* § 1123(a)(5)(D) (sale of assets per plan); *id.* § 1123(b)(4) ("sale of all or substantially all of property" pursuant to a plan); *id.* § 1129 ("confirmation of plan"); FELTON E. PARRISH & JAMES E. MORGAN, SALES OF ASSETS UNDER SECTION 363, COLLIER GUIDE TO CHAPTER 11: KEY TOPICS AND SELECTED INDUSTRIES 3-4 (2016) ("[S]ales of assets under section 363 can range from the sale of office furniture by a chapter 7 trustee to a sale of substantially all assets of a chapter 11 debtor."); TABB, *supra* note 250, at 448 ("In cases under chapter 11 . . . the plan proponent has the alternative of providing *in the plan* for the sale of all or part of the property of the estate."); Scott D. Cousins, *Chapter 11 Asset Sales*, 27 DEL. J. CORP. L. 835, 845 (2002) ("Section 1123(b)(4) contemplates confirmation of a liquidating plan, whereby the debtor sells all of the property under a confirmed plan of reorganization."); Morris A. Karam, *The Chrysler Bankruptcy and the Future of 363(b) Transactions*, 11 HOUS. BUS. & TAX L.J. 395, 403 (2011) ("The significance of a 363(b) transaction emerges when comparing it to analogous provisions in § 1123 of the Code. Section 1123 allows for the 'transfer of all or any part of the property of the estate,' the 'sale of all or any part of the property of the estate, either subject to or free from any lien,' and 'provide[s] for the sale of all or substantially all of the property of the estate . . . . But where a § 363(b) transaction only requires a 'notice and a hearing' under the bankruptcy judge, transactions under § 1123 are subject to a

are assigned, it may be sold to a third party without negating the lender's security interest in the database, or alternatively, the sale of the consumer database may extinguish the lender's security interest under certain circumstances.[258]

If a customer database or list is transferred in a bankruptcy proceeding, a consumer's data will be disclosed to the data buyer. A company's database may include both personally identifiable information about consumers and anonymized data, both of which could be transferred to a purchaser. Even if the customer database transferred to a buyer during bankruptcy contains only anonymized aggregated data, recall that various studies indicate that anonymized data can be re-identified.[259] The robustness of anonymization depends in part on the procedures used by the debtor to anonymize the data prior to disclosure and transfer. In theory, as part of the transfer to the data buyer, anonymization methods may also be disclosed to enable re-identification. Consumers may have little control over how they are subsequently treated by data buyers once their data is acquired and used for data analytics and other purposes after bankruptcy. This includes the potential danger of exclusion. Thus, once a data transfer occurs through the bankruptcy process, the harms discussed previously may arise.[260] Today, one need only look to the Sports Authority, RadioShack, and Toysmart bankruptcies to find recent examples of the attempted sale of consumer data in

---

constellation of requirements prior to their approval."); Miller & O'Rourke, *supra* note 36, at 790 ("[A]ny asset that has value constitutes property of the estate. This may account for the courts' custom of treating customer lists as property of the estate; such lists have value that the trustee can realize through a sale and distribute to the estate's creditors."); Yaad Rotem & Omer Dekel, *The Bankruptcy Auction as a Game—Designing an Optimal Auction in Bankruptcy*, 32 REV. LITIG. 330, 331 (2013) ("A Section 363(b) sale is allowed not only for trustees in Chapter 7 liquidations, but also as an out-of-plan maneuver for debtors-in-possession . . . during a Chapter 11 proceeding."); Jack L. Smith & Erin L. Connor, *Sales Free and Clear—Will the Expansion Continue?*, BANKR. STRATEGIST, Jan. 2004, at 1, 1 ("The alternative to Section 363 sales in Chapter 11 is the sale of assets as part of a Chapter 11 plan, as recognized by 11 U.S.C. §§ 1123(a)(5)(D) . . . and 1141(c) . . . .").

[258] 11 U.S.C.§ 363(e) ("[A]t any time, on request of an entity that has an interest in property used, sold, or leased, or proposed to be used, sold, or leased, by the trustee, the court, with or without a hearing, shall prohibit or condition such use, sale, or lease as is necessary to provide adequate protection of such interest."); *id.* § 363(f) (allowing assets to be transferred free and clear as long as at least one of the listed conditions are met); RUSCH & SEPINUCK, *supra* note 167, at 213 ("Often the trustee will sell the collateral subject to the secured party's lien, in which case the secured party will have to deal with the buyer when seeking to enforce its rights. However, the trustee is also authorized to sell the collateral free and clear of liens provided the trustee adequately protects the interest of the secured party."); Arthur J. Spector & Debi Evans Galler, *Section 363 Sale Subject to Lien May Trigger Due-on-Sale Clause*, AM. BANKR. INST. J., May 2013, at 34, 34 (noting that a section 363 sale "is often 'free and clear' of all liens, claims and encumbrances, but on occasion, the sale will be subject to an existing lien").

[259] *See supra* notes 119–123, 197–200 and accompanying text.

[260] *See supra* notes 131–162 and accompanying text.

bankruptcy proceedings.[261] In the IoT setting, the recent bankruptcy and sale of FiLIP illustrates the potential for valuable IoT consumer data to be transferred during bankruptcy.[262]

III. PRIVACY FRAMEWORKS

Various privacy frameworks have been established to protect consumer data and privacy with limited success. These regimes frequently rely excessively on a notice and choice model and the terms of a company's privacy policy to determine the level of protection given to consumers. In some instances, these frameworks may not cover IoT companies or transactions. Overreliance on the notice and choice model and the language in privacy policies, allows a company to be the primary party that decides when and how consumer data will be used, transferred, and disclosed once the mirage of notice and choice is satisfied. Therefore, legal regimes that depend heavily on a notice and choice model are insufficient at protecting the interests of the consumer in the IoT setting.

A. BAPCPA

The Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 ("BAPCPA") made considerable modifications to the Bankruptcy Code.[263] The act was adopted to address, among other things, consumer privacy concerns raised by the Toysmart bankruptcy and other high-profile bankruptcy cases in which consumer data was offered for sale.[264]

The BAPCPA provides that the sale or lease of "personally identifiable" consumer data is restricted if such a transfer would violate the debtor's privacy policy that was previously provided in connection "with offering a product or service."[265] Health-related and biometric data generated from consumer use of IoT devices may qualify as personally identifiable data

---

[261] *See supra* note 35, 40 and accompanying text (Sports Authority); *infra* note 291 and accompanying text (RadioShack); *infra* notes 312–321 and accompanying text (Toysmart).

[262] *See supra* notes 29–31 and accompanying text.

[263] Lynne F. Riley, *BAPCPA at Ten: Enhanced Domestic Creditor Protections and Enforcement Rights*, 90 AM. BANKR. L.J. 267, 267 (2016) (contending that the BAPCPA "generated the most sweeping changes to the Bankruptcy Code in over twenty-five years").

[264] Susan Jensen, *A Legislative History of the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005*, 79 AM. BANKR. L.J. 485, 544 (2005); Nathalie Martin & Ocean Tama y Sweet, *Mind Games: Rethinking BAPCPA's Debtor Education Provisions*, 31 S. ILL. U. L.J. 517, 518–19 (2007) (noting that the BAPCPA was also intended to increase financial education); Lucy L. Thomson, *Personal Data for Sale in Bankruptcy: A Retrospective on the Consumer Privacy Ombudsman*, AM. BANKR. INST. J., June 2015, at 32, 32 (suggesting that fears related to the transfer of child and health data was also the "impetus" for the BAPCPA); *see infra* notes 312–321 and accompanying text.

[265] 11 U.S.C. § 363(b)(1)(B)(ii) (2012).

under the BAPCPA because the data could potentially lead to the identification of a specific consumer and may be associated with other types of identifiable information, such as names and physical and electronic addresses.[266] Furthermore, as noted above, IoT companies frequently provide privacy policies as part of the sale of IoT devices and the provision of related IoT services and mobile applications.[267]

If the debtor's privacy policy in effect at the commencement of a bankruptcy action prohibits "the transfer of personally identifiable data" to unaffiliated parties, the transfer of the data to a third party is permissible only if the "sale or lease is consistent with" the debtor's existing privacy policy or "after the appointment of a consumer privacy ombudsman" and court approval of the transfer (along with compliance with other applicable statutory requirements).[268] The CPO can be heard at a hearing and is authorized to provide information and recommendations to aid the court in determining whether to approve the sale or lease.[269]

In making the determination to approve or deny the transfer of data to a third party, a court must consider whether the transfer would violate nonbankruptcy law.[270] For instance, the court and CPO may consider the implications of the transfer of the customer database under the Federal Trade Commission Act ("FTCA"), the Children's Online Privacy Protection Act ("COPPA"), and "state consumer protection laws."[271]

In some cases, CPOs have played an important role in ensuring that consumer data are protected. For instance, CPOs have recommended that data purchasers use effective security measures to protect consumer data and be in the same business as the debtor to ensure that consumer data are used for the same purposes as originally contemplated by the debtor and the

---

[266] *See id.* § 101(41A) ("The term 'personally identifiable information' means—(A) if provided by an individual to the debtor in connection with obtaining a product or a service from the debtor primarily for personal, family, or household purposes—(i) the first name (or initial) and last name of such individual, whether given at birth or time of adoption, or resulting from a lawful change of name; (ii) the geographical address of a physical place of residence of such individual; (iii) an electronic address (including an e-mail address) of such individual; (iv) a telephone number dedicated to contacting such individual at such physical place of residence; (v) a social security account number issued to such individual; or (vi) the account number of a credit card issued to such individual; or (B) if identified in connection with 1 or more of the items of information specified in subparagraph (A)—(i) a birth date, the number of a certificate of birth or adoption, or a place of birth; or (ii) any other information concerning an identified individual that, if disclosed, will result in contacting or identifying such individual physically or electronically.").

[267] *See supra* notes 77–129 and accompanying text.

[268] 11 U.S.C. § 363(b); *see also* Luis Salazar, *Privacy and Bankruptcy Law: Part II: Specific Code Provisions*, AM. BANKR. INST. J., Jan. 2007, at 58, 59.

[269] 11 U.S.C. § 332.

[270] *Id.* § 363(b)(1)(B)(ii).

[271] Report of the Consumer Privacy Ombudsman at 17, *In re* RadioShack Corp., No. 15-10197 (BLS) (Bankr. D. Del. May 16, 2015) [hereinafter RadioShack CPO Report].

consumer.[272] In the RadioShack bankruptcy, the parties agreed that the debtor would not transfer consumer birth dates, credit card, and debit card numbers.[273] In the 2016 bankruptcy of QSL, the CPO recommended that the company delete sensitive data (such as the ethnicity, sex, and age of their customers and children) prior to the transfer to the purchaser.[274]

There are several areas in which the application of the BAPCPA falls short of protecting consumer data. First, if the IoT data does not constitute personally identifiable information, then CPO protection and other applicable statutory requirements may not be triggered.[275] To the extent that anonymized consumer data can easily be de-anonymized or re-identified, one could contend that such data should qualify as personally identifiable data, particularly if the data clearly fits into one of the enumerated "personally identifiable information" categories.[276] Despite this, IoT companies may be able to successfully contend that anonymized data does not constitute personally identifiable information because the de-identified data are unlikely to lead to the identification of a specific consumer and may not fall into one of the enumerated categories.

Second, if the debtor did not provide consumers with a privacy policy or if the sale of the data is in accordance with the debtor's privacy policy, a CPO is unlikely to be appointed.[277] Recall that IoT privacy policies routine-

---

[272] *Id.* at 5, 19; *see also* Thomson, *supra* note 264, at 33 (noting that courts have required a buyer of personally identifiable data to be in "materially the same line of business as the debtor" and that "the buyer agrees to use the personally identifiable consumer records for the same purpose(s) as they were used previously and agrees to comply with the debtor's privacy policy").

[273] Notice of Agreement Regarding Sale of Certain Personally Identifiable Information at 6, *In re* RadioShack Corp., No. 15-10197 (BLS) (Bankr. D. Del. May 20, 2015); *State AGs Demand Changes to Bankrupt RadioShack's Use of Customer Data*, HOGAN LOVELLS CHRON. DATA PROT. (July 22, 2015), https://www.hldataprotection.com/2015/07/articles/consumer-privacy/state-ags-demand-changes-to-bankrupt-radio-shacks-use-of-customer-data/ [https://perma.cc/J8AJ-G68P] ("RadioShack struck a deal with the Attorneys General, ultimately agreeing to destroy the majority of its customer data . . . . The data to be destroyed included credit and debit card information, Social Security numbers, telephone numbers, and dates of birth.").

[274] Consumer Privacy Ombudsman Report to the Court at 2–3, 9, *In re* QSL of Medina, Inc., No. 15-52727 (Bankr. N.D. Ohio Mar. 21, 2016).

[275] *In re* Graceway Pharm., LLC, No. 11-13036 (PJW), 2011 WL 6296791, at *4 (Bankr. D. Del. Sept. 30, 2011) (finding that "[t]he Debtors have, to the extent necessary, satisfied the requirements of Bankruptcy Code section 363(b)(1) because no personally identifiable information will be transferred," and "[a]ccordingly, appointment of a consumer privacy ombudsman pursuant to Bankruptcy Code sections 363(b)(1) or 332 is not required with respect to the relief requested in the Motion").

[276] *See supra* note 266 and accompanying text.

[277] *See, e.g.*, *In re* Korea Tech. Indus. Am., Inc., No. 11-32259, 2011 Bankr. LEXIS 5220, at *19 (Bankr. D. Utah Nov. 15, 2011) ("[T]he Sale of the Purchased Assets is consistent with the Debtors' policy concerning the transfer of personally identifiable information and no consumer privacy ombudsman is necessary as set forth in section 363(b)(1) of the Bankruptcy Code."); *In re* TriDimension Energy, L.P., No. 10-33565-SGJ, 2010 Bankr. LEXIS 4838, at *18–19 (Bankr. N.D. Tex. Nov. 19, 2010) (finding that because the "[d]ebtors ha[d] never disclosed a policy to an

ly authorize companies to transfer consumer data in the event of a bankruptcy.[278] Thus, if an IoT company files for bankruptcy, and consumer biometric and other highly sensitive data are part of the company's database, and the sale is permissible under the privacy policy in effect at the time of the commencement of the bankruptcy action (for instance if the privacy policy permits the transfer of personally identifiable data to unaffiliated entities), the data may be sold without CPO input.

The language in the debtor's privacy policy controls the level of scrutiny that will be given to the sale of consumer data in bankruptcy proceedings. For example, in *In re Boscov's Inc.*, the court declined to appoint a CPO, and it appears that no restrictions were placed on the sale of the consumer data.[279] The debtor's privacy policy notified customers that their personal information could be transferred to third parties in connection with a business transition.[280]

In contrast, recall that prior to the Pay by Touch bankruptcy, in which the biometric data of consumers were at risk of being sold, the company's privacy policy provided that personally identifiable information would not be transferred or shared with unaffiliated parties without consumer consent.[281] A CPO was appointed to provide guidance to the court on the sale of consumer data, including biometric information.[282] If Pay by Touch's privacy policy had explicitly permitted the sale of biometric information without consumer consent, it is certainly possible that a CPO would not have been appointed.

---

individual prohibiting the transfer of personally identifiable information [to unaffiliated parties] . . . . there is no requirement that the sale of the Properties . . . be consistent with any privacy policy or that a consumer privacy ombudsman be appointed in connection with same under Bankruptcy Code § 363(b)(1)").

[278] *See supra* note 80–90 and accompanying text.

[279] Order Granting Motion of Debtors for an Order (A) Approving Bidding Procedures for the Sale of Substantially [sic] of Their Assets, (B) Approving the Form and Manner of Notice Thereof, (C) Scheduling an Auction and Sale Hearing and (D) Approving Breakup Fee at 7, *In re* Boscov's Inc., No. 08-11637 (Bankr. D. Del. Oct. 1, 2008) [hereinafter Boscov Order] ("The Sale of the Assets is consistent with section 363(b)(1)(A) of the Bankruptcy Code and the Debtor's privacy policy, and no consumer privacy ombudsman is necessary in connection with the Sale."); S. Jason Teele et al., *The Impact of Privacy on FDIC Resolution Plans*, LAW360 (Nov. 17, 2011, 1:00 PM), https://www.law360.com/articles/286179/print?section=banking [https://perma.cc/JB3B-N9KA] (Boscov's privacy policy stated that "in the event that some or all of the business assets of Boscov's are sold or transferred, Boscov's may transfer the corresponding information about our customers. In light of the language . . . in Boscov's privacy notice, the bankruptcy court approved the sale without appointing a consumer privacy ombudsman or imposing other restrictions on the personal information") (original brackets and internal quotation marks omitted).

[280] Boscov Order, *supra* note 279, at 3–8; Teele, *supra* note 279.

[281] Pay by Touch CPO Report, *supra* note 28, at 3–4.

[282] *Id.* at 1.

In connection with the FiLIP bankruptcy, the company's privacy policy included the standard carve-out authorizing data transfers upon the sale of the company.[283] As part of the court-approved asset purchase agreement, consumers' names, addresses, "relations/friends as configured in [the] system," device data, "network data, SIM card information [and] message data" were transferred to the purchaser.[284] Additionally, prior to its bankruptcy, FiLIP's privacy policy indicated that the company also collected the birthdates, "other personal information of customers as well as that of the child who" used the device, and the physical location of the device.[285] These data were likely also transferred to the purchaser. A CPO does not appear to have been appointed, as the court determined that the sale of the assets to the purchaser was "consistent with the [d]ebtor's privacy policy."[286]

As independent third parties with bankruptcy and privacy expertise, CPOs can play an instrumental role in helping courts to evaluate the costs and benefits of a transfer of consumer data to unaffiliated parties.[287] For instance, in the first reported case involving the appointment of a CPO, the CPO generated a fifty-one-page "report that both reviewed applicable privacy law and analyzed the debtor's privacy policy provisions and the impact of the proposed sale."[288] CPOs have also worked with state attorneys general, and requested and obtained official responses from the Federal Trade Commission ("FTC") regarding their concerns about the sale of consumer data, and appear to have taken these concerns into consideration when making recommendations.[289]

When there are potential ambiguities in the privacy policy language regarding the transfer or disclosure of consumer data, one could easily ar-

---

[283] FiLIP Privacy Policy, *supra* note 82.

[284] FiLIP Sale Exhibit A, *supra note* 31, at 41.

[285] FiLIP Privacy Policy, *supra* note 82.

[286] FiLIP Sale Order, *supra* note 31, at 5.

[287] *See* 11 U.S.C. § 332(b) (2012) (noting that the information CPOs provide to the court can include the "presentation of (1) the debtor's privacy policy, (2) the potential losses or gains of privacy to consumers if such sale or such lease is approved by the court, (3) the potential costs or benefits to consumers if such sale or such lease is approved by the court and (4) the potential alternatives that would mitigate potential privacy losses or potential costs to consumers").

[288] Salazar, *supra* note 268, at 59.

[289] *See* RadioShack CPO Report, *supra* note 271, at 6 ("In formulating the recommendations contained in this Report, the Ombudsman has worked extensively with . . . the FTC, and the Office of the Texas Attorney General, acting on behalf of various state Attorneys General."); Letter from David C. Vladeck, Dir., Bureau of Consumer Prot., Fed. Trade Comm'n, to Michael St. Patrick Baxter and Yaron Dori, Esqs., Covington & Burling LLP (Sept. 14, 2011) [hereinafter FTC Borders Letter] (on file with the FTC) ("This letter responds to your request, in your role as Consumer Privacy Ombudsman ('CPO'), that we provide a written description of our concerns regarding the possible sale as part of a bankruptcy proceeding of certain consumer personal information currently in the possession of Borders Group, Inc. ('Borders').").

gue that the transfer of the data violates the privacy policy and therefore a CPO is required. For example, at the commencement of Borders' bankruptcy, the company's privacy policy provided in part that "circumstances may arise where for strategic or other business reasons, Borders decides to sell, buy, merge or otherwise reorganize its own or other businesses."[290] The FTC contended that a sale of the company's data would violate the privacy policy and that the provisions of the policy authorized the company to "continue to operate as a going concern, but did not authorize a dissolution of the company with piecemeal sales of company assets during bankruptcy."[291] Similarly, in the 2017 bankruptcy case of Gander Mountain Company, the parties disagreed about "the extent of the protections afforded to the Debtors' customers by the privacy policy."[292] The language in the privacy policy was ambiguous, and the CPO determined that the privacy policy was intended to protect users' data given the "[d]ebtors' commitment to affording 'choice' to customers with respect to the use and sharing of their personal information."[293] Companies may draft IoT privacy policies to avoid the ambiguities found in the Gander and Borders privacy policies.[294]

Recall that CPO protection and related statutory requirements are only triggered when the debtor provides a policy to an individual that can be interpreted as prohibiting the transfer of personally identifiable information and that privacy policy is in effect at the time the bankruptcy proceeding commences. Except for possible FTC scrutiny, nothing prevents a company from revising its privacy policy to authorize the sale of customer data and obtaining consumer consent to the same immediately before bankruptcy or when it begins experiencing financial hardships. If a company clearly informs consumers of changes to its privacy policy (such as taking additional steps to notify consumers rather than simply posting a revised policy on a

---

[290] FTC Borders Letter, *supra* note 289.

[291] *Id.*

[292] Gander CPO Report, *supra* note 82, at 7.

[293] *Id.*

[294] *See, e.g.*, *Amazon Privacy Policy*, *supra* note 88 ("Business Transfers: . . . we might sell or buy stores, subsidiaries, or business units. In such transactions, customer information generally is one of the transferred business assets but remains subject to the promises made in any pre-existing Privacy Notice (unless, of course, the customer consents otherwise). Also, in the unlikely event that Amazon.com, Inc., or substantially all of its assets are acquired, customer information will of course be one of the transferred assets."); *Fitbit Privacy Policy*, *supra* note 109 ("If we are involved in a merger, acquisition, or sale of assets, we will continue to take measures to protect the confidentiality of personal information and give affected users notice before transferring any personal information to a new entity."); *Nest Product Privacy Policy*, *supra* note 85 ("Upon the sale or transfer of the company and/or all or part of its assets, your personal information may be among the items sold or transferred. We will request a purchaser to treat our data under the privacy statement in place at the time of its collection.").

website), and obtains consumer consent, the changes to the privacy policy may be valid.[295]

Third, between 2005 and 2015, bankruptcy courts considered the appointment of CPOs in "approximately 400 federal bankruptcy cases," but of these cases only one hundred CPO appointments were made.[296] Even if the potential transfer of consumer data conflicts with the terms of a debtor's privacy policy, some courts have been unwilling to appoint a CPO.[297] These courts have reasoned that if the data buyer agrees to be the "debtor's successor-in-interest" as to the customer data, and consents to using the customer data pursuant to the debtor's existing privacy policy, a CPO is unnecessary.[298] In the FiLIP bankruptcy the court noted that the ultimate purchaser had agreed to adopt the debtor's privacy policy.[299] This rationale places too much reliance on the debtor's existing privacy policy at the time the bankruptcy commences. In focusing on whether the purchaser agrees to comply with the debtor's privacy policy, courts may not sufficiently consider whether the transfer is potentially restricted under non-bankruptcy law.[300] Of course, the analysis of applicable non-bankruptcy law in CPO reports typically involves statutes, such as the FTCA, COPPA, and state consumer protection acts.[301] As will be discussed below, because the FTC's interpretation of the FTCA to some extent relies on the provisions of the debtor's privacy policy, and some state consumer protection statutes may contain language similar to the FTCA, there may be some limitations on the effectiveness of non-bankruptcy law in adequately protecting consumers.[302] Addi-

---

[295] *See In re* Gateway Learning Corp., 138 F.T.C. 443, 450 (2004) (stating that the company "did not notify consumers of material changes to its information practices," but only "posted a revised privacy policy on its Web site without any indication that the policy had materially changed or what aspects of the policy had changed," making "the representation[s] [in the policy] . . . false or misleading").

[296] Thomson, *supra* note 264, at 32.

[297] *Id.* at 33.

[298] *In re* Escada (USA) Inc., No. 09-15008 (SMB), 2010 Bankr. LEXIS 4362, at *11 (Bankr. S.D.N.Y. Jan. 7, 2010); *In re* Reader's Digest Ass'n, No. 09-23529 (RDD), 2010 Bankr. LEXIS 5682, at *17, (Bankr. S.D.N.Y. Jan. 14, 2010) (reasoning that the buyer "agreed to adopt" the debtor's privacy policy and to "provide notice" to specified individuals and therefore a CPO was not needed).

[299] FiLIP Sale Order, *supra* note 31, at 5.

[300] Thomson, *supra* note 264, at 33.

[301] RadioShack CPO Report, *supra* note 271, at 17.

[302] Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation*, 69 FORDHAM L. REV. 1305, 1351–52, 1354 (2001) (describing state consumer protection statutes as "little FTC acts" and contending that "states bas[ing] their interpretations on the FTC Act plays out in a number of ways," but acknowledging that there is variation in the language of each state statute); *see infra* notes 312–333 and accompanying text. Commentators have suggested, however, that state consumer protection statutes may give more protection to consumers in certain instances, particularly because some statutes permit a private cause of action. Spencer Weber Waller et al., Con-

tionally, by declining to appoint a CPO, courts may fail to effectively evaluate the "implementation of an acceptable consent process and data-disposition plan."[303]

Fourth, the appointment of a CPO does not always mean that consumer data will be sufficiently protected. CPOs may recommend that the buyer of consumer data comply with the debtor's existing privacy policy as a condition of the sale.[304] This may be why the courts discussed above fail to appoint CPOs when the purchaser agrees to be bound by prior privacy policies. This recommendation appears to originate from the FTC's proposed Toysmart settlement agreement discussed below in Part II.B.[305] However, this recommendation fails to address potential deficiencies in the underlying privacy policy that may allow the disclosure of the consumer data for monetization or assignment purposes. CPOs recommend, and courts typically require, that the purchaser of the debtor's database obtain consumer consent to change the terms of the debtor's existing privacy policy.[306] Amendments to the existing debtor privacy policy by the buyer of the debtor's assets may be beneficial to consumers when the buyer imposes consumer-friendly restrictions on the monetization or assignment of the data. However, unless the court orders otherwise, nothing prevents the buyer of the debtor's consumer data from amending the privacy policy after conclusion of the bankruptcy to either claw back provisions restricting the disclosure of consumer data to third parties or include additional provisions that permit disclosure of data. If "affirmative consumer consent" to privacy policy amendments are obtained, these changes are likely permissible even if they are detrimental to consumer interests.[307] Given studies that suggest that consumers do not read or understand contract terms and that companies exert significant influence on consumers' perceptions of acceptable data practices, relying solely on consumer consent to justify amendments to privacy policies may not sufficiently protect consumers.

Additionally, rather than requiring consumers to affirmatively opt-in to having their data transferred to a buyer, in some instances CPOs have suggested, and courts have permitted, consumer data to be transferred to a buy-

---

sumer Protection in the United States: An Overview 20 (Jan. 12, 2011) (unpublished manuscript) (on file with author).

[303] Thomson, *supra* note 264, at 33.

[304] RadioShack CPO Report, *supra* note 271, at 3–5.

[305] *See infra* notes 312–321 and accompanying text.

[306] RadioShack CPO Report, *supra* note 271, at 5 (recommending that the successful bidder obtain consumer consent for material amendments to the privacy policy); Thomson, *supra* note 264, at 33.

[307] RadioShack CPO Report, *supra* note 271, at 223.

er unless consumers opt-out.[308] Consumers may also have only a short window of time to opt-out of having their data transferred to the buyer of the debtor's assets after receiving any required notice.[309] Adopting an "opt-out" approach to the buyer's subsequent amendments to the debtor's privacy policy also presents similar problems for consumers.[310]

Lastly, the most important limitation of the BAPCPA is that it only applies when the debtor is in bankruptcy (in limited settings).[311] Thus, the additional safeguards that may be available under the BAPCPA, such as the appointment of a CPO, are not applicable when a secured party attempts to exercise its rights under Article 9 to foreclose on a customer database outside of the bankruptcy context.

B. The FTCA & FTC Intervention

The FTC has taken an active role in bankruptcy proceedings involving consumer data. In connection with the Toysmart bankruptcy, the FTC contended that the company's proposed sale of consumer data was inconsistent with its privacy policy and therefore violated the FTCA.[312] The FTC's proposed settlement with Toysmart authorized the transfer of consumer data under certain conditions, including the requirement that the data buyer be "an entity that is in a related market."[313] Thus, in connection with the

---

[308] *Id.* at 6 (CPOs "have recommended, and Bankruptcy Courts have approved, the sale of [personally identifiable information ("PII")] in contravention of a debtor's existing privacy policy; provided that: . . . (iii) consumers are afforded notice of the proposed sale and given an opportunity to opt-out of the proposed transfer of PII"); Joshua A.T. Fairfield, *The End of the (Virtual) World*, 112 W. VA. L. REV. 53, 90–91 (2009) (contending that "[i]n practice, the recommendations of the ombudsman tend toward three primary suggestions—that the sale be to a 'qualified buyer' who is in the industry of the debtor; that the buyer will serve as successor-in-interest to the debtor's security and privacy policies; and that the customers be provided an opportunity to opt in or (more commonly) opt out of the proposed transfer").

[309] RadioShack CPO Report, *supra* note 271, at 3–4 ("The Successful Bidder agrees to notify customers of the Sale by: . . . [e]mailing, within sixty (60) days of the Closing, the subset of customers whose email addresses are being acquired by the Successful Bidder. Such email should clearly and conspicuously advise such customers that: . . . their email addresses will be transferred to the Successful Bidder unless an opt-out request is received within seven (7) days . . . .").

[310] *See* Thomson, *supra* note 264, at 33 (noting that CPOs and courts have recommended that data buyers provide consumers with opt-out notice prior to implementing changes to the debtor's privacy policy).

[311] Richard Levin & Alesia Ranney-Marinelli, *The Creeping Repeal of Chapter 11: The Significant Business Provisions of the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005*, 79 AM. BANKR. L.J. 603, 627 (2005) (noting that Bankruptcy Code "§ 332 requires appointment of a consumer privacy ombudsman only in the context of sales or leases under § 363(b)(1)").

[312] Complaint for Permanent Injunction and Other Equitable Relief at 2–3, FTC v. Toysmart.com, LLC, No. 00CV11341RGS (D. Mass. July 7, 2000), 2000 WL 34575569 [hereinafter *Toysmart Complaint*].

[313] Press Release, Fed. Trade Comm'n, FTC Announces Settlement with Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations, (Jul. 21, 2001), https://www.ftc.gov/

Toysmart bankruptcy, the FTC set forth specific limitations for buyers of consumer data in the bankruptcy setting. The FTC reaffirmed these conditions in the RadioShack bankruptcy.[314] As mentioned earlier, these conditions have been used by CPOs and bankruptcy courts in subsequent proceedings involving the transfer of consumer data.[315] However, in many instances, some companies have attempted to carve out the application of some of these conditions by specifically providing in their privacy policies that a consumer's data may be sold to a third party that is not "in the same line of business" as the company in a piecemeal manner.[316]

The FTCA proscribes "unfair or deceptive acts or practices in or affecting commerce."[317] The FTC has highlighted three elements that are central to deception cases.[318] Amongst these elements is the requirement that

---

news-events/press-releases/2000/07/ftc-announces-settlement-bankrupt-website-toysmartcom- regarding [https://perma.cc/4U6J-D6CG]; Citron, *supra* note 39, at 783 (discussing state attorneys general objections to the proposed settlement agreement and contending that "[t]he settlement was never approved, and consumers' data was destroyed"); Miller & O'Rourke, *supra* note 36, at 794 (discussing the proposed Toysmart settlement and contending that ultimately "Toysmart withdrew the database from the sale . . . . [and] Disney later agreed to buy and destroy the list, ending the case.").

[314] FTC Press Release, *supra* note 313; *see* Letter from Jessica L. Rich, Dir., Bureau Consumer Prot., Fed. Trade Comm'n, to Elise Frejka, Consumer Privacy Ombudsman for *In re* RadioShack Corporation, No. 15-10197 (BLS) (Bankr. D. Del. May 16, 2015) https://www.ftc.gov/system/files/documents/public_statements/643291/150518radioshackletter.pdf [https://perma.cc/CA34-DL7D]) ("*Toysmart* is instructive on this point. There, the Commission entered into a settlement with the company allowing the transfer of customer information under certain limited circumstances: 1) the buyer had to agree not to sell customer information as a standalone asset, but instead to sell it as part of a larger group of assets, including trademarks and online content; 2) the buyer had to be an entity that concentrated its business in the family commerce market, involving the areas of education, toys, learning, home and/or instruction (*i.e.*, the same line of business that Toysmart had been in); 3) the buyer had to agree to treat the personal information in accordance with the terms of Toysmart's privacy policy; and 4) the buyer had to agree to seek affirmative consent before making any changes to the policy that affected information gathered under the Toysmart policy.").

[315] *See, e.g.*, Gander CPO Report, *supra* note 82; RadioShack CPO Report, *supra* note 271.

[316] *Privacy Policy*, A.O. SMITH CORP., https://www.aosmith.com/Privacy-Policy/ [https://perma.cc/PSX2-DTUN] ("If we or any part of our group is sold, or some of its assets transferred to a third party, your personal information, as an asset, may also be transferred to the acquirer, even if they are not in the same line of business as us. Our customer database could be sold separately from the rest of the business, in whole or in a number of parts . . . . However, use of your personal information will remain subject to this Privacy Policy. Similarly, your personal information may be passed on to a successor in interest in the unlikely event of a liquidation, bankruptcy or administration."); *Privacy*, MARRIOTT VACATION CLUB, https://www.marriottvacationclubme.com/en/privacy.shtml [https://perma.cc/88VN-MQXG] ("[Y]our personal information may be passed on to a successor in interest in the event of a reorganization, reconstruction, liquidation, bankruptcy or administration. It may be that any buyer or successor buys all or only part of our business. It may also be the case that they are not in the same line of business as us.").

[317] 15 U.S.C. § 45(a)(1) (2012).

[318] Letter from James C. Miller, III, Chairman, Fed. Trade Comm'n, to Honorable John D. Dingell, Chairman, Comm. Energy & Commerce (Oct. 14, 1983),

"there must be a representation, omission or practice that is likely to mislead the consumer."[319] Scholars have observed that "[m]uch of the FTC's privacy jurisprudence is based upon a deception theory of broken promises."[320] With respect to privacy policies, a company's failure to provide consumers with sufficient notice of its data collection practices, as well as the company's failure to live up to privacy related promises, may be deemed to be deceptive, as illustrated by the allegations in the FTC's complaint against Toysmart.[321]

The FTC's approach to its deception authority evidences its approval of the notice and choice principle. The FTC has also supported the use of the notice and choice principle in the IoT setting.[322] The agency has played an instrumental role in safeguarding consumer privacy and it is important to acknowledge that the FTC is not limited to exercising only its deception authority. However, to the extent that the agency's deception enforcement actions rely on the sufficiency of notice to consumers of the terms of a company's privacy policy, as well as representations made in privacy policies, FTC action in this area suffers from the same problems seen in BAPCPA determinations.[323] It may be difficult to provide notice of a company's terms and conditions and privacy policy to consumers in the IoT setting because many

---

http://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf [https://perma.cc/9VD6-8R9Z] (Those three elements are: (1) "a representation, omission or practice that is likely to mislead the consumer," (2) "a consumer acting reasonably in the circumstances," and (3) "the representation, omission, or practice must be a 'material' one.").

[319] *Id.*

[320] Solove & Hartzog, *supra* note 93, at 628. Commentators have also noted that "[t]he FTC has developed a theory of deception that not only includes broken promises of privacy and security, but also a general theory of deception in obtaining personal information and deception due to insufficient notice of privacy-invasive activities." *Id.*; *see also* Maureen K. Ohlhausen, Acting Chair, Fed. Trade Comm'n, Remarks at Fed. Commc'ns Bar Ass'n Luncheon: Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases (Sept. 19, 2017) (on file with the FTC) ("We bring many of our privacy and data security cases under our deception authority . . . . In such cases, the complaint alleges that a company misled consumers through material claims about a product or services's [sic] privacy or security features.").

[321] *Toysmart Complaint*, *supra* note 312, at 2–3 ("[D]efendant Toysmart . . . represented that it would 'never' disclose, sell, or offer for sale customers' or registered members' personal information to third parties . . . . [but the company] has disclosed, sold, or offered for sale its customer lists and profiles . . . . [and] [t]herefore, the representation . . . was, and is, a deceptive practice."); *see* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2235 (2015) ("When companies . . . failed to live up to [promises voluntarily made in their privacy policies], the FTC claimed that this was a deceptive trade practice.").

[322] FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (2015) [hereinafter FTC IOT REPORT], https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/2YVR-ZVJJ] (the "staff believes that providing notice and choice remains important" in the IoT setting).

[323] *See supra* notes 275–311 and accompanying text.

IoT devices lack an interface. Further, relying on the adequacy of the notice provided, the promises made by companies in their privacy policies, and consumer consent to validate data collection practices and determine the level of protection that should be given to consumer information is problematic for several reasons (some of which have been previously noted).

Privacy scholars have frequently critiqued the effectiveness of the notice and choice model.[324] Notice and choice presumes that consumers will seek out the terms of privacy policies, pay attention to companies' notices, read and understand privacy policies, and consistently make rational choices about the costs and benefits of disclosing their data. The results of one study on consumers and privacy policies, indicate that consumers "perceive[] the privacy notice as offering greater protections than the actual privacy notice."[325]

Scholars suggest that the FTC has indicated that it will attempt to focus more on consumer expectations and the nature of consumers' entire dealings with a company rather than primarily on the language contained in a company's privacy policy or promises made by the company to consumers.[326] However, a focus on the expectations of the reasonable consumer may be insufficient as the privacy and security expectations of the average consumer may be low even if consumers are unhappy about the collection, transfer, and disclosure of their data.[327] Companies' use of social "shaming and blaming" techniques may engender low consumer privacy expecta-

---

[324] *See, e.g.*, Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF 'INFORMATION ECONOMY' 341, 341 (Jane K. Winn ed., 2006) (contending that the Fair Information Practice Principles "have increasingly been reduced to narrow, legalistic principles (e.g., notice, choice, access, security, and enforcement)" that have "proven unsuccessful in practice"); Kirsten Martin, *Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online*, 34 J. PUB. POL'Y & MARKETING 210, 211 (2015) [hereinafter Martin, *Tabula Rasa*] (critiquing the effectiveness of the privacy notice and choice model and calling on "public policy makers and firms" to "avoid unnecessary and unintentional privacy violations caused by an over-reliance on privacy notices."); Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 544, 564 (2008) (critiquing the effectiveness of the notice and choice model and discussing lack of consumer understanding of privacy policies); Helen Nissenbaum, *A Contextual Approach to Privacy Online*, DÆDALUS, Fall 2011, at 32, 34–35 ("[T]here is considerable agreement that transparency-and-choice has failed . . . . I am not convinced that notice-and-consent, however refined, will result in better privacy online as long as it remains a procedural mechanism divorced from the particularities of relevant online activity.").

[325] Martin, *Tabula Rasa*, *supra* note 324, at 210.

[326] Solove & Hartzog, *supra* note 93, at 667–72.

[327] CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 123 (2016) (noting that in deception cases "the interpretation of that act or practice is considered from the perspective of a reasonable consumer"); Elvy, *supra* note 92, at 1434.

tions.[328] Indeed, the increasing frequency with which IoT devices are designed to collect and use biometric and health-related data in the IoT setting may also negatively influence the privacy expectations of some consumers with respect to these types of data. Scholars have noted that the FTC "has not followed the empirical evidence [regarding consumers' failure to read or understand privacy policies and 'how consumers form their expectations'] to the fullest extent."[329] Furthermore, if a company's privacy policy provides that biometric and health-related data can be sold or disclosed to third parties, it may be difficult to contend that a reasonable consumer has a "preexisting expectation" that the data that they provide to a company will not be provided to third parties. If a company has such a policy in place, and its privacy design and settings are not misleading, there is a strong argument that the sale of consumer data to third parties is in accordance with consumers' expectations about how their information will be collected and used.

Additionally, the acting chair of the FTC has noted that although "substantial injury isn't a prong of the deception legal analysis, which focuses instead on materiality . . . regardless of the legal authority being used, the [FTC], as a matter of good governance, should always consider consumer injury in determining what cases to pursue."[330] Narrow definitions of consumer injury that focus on traditional injuries, such as financial, health or safety harms, may not sufficiently account for intangible harms suffered by consumers as a result of "privacy and data security missteps."[331]

Even if a company has implemented effective security measures to prevent cybersecurity threats, the collection and subsequent assignment and potential disclosure to third parties via a sale or license of consumer IoT data may be a significant privacy intrusion, particularly when health-related and biometric data are involved. There is no meaningful choice provided to consumers regarding the collection of their data because privacy policies are provided on a "take it or leave it" basis via disclosures on a company's

---

[328] Kim & Telman, *supra* note 94, at 736 ("Internet-based companies also use shaming and blaming to shape public opinion and normalize dubious practices.").

[329] Solove & Hartzog, *supra* note 93, at 667–68 (contending that the FTC's deception authority should evolve to evaluate "the effect of particular practices on consumers with flawed assumptions and cognitive biases").

[330] Ohlhausen, *supra* note 320.

[331] Allison Grande, *Biz Groups Push FTC to Avoid 'Theoretical' Privacy Harms*, LAW360 (Nov. 1, 2017, 9:06 PM), https://www.law360.com/articles/980724/biz-groups-push-ftc-to-avoid-theoretical-privacy-harms [https://perma.cc/74AE-LU2P] (contending that the Acting Chair of the FTC has "repeatedly stress[ed] in recent remarks that her focus would be on concrete financial injury, health and safety injury, and broken privacy and data security promises"). *But see* Ohlhausen, *supra* note 320 (suggesting that other types of consumer injuries may be relevant under the FTC's authority, including "unwarranted intrusion injury" and "reputational injury").

website.[332] Over-reliance on consumer consent and notice of privacy practices, as well as on the express and implied promises in a company's privacy policy (or omissions made by the company) constrains efforts to protect consumer privacy.

Given the expected value and importance of IoT data, it is always in a company's best interest to include language in its privacy policy and other materials that authorize the transfer of customer data. One could contend that companies may be reticent to do so because they may fear alarming consumers. However, as discussed in Part I.B, companies continue to include such provisions in their privacy policies. In fact, some companies, such as Amazon, revised their privacy policies in the wake of the Toysmart bankruptcy to ensure that they could sell consumer data.[333] Companies are using the excessive reliance on notice, consumer consent, and express or implied promises made by a company in its privacy policy or other materials, to their advantage.

C. Biometric Data Statutes

While the general data breach and privacy law statutes of some states may apply to biometric data, Illinois, Texas, and Washington have adopted statutes that broadly, exclusively, and clearly address companies' collection and use of biometric data.[334] Efforts to adopt similar legislation in other states and to expand existing statutes in favor of consumers have been sig-

---

[332] *See supra* notes 77–129 and accompanying text.

[333] Daniel Solove, *Going Bankrupt with Your Personal Data*, TEACHPRIVACY: PRIVACY & SEC. BLOG (July 6, 2015), https://www.teachprivacy.com/going-bankrupt-with-your-personal-data [https://perma.cc/38N8-UECQ] ("The Toysmart case led Amazon.com to change its privacy policy" and include explicit language allowing for the sale of "customer information.").

[334] 740 ILL. COMP. STAT. ANN. 14/15 (West 2018); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017); WASH. REV. CODE ANN. § 19.375.010 (West 2017); Roberg-Perez, *supra* note 12, at 61–64 (discussing proposed biometric data legislation in Alaska, Montana, Connecticut and New Hampshire and adopted legislation in Wisconsin and Massachusetts that require notification of data breaches). Wisconsin's "unauthorized acquisition of personal information" statute includes biometric data in the definition of personal information. WIS. STAT. ANN. § 134.98 (West 2017). Other state statutes may also regulate limited aspects of biometric data collection in certain instances. For instance, a California statute addresses "recordings of spoken word collected through the operation of a voice recognition feature by the manufacturer of a connected television for the purpose of improving the voice recognition feature." CAL. BUS. & PROF. CODE § 22948.20(B) (West 2017) (restricting the use of voice recordings collected from a "connected television" for advertisement purposes). Roberg-Perez contends that in addition to state statutes, federal laws, such as the "Genetic Information Nondiscrimination Act (GINA) [which] prohibits discrimination in insurance and employment based on genetic information," and the "Federal Privacy Act [which] restricts access to—and disclosure of—any individual biometric data that is contained within federal records," could also regulate the collection and use of biometric data "depending on the nature of the biometric data, and the context in which the data is collected, used and stored . . . ." Roberg-Perez, *supra* note 12, at 63.

nificantly curtailed by companies' lobbying efforts.[335] Washington's 2017 biometric data statute was enacted only after being significantly weakened.[336] Companies may be subject to fewer restrictions regarding the collection, sale and use of biometric data in states that do not have legislation unambiguously addressing this issue.

The Texas statute proscribes the collection of biometric identifiers for "commercial purpose[s]" unless a consumer is provided with prior notice and consents to the capture of biometric information.[337] Monetizations (such as sales and leases) and disclosures of biometric identifiers are permissible in limited circumstances.[338] These instances include if the consumer consents to the disclosure "for identification purposes in the event of . . . disappearance or death," the biometric identifiers are disclosed in connection with a financial transaction requested or approved by the consumer, or if the disclosure is "required or permitted" by state or federal statutes or made to law enforcement agencies pursuant to a warrant.[339] The statute also obligates companies to exercise reasonable care in connection with their use of biometric data and generally requires the destruction of the data within one year of collection.[340]

The Washington statute requires companies to either provide notice and obtain consent, or implement mechanisms to prohibit later commercial uses prior to collecting and storing a "biometric identifier in a database for a commercial purpose."[341] Notably, the Washington statute specifically excludes from the definition of biometric identifiers "physical or digital photograph[s], video[s] or audio recording[s] or data generated therefrom."[342] The Washington statute adopts a "business-friendly" position by excluding digital photographs and audio recordings that can be transformed into biometric identifi-

---

[335] FACEBOOK BIOMETRIC DATA, *supra* note 137, at 7–8 (discussing Facebook's, Google's and Verizon's successful "hidden lobbying" efforts to block the adoption and expansion of biometric data statutes in various states).

[336] *Id.* (noting the limitations of the Washington statute).

[337] TEX. BUS. & COM. CODE ANN. § 503.001(b). Biometric identifiers are defined as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry." *Id.* § 503.001(a).

[338] *Id.* § 503.001(c).

[339] *Id.* § 503.001(c)(1).

[340] *Id.* § 503.001(c)(2)–(3).

[341] WASH. REV. CODE ANN. § 19.375.010 (West 2017) (defining commercial purpose "[as] a purpose in furtherance of the sale or disclosure to a third party of a biometric identifier for the purpose of marketing of goods or services when such goods or services are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier," but not including "a security or law enforcement purpose"). The granting of a security interest in a customer database containing biometric data, may not qualify as a commercial purpose and to the extent that the statute's requirements are limited to "commercial purposes," they may not be applicable to secured transactions. *See id.*

[342] *Id.*

ers, such as face and voice prints, that could be used to identify consumers.[343] In contrast, under the Illinois statute (discussed below), consumers have sued several companies including Google, Shutterfly, and Facebook for collecting biometric data gleaned from digital pictures.[344] With respect to the sale, lease, and disclosure of biometric identifiers, the Washington statute permits these activities if "consent has been obtained from the individual"[345] or "an enumerated exception" applies.[346] There are several enumerated exceptions, including "complying with a court order."[347] Another exception is obtaining an unaffiliated party's contractual promise to refrain from subsequent disclosures of the data and enrolling the data in a "database for a commercial purpose inconsistent with the notice and consent" rules described in the statute.[348] To the extent that companies use a consumer's biometric identifier for "a security purpose," they need not provide notice or obtain consent.[349] The statute requires companies using biometric identifiers for commercial purposes to exercise "reasonable care" in securing the data.[350] Retention limits are also imposed on companies using biometric identifiers.[351] Additionally, the statute

---

[343] Allison Grande, *Wash. Expands Biometric Privacy Quilt with More Limited Law*, LAW360 (July 21, 2017, 7:15 PM), https://www.law360.com/articles/934030/print?section=consumerprotection [https://perma.cc/E3GD-A3C8] (contending that "Washington deviates sharply from Illinois by omitting hotly contested provisions that businesses argue expose them to heightened legal liability, notably the right of consumers to sue and for companies to be held accountable for the collection and handling of digital photographs and audio recordings").

[344] Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 U.S. Dist. LEXIS 149604, at *13–14 (N.D. Ill. Sept. 15, 2017) (denying Shutterfly's motion to dismiss and reasoning that "advances in technology are what drove the Illinois legislature to enact the [Illinois statute] in the first place, so it is unlikely that the statute sought to limit the definition of biometric identifier by limiting how the measurements are taken") (internal quotation marks omitted); Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1095, 1104 (N.D. Ill. 2017) (denying Google's motion to dismiss, rejecting Google's argument that by excluding photographs from the definition of biometric data the Illinois statute covers only facial scans "done in person" and reasoning that the statute does not "support this interpretation" as it does not address "how the biometric measurements must be obtained"); Gullen v. Facebook.com, Inc., No. 15 C 7681, 2016 U.S. Dist. LEXIS 6958, at *9 (N.D. Ill. Jan. 21, 2016) (dismissing plaintiff's claim of violations of the Illinois statute based on biometric data collected from digital photographs for lack of jurisdiction); Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015) (denying defendant's motion to dismiss and reasoning that given the Illinois statute's definitions of "biometric identifier" and "biometric information," plaintiff "plausibly stated a claim" by alleging that "defendants are using his personal face pattern to recognize and identify [him] in photographs posted to Websites," among other things).

[345] WASH. REV. CODE ANN. § 19.375.020(3) (West 2017).

[346] Kay & McHugh, *supra* note 27; *see* WASH. REV. CODE ANN. § 19.375.020(3)(a)–(f).

[347] Kay & McHugh, *supra* note 27.

[348] WASH. REV. CODE ANN. § 19.375.020(3)(c).

[349] *Id.* § 19.375.020(7).

[350] *Id.* § 19.375.020(4)(a).

[351] *Id.* § 19.375.020(4) ("A person who knowingly possesses a biometric identifier of an individual that has been enrolled for a commercial purpose: . . . (b) [m]ay retain the biometric identifier no longer than is reasonably necessary to: (i) [c]omply with a court order, statute, or public records retention schedule specified under federal, state, or local law; (ii) [p]rotect against or pre-

prohibits companies that have obtained biometric identifiers from using or disclosing "it in a manner that is materially inconsistent with the terms under which the biometric identifier was originally provided without obtaining consent for the new terms of use or disclosure."[352]

The Illinois statute prohibits sales and leases of biometric data, and obligates private entities that collect biometric data to provide a "written policy" detailing a data retention and destruction schedule.[353] Unlike the Texas and Washington statutes, which impose only general requirements of notice and consent,[354] the Illinois statute contains specific conditions that must be

---

vent actual or potential fraud, criminal activity, claims, security threats, or liability; and (iii) [p]rovide the services for which the biometric identifier was enrolled.").

[352] *Id.* § 19.375.020(5).

[353] 740 ILL. COMP. STAT. ANN. 14/15(a)–(b) (West 2018) ("(a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information[,] . . . . [and] (c) [n]o private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information."). Biometric identifier is defined as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," and biometric information includes "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id.* 14/10. In some instances, even if a company has failed to comply with the disclosure and retention requirements of the Illinois statute, standing issues may prove challenging to consumer claims. In 2017, in *Vigil v. Take-Two Interactive Software, Inc.*, the plaintiffs alleged that by failing to "provide a retention schedule" or data destruction information for their biometric data and obtain their consent in writing, the company violated the requirements of the Illinois statute. 235 F. Supp. 3d 499, 506–07 (S.D.N.Y 2017), *aff'd in part, vacated in part*, Santana v. Take-Two Interactive Software, Inc., No. 17-303, 2017 U.S. App. LEXIS 23446 (2d Cir. Nov. 21, 2017). The district court labeled the plaintiffs' allegations as mere "technical violations" of the Illinois statute. *Id.* at 515. The court reasoned that the plaintiffs had failed to show that the company's practices "resulted in any imminent risk that the data protection goal of the [Illinois statute] would be frustrated" and, "[c]onsequently, more extensive notice and consent could not have altered the standing equation because there ha[d] been no material risk of harm to a concrete . . . interest [under the Illinois statute] that more extensive notice and consent would have avoided." *Id.* at 513. *But see Monroy*, 2017 U.S. Dist. LEXIS 149604, at *23 n.5 (finding that plaintiff "alleged a sufficient injury-in-fact for Article III purposes" because unlike the plaintiffs in *Vigil* who "voluntarily provided their biometric data," the plaintiff was not aware that his biometric data was collected by Shutterfly, which is a sufficient allegation of "invasion of privacy" and is more than a mere "procedural or technical violation" of the Illinois statute). The court's rationale in *Monroy* suggests that whether the consumers voluntarily provided their biometric data or consented to the collection of their data can influence the standing analysis. This is particularly concerning in light of the limitations of relying on consumer consent to justify data collection and use practices as discussed in Part I.B of this Article.

[354] TEX. BUS. & COM. CODE ANN. § 503.001(b) (West 2017) ("(b) A person may not capture a biometric identifier of an individual for a commercial purpose unless the person: (1) informs the individual before capturing the biometric identifier; and (2) receives the individual's consent to capture the biometric identifier."); WASH. REV. CODE ANN. § 19.375.020 (West 2017) ("(1) A person may not enroll a biometric identifier in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose. (2) Notice is a disclosure, that is not considered

satisfied for effective consumer consent to biometric data collection.[355] For instance, under the Illinois statute not only must an individual consent prior to collection, but the individual must be informed "in writing of the specific purpose" for which the data are being "collected, stored and used," and "a written release executed by" the consumer must be obtained.[356] If these requirements are not satisfied, a company may not "collect, capture, purchase, receive through trade, or otherwise obtain" the data.[357] In contrast to the Texas and Washington statutes, the Illinois statute gives aggrieved consumers a right of action for statutory violations.[358]

All three statutes address the monetization of biometric data. However, the statutes do not explicitly reference the creation of security interests in biometric data, databases containing such data, or the transfer of biometric data during bankruptcy proceedings or Article 9 foreclosure sales. Arguably, language in the statutes restricting the transfer, acquisition, and use of biometric data could also apply to impact sales of the data (or databases containing the data) to a third party in bankruptcy, to the extent that state law influences "property rights in bankruptcy" proceedings.[359] This may create tensions with "bankruptcy law's goal of maximizing the size of the estate available for distribution to creditors."[360] Bankruptcy case law suggests that "[w]hile state law creates the [property] right, federal law determines

---

affirmative consent, that is given through a procedure reasonably designed to be readily available to affected individuals. The exact notice and type of consent required to achieve compliance with subsection (1) of this section is context-dependent.").

[355] 740 ILL. COMP. STAT. ANN. 14/15.

[356] *Id.* 14/15(b).

[357] *Id.* 14/15.

[358] *See id.* 14/20 ("Any person aggrieved by a violation of this Act shall have a right of action . . . against an offending party."); TEX. BUS. & COM. CODE ANN. § 503.001(d) ("The attorney general may bring an action to recover the civil penalty."); WASH. REV. CODE ANN. § 19.375.030 ("This chapter may be enforced solely by the attorney general . . . .").

[359] Barnhill v. Johnson, 503 U.S. 393, 398 (1992) ("In the absence of any controlling federal law, 'property' and 'interests in property' are creatures of state law.") (internal modifications omitted); *In re* Costas, 555 F.3d 790, 793 (9th Cir. 2009) (quoting Butner v. United States, 440 U.S. 48, 54 (1979) ("The Code does not define 'property' or 'an interest . . . in property.' Rather, 'Congress has generally left the determination of property rights in the assets of a bankrupt's estate to state law . . . .'"); *In re* Nejberger, 934 F.2d 1300, 1302 (3d Cir. 1991) (noting that although the Bankruptcy Code "defines property of the estate, we must look to state law to determine if a property right exists and to stake out its dimensions"); *In re* Terwilliger's Catering Plus, Inc., 911 F.2d 1168, 1172 (6th Cir. 1990) (citing *In re* N.S. Garrott & Sons, 772 F.2d 462, 466 (8th Cir. 1985)) ("While the nature and extent of the debtor's interest are determined by state law once that determination is made, federal bankruptcy law dictates to what extent that interest is property of the estate.") (internal quotation marks omitted); Juliet M. Moringiello, *A Tale of Two Codes: Examining § 522(F) of the Bankruptcy Code, § 9-103 of the Uniform Commercial Code and the Proper Role of State Law in Bankruptcy*, 79 WASH. U. L. Q. 863, 864 (2001) (contending the "[Bankruptcy] Code begs an answer to the question of whether state law or federal law defines property rights in bankruptcy").

[360] Miller & O'Rourke, *supra* note 36, at 789–90.

whether it is 'property' for purposes of the federal bankruptcy laws . . . ."[361] However, if a CPO is appointed in accordance with the BAPCPA in a bankruptcy proceeding involving the potential transfer of biometric data, the CPO could evaluate whether the data transfer would violate the provisions of an applicable state biometric data statute. The issue of security interests is murkier.

Article 9 also applies to transactions involving a "sale of accounts, chattel paper, payment intangibles, or promissory notes," but not to a direct sale of general intangibles that are not payment intangibles.[362] Of course, to the extent that a security interest is granted in a general intangible, Article 9 will normally apply to the transaction.[363] It is unclear whether the initial granting of a security interest in biometric data (or a database containing such data) qualifies as a commercial purpose, lease, or sale under these state biometric data statutes. However, a foreclosure of such collateral pursuant to Article 9 may effectuate a sale under these statutes even if the initial assignment does not.

Recall that the Illinois statute prohibits the collection and "purchase" of biometric data unless specific consent requirements are satisfied.[364] The term "purchase" is not defined in the definitions section of the statute, but under the UCC, the term "purchase" includes a security interest.[365] To the extent that the term "purchase," as used in the Illinois statute, includes the granting of a security interest, the statute's restrictions would also apply to secured credit transactions.

One could argue that language in the Illinois statute preventing a business from "otherwise obtain[ing] a person's or a customer's biometric" data unless certain requirements are satisfied[366] should also be interpreted to re-

---

[361] *In re* Burgess, 234 B.R. 793, 797 (D. Nev. 1999).

[362] U.C.C. § 9-109(a)(3) (AM. LAW INST. & UNIF. LAW COMM'N 2017); *id.* § 9-102 cmt. 5(d) ("'Payment Intangible' is a subset of the definition of 'general intangible.' The sale of a payment intangible is subject to this Article."); N.Y. U.C.C. LAW § 9-408 cmt. 4 (McKinney 2017) ("The only sales of general intangibles that create security interests are sales of payment intangibles."); DAVID S. WILLENZIK, LOUISIANA PRACTICE SERIES: SECURED TRANSACTIONS § 11.26, Westlaw (database updated Dec. 2012) ("While UCC Article 9 applies to true sales of accounts, La UCC § 9-102(1)(b), Article 9 does not apply to true sales or transfers of general intangibles.").

[363] U.C.C. § 9-408 cmt. 2 ("This result allows the creation, attachment, and perfection of a security interest in a general intangible, such as an agreement for the nonexclusive license of software . . . ."); *In re* Emergency Beacon Corp., 23 U.C.C. Rep. Serv. 766, 769–70 (S.D.N.Y. 1977) ("[P]atent rights, tradename, customer lists, books and records and [the] right to manufacture or sell emergency beacons and related electronic equipment are general intangibles [under Article 9]."); 2-29 COMMERCIAL LAW AND PRACTICE GUIDE § 29.03, Lexis (database updated June 2017) (describing "computer data and programming" as general intangibles).

[364] 740 ILL. COMP. STAT. ANN. 14/15 (West 2018).

[365] U.C.C. § 1-201(b)(29) (stating that the term "'[p]urchase' means taking by . . . security interest," among other things).

[366] 740 ILL. COMP. STAT. ANN. 14/15.

fer to transactions involving security interests in data. The disclosure of biometric data to the secured party during due diligence, or subsequently as part of the secured party's inspection or audit of the collateral, may also be subject to the statute's requirements.[367] Companies in need of financing may ultimately find new ways to permit lenders to verify the source and value of their customer databases without disclosing biometric data prior to obtaining consumer consent. Additionally, language in all three statutes regarding retention (and possible destruction) of biometric data after a specified period may severely impact the value of such data for secured credit purposes. The language in the Illinois statute expressly prohibiting the sale and lease of biometric data may also lead biometric databases to be viewed as less attractive assets for secured financing purposes.

As previously mentioned, subject to one exception, the Texas statute authorizes the sale, lease, and disclosure of biometric data if a state or federal statute requires or permits the disclosure.[368] In contrast, the Illinois statute does not authorize sales or leases, but permits disclosures of biometric data in certain instances, such as when "State or federal law or a municipal ordinance" requires the disclosure to be made.[369] The Washington statute permits transfers and disclosures of biometric data if "required or expressly authorized" by statute.[370]

Debtors are not required by Article 9 to enter into a secured transaction, and so any resulting disclosure or transfer of consumer biometric information is arguably not required by a state's version of the UCC for purposes of the

---

[367] *Id.* 14/15(d) ("No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless: (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure; (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative; (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.").

[368] TEX. BUS. & COM. CODE ANN. § 503.001(b)–(c) (West 2017) ("(b) A person who possesses a biometric identifier of an individual that is captured for a commercial purpose: (1) may not sell, lease, or otherwise disclose the biometric identifier to another person unless: . . . [(c)(1)](C) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552, Government Code . . . .").

[369] 740 ILL. COMP. STAT. ANN. 14/15(d) ("No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless: . . . (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance . . . .").

[370] WASH. REV. CODE ANN. § 19.375.020(3) (West 2017) ("Unless consent has been obtained from the individual, a person who has enrolled an individual's biometric identifier may not sell, lease, or otherwise disclose the biometric identifier to another person for a commercial purpose unless the disclosure: . . . (d) [i]s required or expressly authorized by a federal or state statute, or court order . . . .").

Washington and Illinois statutes. On the other hand, once a security interest is created, Article 9 grants certain rights to secured parties, and arguably these provisions may authorize the disclosure and transfer of the debtor's collateral, including customer databases containing biometric data. Because the Illinois statute contains an exception only for the disclosure (not the sale or lease) of biometric data under certain circumstances, such as when the consumer consents, the ability of secured parties to foreclose on collateral involving biometric data may also be restricted.[371] In contrast, under the Texas statute, one could contend that Article 9 (as enacted by the state) is a statute that permits secured parties to receive an interest in and possibly obtain and dispose of the debtor's collateral, and therefore the sale by, or disclosure of biometric data to, secured parties in accordance with Article 9 is permissible. This rationale could also be used to justify the sale of such data under the Bankruptcy Code.

A secured party may not always want to sell or lease the collateral to third parties but could be interested in using the collateral in its own business as permitted under Article 9. The language of the Texas statute may not deter secured parties from taking security interests in customer databases containing biometric data when the secured party is in the same line of business as the debtor or would like to operate the debtor's business. In *Information Exchange Systems, Inc. v. First Bank National Ass'n*, after default, an unaffiliated party that obtained its rights in the debtor's collateral via assignment from the original lender, "strictly foreclosed the security interest[]" in the debtor's collateral and then used the debtor's assets to conduct its business operations.[372]

Recall that the Illinois statute provides that to the extent that a company is in possession of biometric data, it may not "sell, lease, trade, or otherwise profit from" the data.[373] Thus, unlike the Washington and Texas statutes which authorize such activities when notice and consent is met, among other things, the Illinois statute's prohibition on such activities may provide more protection to consumers. As noted above, with the exception of a sale that effectuates a foreclosure, collateral is not otherwise sold or leased when a traditional security interest is created.[374] Arguably, a company obtains no "profit" from encumbering its collateral even though value is given as part of the transaction. It is unclear whether the language "otherwise profit from" was also intended to cover value transferred to the debtor as part of a secured financing transaction under Article 9.

---

[371] *See* 740 ILL. COMP. STAT. ANN. 14/15 (West 2018).

[372] Info. Exch. Sys., Inc. v. First Bank Nat'l Ass'n, Nos. CIV. 4-91-902, CIV. 4-92-224, 1992 WL 494607, at *1 (D. Minn. July 23, 1992), *aff'd*, 994 F.2d 478, 481 (8th Cir. 1993); *see also* Nguyen, *Collateralizing*, *supra* note 19, at 589–90 (discussing the *Information Exchange* case).

[373] 740 ILL. COMP. STAT. ANN. 14/15(c).

[374] *See supra* note 362–365 and accompanying text.

The statutes' disclosure provisions may also apply to a company's use of third-party service providers for data analytics, processing, and monitoring purposes. Arguably, the language "otherwise profit from" in the Illinois statute could be interpreted as prohibiting the use of data analytics when biometric data are involved. Companies can profit from data analytics in many ways. Data analytics allows companies to gain insights into customer behavior, "[b]oost [j]ob [s]atisfaction" and "[i]mprove [s]ervice" to customers.[375] However, other provisions of the Illinois statute suggest that if a consumer consents to the disclosure of their biometric data to third-party service providers, the disclosure may be permissible.

In short, these biometric data statutes may authorize the disclosure or transfer of consumer data when consumer consent is received. The limitations of notice and choice are problematic, as discussed in earlier parts of this Article, including because companies could ultimately influence consumers' perceptions about acceptable disclosures and uses of biometric data, and may exert pressure to normalize dubious biometric data disclosure and transfer practices.[376] As a result, various aspects of these statutes suffer from similar defects found in other frameworks that also rely on a notice and choice model as the primary method of consumer protection. The statutory restrictions on the use of biometric data may also rely on the express terms of a company's privacy policy as a means of safeguarding consumers, as evidenced by the Washington statute's prohibition on subsequent materially inconsistent uses and disclosures in the absence of consumer authorization.[377] If the terms initially provided by the company in connection with the collection of the data are drafted broadly to authorize various uses by the company, subsequent uses of the data (even for dubious purposes) may be permissible. Even terms that were narrowly drafted initially could be revised to authorize later disclosures and uses as long as consumer consent is received. Lastly, the status of security interests under these statutes is not entirely clear.

D. HIPAA

The Health Insurance Portability and Accountability Act ("HIPAA")[378] protects healthcare information when the data are collected by a health care

---

[375] Paul Rubens, *6 Ways to Profit from Data Analytics*, ENTERPRISE APPS TODAY (Mar. 10, 2016), http://www.enterpriseappstoday.com/business-intelligence/6-ways-to-profit-from-data-analytics.html [https://perma.cc/7PSQ-XXKN].

[376] *See supra* notes 263–333 and accompanying text.

[377] WASH. REV. CODE ANN. § 19.375.020(5) (West 2017).

[378] This section does not address state laws that may also impact health-related data but rather focuses on HIPAA, as such an assessment is beyond the scope of this Article. Moreover, as one scholar has noted, "state laws are varied and inconsistent, often providing piecemeal protection for

provider, health plan, or health care clearinghouse, or the business associates of these entities.[379] Organizations covered by HIPAA are required to comply with regulations regarding protected "health information."[380]

The collection and use of health-related data generated by IoT devices may not be governed by HIPAA.[381] Many IoT companies do not qualify as "covered entities" because they are unlikely to provide "medical or health

---

some types of data but not others and these protections maybe scattered among multiple laws." HOFFMAN, *supra* note 197, at 135.

[379] 42 U.S.C. §§ 1320d–1320d-8 (2012) (statutory authority); 45 C.F.R. § 160.103(3) (2017) (defining a "covered entity" as a "health plan," "health care clearinghouse," "health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter," or "business associate of another covered entity"); 45 C.F.R. §§ 160.101–.534 (privacy rule); 45 C.F.R. §§ 164.302–.318 (security rule); HOFFMAN, *supra* note 197, at 73 (HIPAA "regulations define 'covered entities' as including health plans, health-care clearing houses, healthcare providers . . . and their business associates. Consequently, doctors, hospitals, pharmacists, health insurers, and HMOs must comply with the HIPAA privacy standards but not all parties possessing identifiable health data are covered."); Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 336 (2007) (The HIPAA "Security Rule is part of the larger HIPAA Privacy Rule established in the HIPAA privacy regulations promulgated pursuant to HIPAA's statutory authority"); Stacey A. Tovino, *Silence Is Golden . . . Except in Healthcare Philanthropy*, 48 U. RICH. L. REV. 1157, 1162 (2014) ("The original HIPAA statute clarified . . . that any privacy regulations adopted by HHS must be made applicable only to three classes of individuals and institutions: (1) health plans; (2) health care clearinghouses; and (3) health care providers who transmit health information in electronic form in connection with certain standard transactions . . . .").

[380] *See* 45 C.F.R. § 160.103 (defining health information as information that "[i]s created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse . . . [that] relates to the . . . health or condition of an individual . . ."). The term "individually identifiable health information" is defined "as a subset of health information" and "protected health information" is defined as "individually identifiable health information." *Id.*

[381] FTC IOT REPORT, *supra* note 322, at 52 (noting that frequently "health apps are collecting [private patient information, such as their medical history,] through consumer-facing products, to which HIPAA protections do not apply"); Jillisa Bronfman, *Weathering the Nest: Privacy Implications of Home Monitoring for the Aging American Population*, 14 DUKE L. & TECH. REV. 192, 201–02 (2016) (contending that "if the entity gathering health data is not a covered provider like a hospital or medical care provider, there is no protection from HIPAA"); Elizabeth A. Brown, *The Fitbit Fault Line: Two Proposals to Protect Health and Fitness Data at Work*, 16 YALE J. HEALTH POL'Y L. & ETHICS 1, 24 (2016) ("When a Fitbit or iPhone app tells an employer how much an employee has exercised, what her heart rate is, or how high her blood sugar levels are, those data do not fall within the scope of HIPAA protection."); Nissenbaum & Patterson, *supra* note 16, at 92 ("[H]ealth-self tracking information does not usually fall under the purview of HIPAA because the law is limited to discrete healthcare relationships, rather than health information."); Elizabeth Snell, *How Do HIPAA Regulations Apply to Wearable Devices?*, HEALTHITSECURITY (Mar. 23, 2017), http://healthitsecurity.com/news/how-do-hipaa-regulations-apply-to-wearable-devices [https://perma.cc/5JMG-3RJB] ("[W]here a company that offers a wearable, or a mobile app that collects health information, where that arrangement is just directly between the device maker and the individual. Or it's between the app maker and the individual, and there's no covered entity or business associate involved. Then there's no application of HIPAA . . . .") (internal quotation marks omitted).

services," health insurance plans, or process health care information in connection with the sale of IoT devices and the provision of related services and software to consumers.[382] The use of health-related data shared by consumers who use IoT devices is likely to be governed mainly by the entities' privacy policy.

IoT companies also may not qualify as business associates under HIPAA regulation because they are unlikely to be hired to perform activities or services, such as "claim processing, administration [and] data analysis," in connection with "protected health information" on behalf of HIPAA covered entities.[383] If IoT companies begin to integrate their services and devices with the offerings of HIPAA covered entities and handle "protected health information" on behalf of such entities, there would be a stronger argument for HIPAA compliance.[384]

HIPAA regulation does not always restrict the use of health information, and it permits covered entities to use and transfer certain health related information after receiving individual authorization.[385] One scholar

---

[382] *See* 45 C.F.R. § 160.103 (defining health care provider, health care clearing house, and insurance plan); *see also* FTC IOT REPORT, *supra* note 322, at 52; Nissenbaum & Patterson, *supra* note 16, at 92 (although under HIPAA "physicians or insurance plans are subject to restrictions regarding storage and distribution of their patients' or customers' health self-tracking data, commercial actors and others who hold the same data are not"); MICHELLE DE MOOY, CTR. FOR DEMOCRACY & TECH, SHELTON YUEN, FITBIT, INC., TOWARD PRIVACY AWARE RESEARCH AND DEVELOPMENT IN WEARABLE HEALTH 8 (May 2016), https://cdt.org/files/2017/07/2016-05-17-Fitbit-FNL1.pdf [https://perma.cc/ZG2B-96WQ] ("Some wearables involved in health and wellness collect and use sensitive personal health information, but because the data generated by them is [sic] created at the direction of the user, it is mostly outside of the disclosure restrictions and requirements found in [HIPAA] . . . .").

[383] *See* 45 C.F.R. § 160.103 (defining business associate); *id.* § 164.502 (providing rules applicable to business associates); J. Frazee et al., *mHealth and Unregulated Data: Is this Farewell to Patient Privacy?*, 13 IND. HEALTH L. REV. 385, 392 (2016) (contending that mobile health applications "that are consumer oriented manage user-generated information that is not HIPAA protected, such as the calories in one's meal or the amount of steps one has taken on a given day," and "[a]s long as [the mobile health] app does not deal in [protected health information] or communicate with a covered entity or business associate it is not subject to HIPAA").

[384] Press Release, Fitbit, Fitbit Extends Corporate Wellness Offering with HIPAA Compliant Capabilities (Sept. 16, 2015), https://investor.fitbit.com/press/press-releases/press-release-details/2015/Fitbit-Extends-Corporate-Wellness-Offering-with-HIPAA-Compliant-Capabilities/default.aspx [https://perma.cc/XD9E-R3P9] (describing Fitbit's support of HIPAA compliance to enable "Fitbit Wellness to more effectively integrate with HIPAA-covered entities, including corporate wellness partners, health plans and self-insured employers").

[385] HOFFMAN, *supra* note 197, at 132 ("The HIPAA Privacy Rule generally prohibits disclosure of individually identifiable health information without patient authorization, unless the information is transmitted for purposes of treatment, payment, or healthcare operations."); Beverly Cohen, *Regulating Data Mining Post-*Sorrell*: Using HIPAA to Restrict Marketing Uses of Patients' Private Medical Information*, 47 WAKE FOREST L. REV. 1141, 1165, 1170 (2012) (suggesting that individual authorization is needed prior to de-identifying protected health information when the purpose is for marketing and that "HIPAA's primary marketing restriction is that whenever a covered entity uses or discloses protected health information for marketing purposes, the

notes that under HIPAA, "[a] covered entity must obtain consent to share [protected health information] if the entity sells the information for either direct or indirect compensation, or marketing."[386] Thus, the HIPAA regime also adopts a notice and consent model that allows covered entities, in some instances, to transfer consumer health-related data when consent is received.[387] Additionally, the HIPAA privacy rule "does not prohibit covered entities from disclosing deidentified data to third parties . . . ."[388] Recall that de-identified data can be re-identified through the use of "powerful re-identification algorithms."[389] Other scholars have noted that under HIPAA, "a patient's right to restrict sharing of her data is quite limited."[390]

To the extent that HIPAA regulation permits disclosures and transfers to unaffiliated parties for non-research or non-healthcare purposes, and relies excessively on a notice and consent model to regulate data disclosures, the HIPAA regime also suffers from similar limitations found in other privacy frameworks. Most concerning is the likely exclusion of IoT companies and much of the health-related data obtained from consumers' use of IoT devices and services from HIPAA's limited protections. In such instances,

---

individual must expressly authorize the use or disclosure"); U.S. DEP'T HEALTH & HUM. SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 4 (revised May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf?language=es [https://perma.cc/FPK4-XV3V] ("A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.").

[386] Janine S. Hiller, *Healthy Predictions? Questions for Data Analytics in Health Care*, 53 AM. BUS. L.J. 251, 283 (2016); *see* 42 U.S.C. § 17935(d) (2012 & Supp. IV 2016) ("Prohibition on sale of electronic health records or protected health information" in the absence of individual consent subject to some exceptions); 45 C.F.R. § 164.502 (providing rules for use and disclosure of data by covered entities); 45 C.F.R. § 164.508(a) (imposing consent requirements for the sale of protected health information and providing rules for the use and disclosure of health information for marketing purposes); *see also* Christopher R. Smith, *Somebody's Watching Me: Protecting Patient Privacy in Prescription Health Information*, 36 VT. L. REV. 931, 950 (2012) ("[C]overed entities and business associates are prohibited from selling protected health information without patient authorization, except under certain circumstances.").

[387] Robert Gellman, Fair Information Practices: A Basic History 19 (Apr. 10, 2017) (unpublished manuscript) (on file with author) (contending that the "U.S. Department of Health and Human Services relied upon FIPs in issuing a privacy rule under . . . [HIPAA]," and describing the origins and impact of FIPs on the U.S. privacy regime). "Notice/Awareness" and "Choice/Consent" are two of five "core principles" embodied in FIPs. *Id.*

[388] HOFFMAN, *supra* note 197, at 132.

[389] Arvind Narayanan & Vitaly Shmatikov, *Myths and Fallacies of "Personally Identifiable Information,"* COMM. ACM, June 2010, at 24, 25–26 (discussing the safe harbor provisions of the HIPAA Privacy Rule and contending that "[t]he emergence of powerful re-identification algorithms demonstrates not just a flaw in a specific anonymization technique(s), but the fundamental inadequacy of the entire privacy protection paradigm based on 'de-identifying' the data"); *see supra* notes 119–123, 197–200 and accompanying text.

[390] Hiller, *supra* note 386, at 283.

protection of consumer IoT health-related data is primarily left to a company's privacy policy, unless another source of law regulates this information.

IV. PATHS FORWARD

The limitations of existing privacy frameworks that rely excessively on a notice and choice model and the terms of a company's privacy policy, combined with the exponential growth and proliferation of new types of highly sensitive IoT consumer data, necessitate new discussions and solutions on how best to ensure the protection of consumer privacy and data in the IoT setting.

Admittedly, there may be numerous frameworks in need of revision in order to adequately safeguard consumers in the IoT setting. Commercial law is a productive place to begin this endeavor given the potential value of IoT data as a source of financing, the numerous bankruptcy proceedings involving consumer data, and the provisions of privacy policies that frequently permit the disclosure of consumer data in commercial transactions.

The statutory solutions proposed in this Part are not meant to suggest that Article 9 or the Bankruptcy Code alone can protect consumers from all harms associated with data transfers and disclosures or other issues related to privacy and data security. A comprehensive shift in the way companies view consumer data and design consumer products that collect data is also necessary. Consideration must also be given to monetizations of consumer IoT data that occur outside of the Article 9 and bankruptcy context, such as direct sales of consumer related data. Furthermore, simultaneous use of various "data protection models" that regulate the initial collection and subsequent distribution and transfer of consumer data as well as other types of permissible data uses, are needed in the IoT setting to sufficiently protect consumer interests.[391] Lastly, consideration should also be given to whether

---

[391] *See* Nicolas P. Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 HEALTH MATRIX 65, 66 (2014) (discussing "health privacy exceptionalism" and noting that "while upstream data protection models limit data collection, downstream models primarily limit data distribution *after* collection"); Revised Statement of Commissioner Brill, in Which Chairman Leibowitz and Commissioners Rosch and Ramirez Join, In the Matter of SettlementOne Credit Corporation, In the Matter of ACRAnet, Inc., In the Matter of Fajilan and Associates, FTC File Nos. 082-3208, 098-3088, 092-3089 (Aug. 15, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819settlementonestatement.pdf [https://perma.cc/P7WA-H9JN] (describing the "first cases in which the [FTC] has held resellers responsible for downstream data protection failures"). The Supreme Court's anticipated decision in *United States v. Carpenter* may also impact privacy expectations and views about the collection and disclosure of data in certain settings. 819 F.3d 880 (6th Cir. 2016) (holding that "the government's collection of business records containing cell-site [location] data was not a search under the Fourth Amendment"), *cert. granted*, 137 S. Ct. 2211 (2017); Allison Grande, *Privacy Fights to Watch at the Supreme Court*, LAW360 (Sept. 29, 2017, 11:59 PM), https://www.law360.com/articles/969610/privacy-fights-to-watch-at-the-supreme-court [https://perma.cc/3U5Z-67ZA] (discussing the implications of the *Carpenter* case).

amendments to HIPAA are necessary to address concerns regarding health-related data collected by IoT devices.

The remainder of this Part offers various proposals to engender movement away from an overreliance on the notice and choice model and the terms of privacy policies and decrease the various moments of data disclosures authorized by privacy policies and the financial frameworks of Article 9 and the Bankruptcy Code. Reducing moments of data transfers and disclosures may alleviate and prevent some of the significant privacy violations and harms that can occur from the disclosure of highly-sensitive IoT consumer data via Article 9 and the Bankruptcy Code.

A. Transfer & Assignment Restrictions

As other scholars have argued, because of the "highly personal nature" of certain types of consumer data, some categories of personal information may be adequately protected only if the data are rendered inalienable.[392] Consumers may be unable to appreciate the dangers involved with the potential assignment or sale of biometric and health-related data. Given the lack of consumer understanding of the risks associated with the disclosure of their data it is not surprising that "[t]he market for the sale of personal information is often inefficient . . . ."[393] Consumers may not understand the applicable legal rules that permit disclosure of their data. Companies should not be permitted to exploit consumer ignorance about the value of their data.

While some privacy policies may contain contractual restraints—for instance by limiting the parties to whom data can be transferred—privacy policies cannot be solely relied upon to protect consumer interests. Statutory restraints on the transfer of rights in consumer data assets will likely be necessary.

The transfer and assignment restrictions proposed below do not prohibit consumers from providing biometric or health-related data to companies, but rather focus on restricting companies' subsequent assignment of rights in and transfer of such data pursuant to Article 9 and the Bankruptcy Code with the goal of "reducing their value and disincentivizing collection."[394] However, as noted earlier, restrictions on the initial data collection by companies and other types of consumer data uses, as well as the imposition of specific obligations on companies with respect to consumer data, may also be necessary to adequately protect consumer interests. Additional-

---

[392] Miller & O'Rourke, *supra* note 36, at 847.

[393] *Id.*

[394] *See* Nicolas P. Terry, *Regulatory Disruption and Arbitrage in Health-Care Data Protection*, 17 YALE J. HEALTH POL'Y L. & ETHICS 143, 152 (2017) [hereinafter Terry, *Regulatory Disruption*].

ly, these restraints should not negatively impact the use of such data for research or healthcare purposes.

As other privacy scholars have noted, regulation aimed at protecting consumer privacy should consider "who is gathering the information, who is analyzing it, who is disseminating it and to whom [as well as] the nature of the information."[395] The transfer restrictions discussed in the remainder of this section focus on biometric and health-related data given their highly sensitive nature and the dangers associated with companies' disclosure and transfer of same.[396] Biometric data are generally immutable and, in this

---

[395] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV 119, 154 (2004). *See generally* Helen Nissenbaum, *"Respect for Context": Fulfilling The Promise of the White House Report*, *in* PRIVACY IN THE MODERN AGE: THE SEARCH FOR SOLUTIONS 152, 161 (Marc Rotenberg et al., eds., 2015) (discussing contextual integrity and suggesting that "information flows [should] be characterized in terms of information types, actors, and transmission principles and evaluated in terms of the balance of interests and impacts on values and contextual aims"); Narayanan & Shmatikov, *supra* note 389, at 25 (critiquing the HIPAA Privacy Rule's reliance on the term "personally identifiable information" and anonymization) ("The natural approach to privacy protection is to consider both the data and its proposed use(s) and to ask: What risk does an individual face if her data is used in a particular way? Unfortunately, existing privacy technologies such as *k*-anonymity focus instead on the data alone").

[396] One potential critique of imposing transfer and assignment restrictions is that such limitations implicate First Amendment concerns given the Supreme Court's decision in *Sorrell v. IMS Health Inc.* in 2011. 564 U.S. 552, 552–59 (2011) (holding that a Vermont statute that restricted specific entities' ability to sell or use "prescriber-identifying information" for "marketing or promoting a prescription drug, unless the prescriber consents . . . . impose[d] content- and speaker-based burdens on protected expression [and was] subject to heightened judicial scrutiny"); *see also* Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 71 (2014) (contending that part of the *Sorrell* "opinion suggested that the restriction on transfers of data between willing givers and receivers was automatically a restriction of speech"); Ashutosh Bhagwat, Sorrell v. IMS Health: *Details, Detailing, and the Death of Privacy*, 36 VT. L. REV. 855, 856 (2012) (suggesting that "hints" left by the *Sorrell* court may negatively impact the validity of rules aimed at protecting privacy). Although the impact of the holding in *Sorrell* is unclear and privacy scholars continue to debate its holding, restrictions on data usage and transfers may be constitutional even after *Sorrell*. *See* Bambauer, *supra*, at 64 ("Although the First Amendment creates a barrier to the enforcement of new and existing information laws, that barrier is not insurmountable."). Furthermore, one scholar notes that "[a]lthough the Court [in *Sorrell*] hinted that the sale of a database might be speech, the Court stopped short of that sweeping conclusion because the regulation's discrimination against marketers was a content- and viewpoint-based restriction." Neil Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1506, 1521–24 (2015) (contending that the *Sorrell* decision does not upset the well-established understanding that "general commercial regulation of the huge data trade [is] not censorship"). The Vermont statute at issue failed to "regulate enough" speech as it "discriminated against particular kinds of protected speech (in-person advertising) and particular kinds of protected speakers (advertisers but not their opponents)." *Id.* at 1501, 1506; *see Sorrell*, 564 U.S. at 580 (stating that "the State has left unburdened those speakers whose messages are in accord with its own views"). Furthermore, rather than directly regulating the disclosure of consumer data, the Vermont statute in *Sorrell* appears to have been aimed at decreasing drug prices and protecting doctors' prescribing information to curb the impact of data brokers on doctors' prescription decisions. Richards, *supra*, at 1518. Post-*Sorrell*, some federal courts have declined to adopt an expansive view of the case's holding, and at least one court has upheld a statute restricting the transfer and disclosure of consumer information. *See,*

way, share some characteristics with other parts of the body that our society has determined should not be sold.[397] Other types of traditional data that are not alterable by consumers could also be viewed as immutable. As more disruptive technological developments arise, proactive diligence in thinking through the scope of rights in IoT data will be needed. There may ultimately come a time when certain types of data and information about an individual becomes indistinguishable from personhood.

As IoT technology evolves, additional restraints on transfers may be necessary for other types of highly sensitive IoT data as well, such as information about consumers that is embarrassing, intimate, or that may negatively impact a person's reputation.[398] Consider that self-driving cars can

---

e.g., Boelter v. Hearst Commc'ns, Inc., 192 F. Supp. 3d 427, 435, 446–47 (S.D.N.Y. 2016) (applying *Sorrell* and rejecting a First Amendment challenge to a Michigan statute that prohibited individuals "engaged in the business of selling at retail, renting, or lending books or other written materials, sound recordings, or video recordings" from "disclos[ing] to any person, other than the customer, information" that could identify consumers); King v. General Info. Servs., Inc., 903 F. Supp. 2d 303, 308–09 (E.D. Pa. 2012) (rejecting a First Amendment challenge to 1681(c) of the Fair Credit Reporting Act and reasoning that "the *Sorrell* Court did not take issue with Vermont's law merely because it imposed a content- and speaker-based restriction on commercial speech, but because its restriction could not be justified on neutral grounds . . . [and post-*Sorrell*,] the typical commercial speech inquiry under intermediate scrutiny of [the *Central Hudson* test] remains valid law"). The *Boelter* court reasoned that the Michigan statute at issue "indiscriminately" restricted "the group of individuals most likely to reveal consumer identifying information," in contrast to the Vermont statute at issue in *Sorrell*, that was "targeted at certain speakers who were but a minority of those able to acquire or use the protected information." *Boelter*, 192 F. Supp. at 450. The *Boelter* decision suggests that even post-*Sorrell*, courts may be willing to uphold legislation aimed at protecting consumer privacy. *Id.* at 446 (stating that "Michigan [should] be afforded greater leeway in regulating the dissemination of consumer data"). Moreover, the *Sorrell* court acknowledged that "content-based restrictions on [commercial speech] are sometimes permissible," and that "the government's legitimate interest in protecting consumers from 'commercial harms' explains 'why commercial speech can be subject to greater governmental regulation than noncommercial speech.'" *Sorrell*, 564 U.S. at 579. Like the Michigan statute in *Boelter*, the restrictions proposed in this Article are aimed at protecting the privacy of consumers. *See Boelter*, 192 F. Supp. 3d at 435. Given the "volume, velocity and variety of data" generated by the IoT, there is a substantial governmental interest in protecting the privacy of consumers in the IoT setting. *See supra* notes 11–13, 49 and accompanying text. A reasonable fit likely exists between regulation that prohibits and restricts the dissemination of highly sensitive consumer data and advances the substantial interest of protecting consumer privacy (consumer protection). Lastly, to the extent that the restrictions proposed in this Article can be viewed as prohibiting consumers from granting companies rights in their data for purposes of assignments and sales in the bankruptcy and Article 9 contexts or "waiving their privacy rights" in connection with such transactions, one could contend that any such adopted legislation is grounded in contract law and therefore avoids First Amendment concerns. Richards, *First Amendment*, *supra* note 221, at 1204 ("Instances of contractual commercial regulation are well outside the scope of the First Amendment.").

[397] *Cf.* National Organ Transplant Act, 42 U.S.C. § 274e(a) (2012) ("It shall be unlawful for any person to knowingly acquire, receive, or otherwise transfer any human organ for valuable consideration for use in human transplantation if the transfer affects interstate commerce.").

[398] Additionally, one could posit that to the extent that IoT data are an asset under financial frameworks, companies that provide IoT products should not be permitted to reap all of the profits or benefits generated from such data to the exclusion of consumers. Continuing that line of argu-

identify how many people are inside a vehicle and "what they are doing."[399] This information could also be viewed as highly sensitive and in need of protection.

To give effect to restrictions that would limit the disclosures and transfers authorized by privacy policies and financial frameworks, separate state statutes and amendments to Article 9 and the Bankruptcy Code could be adopted.

1. Separate State Statutes

State statutes, to the extent that they do not already, could require explicit consumer consent for the creation of security interests in health-related or biometric data (or databases storing such data). Alternatively, state statutes could specifically prohibit companies' assignment of rights in, or a transfer of, biometric and health-related data or databases containing these data regardless of receipt of consumer consent.[400] The latter solution is preferable in light of earlier discussions regarding the limits of consumer consent and could broadly apply to various types of monetizations.[401]

Section 9-201 provides that agreements that are governed by Article 9 can also be subject to laws that provide distinct rules for consumers (e.g. consumer protection statutes) and any such laws control in the event of a conflict with Article 9.[402] The state statutes proposed above restricting the transfer and

---

ment, the provision of IoT services and goods should not be the point at which a monopoly on the data is conferred to companies. One could also contend that when a consumer is a high-value data generator, consumers should be able to monetize their own data in some instances. Companies, such as Datacoup, are in the business of providing financial compensation directly to consumers who provide their data. *See generally* Elvy, *supra* note 92 (discussing personal data economy companies, such as Datacoup). Although this Article does not contend that biometric data or other types of IoT consumer data should never be collected, there are potential concerns with permitting certain types of IoT data to be freely transferred and monetized by companies. The transfer or disclosure of such data by consumers also presents similar concerns. *Id.* (discussing concerns associated with personal data economy models).

[399] Devin Coldewey, *In-Car Cameras Let Autonomous Vehicles Track Passengers as Well as Pedestrians*, TECHCRUNCH (Aug. 1, 2016), https://techcrunch.com/2016/08/01/in-car-cameras-let-autonomous-vehicles-track-passengers-as-well-as-pedestrians/ [https://perma.cc/PUK4-Z83X]; Edward Niedermeyer, *Your Tesla Is Watching You—Whether or Not You're Watching the Road*, QUARTZ (Aug. 17, 2016), https://qz.com/759896/your-tesla-is-watching-you-whether-or-not-youre-watching-the-road/ [https://perma.cc/A9QE-56SZ].

[400] A federal statute addressing this issue may be preferable.

[401] *See supra* notes 94–129 and accompanying text.

[402] *See* U.C.C. § 9-201(b)–(c) (AM. LAW INST. & UNIF. LAW COMM'N 2017); *In re* Howard v. AmeriCredit Fin. Servs., 597 F.3d 852, 856 (7th Cir. 2010) ("Article 9 of the UCC states that transactions governed by it are subject to statutes that establish 'a different rule for consumers,' . . . which in Illinois includes the Motor Vehicle Retail Installment Sales Act."); *In re* Visnicky, 401 B.R. 61, 66 (Bankr. D. R.I. 2009) ("'[T]he most important provisions in Article 9 are found in Rev. UCC 9-201, which defers to any consumer protection legislation of the enacting state in conflict with the UCC.'"); Juliet M. Moringiello, *(Mis)Use of State Law in Bankruptcy: The*

assignment of rights in consumer generated data could be viewed as consumer protection legislation, and one could contend that Article 9's provisions must defer to any such legislation in accordance with section 9-201. However, consumers are unlikely to be directly involved in a transaction between the debtor company and the secured lender even though consumer generated data may be at issue.[403] Further, given the provisions of Article 9, which will be discussed in detail below, that negate statutory and contractual attempts to restrict the creation of a security interest in certain types of collateral, revisions to Article 9 may still be necessary even if separate state statutes are adopted. Such revisions to Article 9 could promote consistency across all related state statutes, including Article 9, clarify whether Article 9's anti-assignment provisions supersede the assignment and transfer restrictions contained in any such state statutes, and to the extent that 9-201 is applicable, avoid disputes about whether the state statute conflicts with Article 9.[404]

2. Article 9 Amendments

Article 9 could be amended to include assignment restrictions on consumer data. It could provide that even if a consumer consented to a privacy policy that contained provisions permitting the transfer or disclosure of such data as part of a secured financing transaction subject to Article 9, the secured party and other unaffiliated entities are prevented from obtaining the biometric or health-related data. By focusing on biometric and health-related data, the proposed Article 9 amendments discussed below attempt to

---

Hanging Paragraph Story, 2012 WIS. L. REV. 963, 979 & n.76 ("Although the UCC includes some sections that may appear to be protective of consumers, it expressly yields to consumer protection statutes."). By its language, section 9-201(b)'s provisions are also subject to state variation and can include specific references to state consumer protection statutes as well as "any other statute or regulation that regulates the rates, charges, agreements, and practices for loans, credit sales, or other extensions of credit." U.C.C. § 9-201(b).

[403] *See* RUSCH & SEPINUCK, *supra* note 167, at 145–46 ("[A] secured party enforcing its security interest against a consumer must also comply with whatever consumer-protection laws might be applicable."). *But see* Tex. Lottery Comm'n v. First State Bank of Dequeen, 325 S.W.3d 628, 637 (Tex. 2010) (rejecting an argument that a state statute provides a separate rule for consumers because a consumer was involved in the transaction and reasoning that "the UCC does not address individual transactions undertaken by consumers," but instead "addresses rules of law, statutes, and regulations that apply broadly").

[404] *Tex. Lottery Comm'n*, 325 S.W.3d at 637–39 (finding that the state lottery statute at issue applied to all individuals and was "not a statute or rule of law that establishe[d] a different rule for consumers within the meaning of 9-201(b)" and that section 9-406's anti-assignment provisions invalidated the anti-assignment provisions of the lottery statute); *see* U.C.C. § 9-201(c) ("Failure to comply with a statute or regulation described in subsection (b) has only the effect the statute or regulation specifies."); RUSCH & SEPINUCK, *supra* note 167, at 146 ("In the rare instance when the rules on enforcement in Article 9 conflict with some other applicable rule of law (such that compliance with both laws is not possible), the creditor might need to file a declaratory action to seek a court determination of which set of requirements is paramount.").

strike a balance between protecting consumer privacy and permitting companies to use other types of IoT data for asset based financing transactions. One approach to amending Article 9 would be to have individual states make non-uniform amendments, which may then lead to amendments of the official text of Article 9. To impose comprehensive assignment restrictions, Article 9 would need to be amended to limit the creation and enforceability of a security interest in biometric and health-related data, the customer database and rights to the customer database containing biometric and health-related data. This could occur in several ways.

The scope provisions of section 9-109(d)[405] could be amended to exclude assignments in biometric and health-related data (and databases containing such information) when the proposed debtor is a company. To the extent that such an amendment is made, consideration must also be given to whether excluding the transaction from Article 9 simply results in another source of law governing liens in consumer data.[406] Additionally, even if separate state statutes restricting transfers and assignments (as described above) are adopted, section 9-109(c)[407] could also be revised to provide that Article 9 does not apply to the extent that state statutes regarding consumer data restrict the assignment and disclosure of consumer data by companies. Rather than simply referencing state statutes that provide "a different rule for consumers" section 9-201 could also explicitly reference state data protection and privacy statutes and clearly provide that Article 9 must always defer to any state statute that restricts an assignment or transfer of rights in biometric or health-related data.[408]

The widespread use and collection of biometric and health-related data along with the development of cryptocurrencies, such as bitcoins, evidence the significant role of emerging technologies.[409] These developments war-

---

[405] *See* U.C.C. § 9-109(d) (describing transactions to which Article 9 "does not apply").

[406] *See* RUSCH & SEPINUCK, *supra* note 167, at 51 ("There are some types of transactions that create a security interest in personal property but which are not governed by Article 9 . . . . This does not mean that the property involved in such transactions cannot be used as security for an obligation; it means merely that the law governing such liens is found elsewhere.").

[407] U.C.C. § 9-109(c).

[408] *Id.* § 9-201(b)–(c).

[409] *See* Chelsea Deppert, *Bitcoin and Bankruptcy: Putting the Bits Together*, 32 EMORY BANKR. DEV. J. 123, 137 (2015) (discussing bitcoins as general intangibles under Article 9); Jeanne L. Schroeder, *Bitcoin and the Uniform Commercial Code*, U. MIAMI BUS. L. REV., Spring 2016, at 1, 1 (contending that "[i]f held directly by the owner, bitcoin constitutes a 'general intangible'" and because "general intangibles are non-negotiable . . . . [t]his could greatly impinge on bitcoin's liquidity and, therefore, its utility as a payment system"); George K. Fogg, *The UCC and Bitcoins: Solution to Existing Fatal Flaw*, BLOOMBERG: BNA (Apr. 1, 2015), https://www.bna.com/ucc-bitcoins-solution-n17179924871/ [https://perma.cc/FRZ4-8JQ9] (describing bitcoins as general intangibles rather than "'money' as defined by the UCC"). *See generally* Stephen McJohn & Ian McJohn, *The Commercial Law of Bitcoin and Blockchain Transactions*, 47 UCC L.J. 187

rant changes in the definition of general intangibles in Article 9 and a new category of collateral, or at the very least, discourse about the transfer and assignment of rights in the new types of IoT-generated consumer data. The definition of "general intangible" in section 9-102(a)(42)[410] can be revised to exclude consumer data held by companies.

As previously noted, a separate and new definition of this type of asset could be included in section 9-102. Consumer data could be defined as all information or data concerning consumers and intellectual property rights associated with such data regardless of what medium is used to store or obtain the information. Alternatively, the definition of consumer data could be limited to cover only biometric and health-related data and associated rights. Such a limited definition offers a way to preserve the value of IoT data as a source of financing for companies while simultaneously protecting consumers' privacy by preventing an Article 9 assignment by companies of their most sensitive data (biometric and health-related data). Consumer data could also be generally defined as data that could reasonably lead to the identification of a consumer, and companies could be required to de-identify or anonymize consumer data before using it for secured credit purposes. However, as previously mentioned, anonymized data can be de-anonymized.[411] Thus, a definition that relies primarily on anonymization is not the best approach.

Section 9-203, which provides rules regarding the attachment of a security interest, could be amended to provide that if a security interest is granted in general intangibles consisting of consumer data or intellectual property rights associated with such data, the security interest would not extend to health-related or biometric data held by non-consumer persons.[412] Admittedly, this proposal may create tensions between Article 9 and intellectual property law. As state law, the UCC does not apply to the extent that it is preempted.[413] The dangers associated with the disclosure of these types of IoT data justify potential restrictions on the transfer of intellectual property rights related to the data, to the extent that such data or a database containing the data qualifies for intellectual property protection as discussed in Part II.B.[414]

(2017) (questioning "whether Article 9 should be made more flexible in order to account for bitcoin financing and blockchain transactions").

[410] *See* U.C.C. § 9-102(a)(42) (AM. LAW INST. & UNIF. LAW COMM'N 2017) (defining general intangible).

[411] See *supra* notes 119–123, 197–200 and accompanying text.

[412] *See* U.C.C. § 9-203 (describing the requirements for the attachment of a security interest).

[413] *Id.* at § 9-109(c)(1) ("This article does not apply to the extent that: (1) a statute, regulation, or treaty of the United States preempts this article."); *see also* U.S. CONST. art. VI, cl. 2 ("This Constitution, and the laws of the United States . . . shall be the supreme law of the land . . . .").

[414] *See supra* notes 242–249 and accompanying text.

One could contend that perhaps consumers should be viewed as giving only a license (rather than "ownership") to a company to use their data for purposes of allowing the consumer to enjoy all aspects of IoT products and services. Such a license could expire upon the decommissioning of the service or device, or when the consumer elects to terminate their relationship with the company. Companies could also simply be viewed as stewards or custodians of consumer IoT data.[415] However, as noted in Part II.B, under Article 9 a company need not own collateral in order to transfer rights in the personal property.[416]

The provisions of Article 9 authorizing the secured party to accept the collateral in full or partial satisfaction of the debtor's obligations, sell the collateral, or seek judicial intervention to obtain the collateral, could be revised to provide that in no event will these enforcement rights extend to biometric or health-related data, those portions of the customer database containing health-related or biometric data, or intellectual property rights related to such data. Article 9 could also be amended to obligate the debtor to use effective procedures to destroy the health-related and biometric data prior to transferring the database to the secured party in the event of default. To give effect to these proposals, a comprehensive revision of many of the provisions in Part 6 of Article 9 would be needed. These provisions may include, but are not limited to, sections 9-601 (establishing secured parties' "rights after default"), 9-602 ("waiver and variance of rights and duties"), 9-610 ("disposition of collateral after default"), 9-617 ("rights of transferee of collateral"), and 9-620 ("acceptance of collateral in full or partial satisfaction of obligation").[417]

Additionally, debtors could be required to ensure that consumer data are not disclosed to the secured party during audits of the collateral, or during the due diligence process.

Recall that Article 9 also contains various rules that attempt to limit the effect of contractual and legal anti-assignment provisions.[418] For instance, section 9-408(a) and (c) generally provide that if a provision in a contract that relates to a general intangible "prohibits, restricts, or requires the consent of . . . the account debtor to, the assignment or transfer of or creation, attachment or perfection of a security interest,"[419] or if a "rule of law, statute, or regulation that prohibits, restricts, or requires the consent of . . . [an]

---

[415] *See generally* DE MOOY & YUEN, *supra* note 382 (discussing "data stewardship" and wearable devices).

[416] *See supra* notes 242–249 and accompanying text.

[417] *See* U.C.C. §§ 9-601, 9-602, 9-610, 9-617, 9-620 (AM. LAW INST. & UNIF. LAW COMM'N 2017).

[418] *See generally id.* §§ 9-406 to -409.

[419] *Id.* § 9-408(a).

account debtor to the assignment or transfer of, or creation of a security interest,"[420] such contract terms or legal rules are "ineffective to the extent that [they] would impair the creation, attachment, or perfection of a security interest" or would qualify as an event of default.[421] The official comments to section 9-408 suggest that subsections 9-408(a) and (c) are intended to increase debtors' abilities to acquire financing.[422] Additionally, even though 9-408(a) invalidates contract provisions that would "prohibit, restrict or require consent to an assignment," it does not render ineffective all contract terms that may impact assignment, such as non-disclosure provisions.[423]

Section 9-408(d) then goes on to insulate "the account debtor on a general intangible" from the impact of the creation of a security interest by restricting the ability of the secured party to enforce its interest.[424] The comments provide that section 9-408(d) is intended to protect the account debtor "from adverse effects arising from the security interest" and "[i]t leaves the account debtor's or obligated person's rights and obligations unaffected in all material respects if a restriction rendered ineffective by subsection (a) or (c) would be effective under law other than Article 9."[425]

The official comments to 9-408 then offer the example of an anti-assignment provision in a software licensing agreement that restricts the

---

[420] *Id.* § 9-408(c).

[421] *Id.* § 9-408(a), (c); Neil B. Cohen & William H. Henning, *Freedom of Contract vs. Free Alienability: An Old Struggle Emerges in a New Context*, 46 GONZ. L. REV. 353, 371 (2010) ("Although section 9-408(c) overrides legal transfer restrictions . . . it does so only to the extent necessary to permit the creation, attachment, and perfection of a security interest."); Lipson, *supra* note 173, at 1127 ("Rev. § 9-408(a) and (c) permit a security interest to attach notwithstanding contractual or legal provisions to the contrary."); Juliet M. Moringiello, *Seizing Domain Names to Enforce Judgments: Looking Back to Look to the Future*, 72 U. CIN. L. REV. 95, 127 (2003) ("Under Revised Article 9, all legal and contractual restrictions on the assignment of . . . general intangibles are rendered invalid at least to the extent that such restrictions hinder a debtor's ability to grant a security interest in the right.").

[422] U.C.C. § 9-408 cmt. 2 (AM. LAW INST. & UNIF. LAW COMM'N 2017) ("This enhances the ability of certain debtors to obtain credit.").

[423] *Id.* § 9-408 cmt. 6. Some scholars suggest that some states have made non-uniform amendments to the anti-assignment provisions of Article 9 to make them inapplicable in certain instances. Cohen & Henning, *supra* note 421, at 370 ("[A] few states, notably Delaware, adopted nonuniform provisions excluding assignments of interests in partnerships and LLCs from the scope of sections 9-406 and 9-408.").

[424] U.C.C. § 9-408(d); *see also* Raymond T. Nimmer, *Revised Article 9 and Intellectual Property Asset Financing*, 53 ME. L. REV. 287, 353 (2001) ("[S]ection 9-408[d] sets out six express limits on its rule and what the creditor can do with the interest it can create despite contrary contract or legal terms. These include that the interest created in the licensee's interest: is not enforceable against the licensor; does not impose duties or obligations on the licensor; does not require that the licensor render any performance to the lender; does not entitle the lender to use or assign the licensee's rights; does not entitle the secured party to use, assign, possess, or have access to any trade secrets or confidential material; and does not entitle the secured party to enforce the security interest.").

[425] U.C.C § 9-408 cmt. 2.

licensee's ability to assign any of its software related rights and authorizes the licensor to terminate the contract if an assignment is attempted.[426] Under section 9-408, the anti-assignment provision is "ineffective to prevent the creation, attachment, or perfection of the security interest or entitle the licensor to terminate the license agreement."[427] Thus, the licensee could grant a lender a security interest in its rights under the agreement. However, pursuant to section 9-408(d), the lender cannot enforce its interest without the licensor's agreement, but the licensor is not obligated to acknowledge the interest of the lender in the collateral.[428]

Reading these rules together, what section 9-408(a) and (c) give to secured parties, section 9-408(d) seemingly takes away. The value of the security interest to the secured party decreases significantly under the operation of 9-408(d).[429] However, as one commentator has suggested, "the protections of 9-408(d) [may] be illusory."[430] The official comments to section 9-408 indicate that a "secured party may ascribe value to the collateral," even though it may not enforce its security interest without the account debtor's consent.[431] This is likely to occur when the secured lender believes either that it may acquire the agreement at some later date or if it believes that the collateral may generate other proceeds.[432]

Given these rules that may negate the effectiveness of contractual agreements (for instance a privacy policy provision that requires consumer consent to the creation of a security interest), and legal rules or statutes that limit the creation of security interests, one could contend that these provisions should also be amended to clearly provide that in no event will such provisions apply to statutes or rules aimed at protecting consumer data, and when consumer data are at issue such provisions will defer to the other sections of Article 9, such as the proposed amendments to 9-109, 9-203 and Part 6 of Article 9 as discussed above.[433] Such an amendment may be nec-

---

[426] *Id.*

[427] *Id.*

[428] *Id.*

[429] Cohen & Henning, *supra* note 421, at 367.

[430] D. Fenton Adams, *Sales of Personal Property as Secured Transactions Under Article 9 of the Uniform Commercial Code*, 31 U. ARK. LITTLE ROCK L. REV. 1, 100 (2008) (suggesting that despite section 9-408(d) limitations on secured parties "there may be further advantages for the secured party in the event that the assignor goes into bankruptcy"); Lipson, *supra* note 173, at 1127 (describing the potential use and impact of "hell or high-water clauses" in software licensing agreements which "require the licensee to satisfy its obligations under the contract, notwithstanding its claims or defenses").

[431] U.C.C. § 9-408 cmt. 8 (AM. LAW INST. & UNIF. LAW COMM'N 2017).

[432] *Id.*

[433] *See supra* notes 405–407 and accompanying text (proposing amendments to section 9-109); *supra* note 412 and accompanying text (proposing amendments to section 9-203); *supra* note 417 and accompanying text (proposing amendments to Part 6 of Article 9).

essary if consumer data are not carved out of the definition of general intangibles.

Prior to the implementation of any amendments to the anti-assignment provisions, careful consideration must be given to the following concerns. Section 9-408's anti-assignment provisions seemingly apply to agreements between debtors and account debtors with respect to "certain general intangibles."[434] It is not entirely clear whether a consumer would qualify as an account debtor under Article 9 in a transaction in which the consumer simply provides data that can be collected and used by a company.[435] To the extent that consumers do not qualify as account debtors then amendments to the anti-assignment provisions may be unnecessary. Additionally, scholars have contended that "whether Article 9 will override another statute that restricts assignment is somewhat questionable" given conflicting case law on this issue.[436] In light of this lack of clarity, careful attention must be paid to the interaction between contractual provisions, state statutes restricting the transfer or assignment of rights in consumer data, and the anti-assignment provisions of Article 9. These ambiguities must be resolved to ensure that consumers' interests are adequately protected.

3. Bankruptcy Code Amendments

A similar approach could also be taken under the Bankruptcy Code. If a company files for bankruptcy and its assets include consumer health-related or biometric data, the company could be prohibited from transferring and disclosing this data. The Bankruptcy Code could expressly require the debtor to destroy the biometric and health-related data before the sale or transfer of the customer database to a third party, while retaining CPOs' abilities to provide recommendations with respect to other types of consumer data.[437] Various provisions of the Bankruptcy Code would need to be re-

---

[434] U.C.C. § 9-408; *id.* § 9-408 cmt. 4 ("Subsection (a) does not render ineffective any term, and subsection (c) does not render ineffective any law, statute or regulation, that restricts outright sales of general intangibles other than payment intangibles. They deal only with restrictions on security interests."); *id.* § 9-408(a) cmt. 6 ("Subsections (a) and (c) affect two classes of persons. These subsections affect account debtors on generable intangibles and healthcare insurance receivables and persons obligated on promissory notes."); Draft for Public Comment, Permanent Editorial Bd., U.C.C., Application of UCC Sections 9-406 and 9-408 to Transfers of Interests in Unincorporated Business Organizations (Feb. 1, 2012) (on file with Gonzaga University) (stating that "[b]oth § 9-406 and § 9-408 express their overrides with regard to certain transfer restrictions for the benefit of the 'account debtor'").

[435] U.C.C. § 9-102(a)(3) (defining "account debtor" as a "person obligated on an account, chattel paper, or general intangible . . . .").

[436] RUSCH & SEPINUCK, *supra* note 167, at 187 (discussing conflicting case law evaluating state statutes restricting the assignment of state lottery winnings).

[437] It should be noted that the Bankruptcy Code also contains various provisions applicable to healthcare records and a "health care business" that files for bankruptcy. 11 U.S.C. § 333 (2012)

vised to restrict the transfer of such data and give effect to the proposal discussed in this Article. In implementing such amendments, consideration must be given to bankruptcy law's reliance on state law, the current provisions of the BAPCPA discussed in Part III.A (sections 332 and 363), and the provisions of the Bankruptcy Code (i) defining the debtor's estate and "personally identifiable information," and (ii) limiting attempts to prevent property from becoming part of the debtor's estate.[438]

4. Criticisms of Transfer & Assignment Restrictions

a. Shift from Financing to Selling

If transfer and assignment constraints are imposed in the Article 9 context, companies may avoid using their data assets (which may include biometric and health-related data) for Article 9 transactions and instead resort to directly selling consumer-related data to third parties to obtain funding. Thus, transfer and assignment restrictions could amplify companies' use of other data monetization methods, thereby rendering any such restrictions ineffective. As previously mentioned, this Article does not suggest that Article 9 assignment restrictions will remedy all concerns associated with data monetizations. Instead, it argues that the moments of data disclosures permitted under Article 9 could be decreased through the imposition of specific restrictions. Further, this Article calls for the simultaneous use of different data protection models to protect consumers in various settings. Concerns associated with other types of monetizations, such as direct sales of consumer data, could be remedied by adopting restrictions in the non-Article 9 context. For instance, recall that the Illinois biometric data statute forbids companies from selling biometric data. Similar legislation could be adopted in other states.

("[a]ppointment of patient care ombudsman"); *id.* § 351 ("disposal of patient records"); *id.* § 101(27A) (generally defining "health care business[es]" as entities that mainly provide health care related services, such as "the diagnosis or treatment of injury, deformity, or disease"). It is unlikely that IoT companies will qualify as "health care businesses" under the Code. IoT health-related data may not meet the definition of "patient records," which also relies on the collection of data by a "health care business." *Id.* § 101(40A)–(40B) ("The term 'patient' means any individual who obtains or receives services from a health care business" and "[t]he term 'patient records' means any record relating to a patient, including a written document or a record recorded in a magnetic, optical, or other form of electronic medium.").

[438] *See* 11 U.S.C. § 101(41A) (defining "personally identifiable information"); *id.* § 541 (2012 & Supp. II 2014) (defining debtor's estate); *id.* § 541(c) (limiting the effect of contractual agreements and non-bankruptcy law that attempt to prevent property from becoming part of the debtor's estate); John K. Eason, *Retirement Security Through Asset Protection: The Evolution of Wealth, Privilege, and Policy*, 61 WASH. & LEE L. REV. 159, 206 (2004) ("[T]he Code ignores anti-alienation provisions and requires the court to bring the affected interest into the bankruptcy estate for application in satisfaction of creditor claims."); Miller & O'Rourke, *supra* note 36, at 789 (noting that the "Code leaves the definition of 'property' to other state or federal law"); *supra* notes 263–311 and accompanying text.

b. Practical Concerns

Another critique of the restriction on transfers and assignments approach is that it may be difficult for IoT companies to separate biometric and health-related data from other personally identifiable or non-identifiable consumer information. To ameliorate this concern, companies could consistently encrypt biometric and health-related data, store these data apart from other types of consumer data in separate databases and servers upon collection, and develop new ways to ensure that the data are kept secure.

c. Innovation and Costs

Other criticisms include that transfer and assignment restrictions may have a negative impact on innovation, do serious harm to the viability of IoT companies that specialize in producing devices that collect IoT data, and increase the price of IoT products. Following this line of reasoning, certain IoT companies may produce IoT devices that collect and rely mainly on health-related or biometric data. Thus, preventing these companies from using such data for secured transactions purposes or in bankruptcy proceedings will have a significant impact on their ability to obtain financing or transfer substantially all of their assets if they experience financial difficulties.

One response to these critiques is that customer databases can still be valuable assets to companies without the inclusion of biometric or health-related data. For instance, RadioShack sold its customer database and other assets for $26.2 million even though significant pieces of consumer information were not transferred as part of the sale.[439] Thus, requiring the removal of health-related or biometric data prior to the sale or disclosure of other types of consumer data does not completely eradicate the value of the asset.

One could also contend that allowing biometric and health-related data to be sold to third parties as part of an Article 9 or bankruptcy sale or other business transition is beneficial to consumers, particularly when data are transferred to a third party that will continue to operate the debtor's business or is in the same line of business as the debtor. In such an instance, the transfer of the data may allow the device to continue to function and prevent service interruptions that may impact the consumer. However, to the extent that this information is transferred to a third party during bankruptcy or to a secured party in the same line of business, these companies should

[439] *See* Hiltzik, *supra* note 34 (discussing how RadioShack's "hoard of customers' personally identifiable information" was sold for $26.2 million); Isidore, *supra note* 33 ("RadioShack struck a deal with a coalition of 38 state attorneys general to destroy most of RadioShack's consumer data, and stipulated that no credit or debit card account numbers, social security numbers, dates of birth or even phone numbers would be transferred.").

be prohibited from further monetizing and assigning the data and should only be permitted to use the data to the extent necessary for the device to function and to meet consumer needs.

Moreover, even if transfer restrictions may impact the price and operations of IoT devices and services, the potential dangers of continually disclosing and transferring highly sensitive consumer data from party to party, server to server, and network to network justify the imposition of transfer and assignment constraints. Consider that in 2015 the U.S. Office of Personnel Management ("OPM") announced that the fingerprint data of approximately 5.6 million individuals were stolen when the agency's systems were hacked.[440] Given the generally immutable nature of fingerprints, individuals impacted by the breach "may find themselves grappling with the fallout for years."[441] Consumers may ultimately have to forego some of the convenience obtained from the use of IoT devices and services in order for their privacy concerns to be effectively addressed. If the OPM cannot keep the fingerprint scans of millions of citizens secure, should IoT companies, including small start-ups, be permitted to freely collect, transfer, and use biometric data simply because consumers were provided with notice of the terms of a privacy policy and given an artificial choice? Databases and servers that are rich with highly sensitive data, including biometric and health-related data, are attractive targets for foreign and domestic hackers. Companies' unrestricted collection, disclosure, or use of biometric or health related data may also implicate national security concerns as evidenced by recent reports of a health-tracking mobile application that "exposed the location of [secret] military bases."[442] Consumers may be better served if companies are discouraged from routinely collecting or disclosing biometrics and health-related data in connection with IoT devices and services, and limitations are placed on companies' ability to transfer, use, and disclose such data.

---

[440] Andrea Peterson, *OPM Says 5.6 Million Fingerprints Stolen in Cyberattack, Five Times as Many as Previously Thought*, WASH. POST (Sept. 23, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/ [https://perma.cc/NY3M-Q988].

[441] *Id.*

[442] Ryan B. Browne, *The App That Exposed the Location of Military Bases with a Heat Map Is Reviewing Its Features*, CNBC (Jan. 30, 2018, 6:33 AM), https://www.cnbc.com/2018/01/30/strava-reviewing-features-after-military-bases-were-found-on-heat-map.html [https://perma.cc/5ZBR-BSW3]; Matt Burgess, *Strava's Data Lets Anyone See the Names (and Heart Rates) of People Exercising on Military Bases*, WIRED (Jan. 30, 2018), http://www.wired.co.uk/article/strava-military-bases-area-51-map-afghanistan-gchq-military [https://perma.cc/E8PN-U325] (discussing the Strava app's disclosure of user's heart rates and military base locations).

d. Competition Concerns

Restricting the flow of data to third parties may also implicate concerns related to competition. One commentator suggests that control of consumer data rests with a "handful of dominant players" and "with little competition to worry about, they are likely to keep collecting more and more data; effectively creating a status quo or glass ceiling that cannot be breached."[443] The Economist magazine also notes that data "titans," such as Apple, Google, and Facebook, dominate the big data industry.[444] This market domination may create insurmountable hurdles for small businesses and start-ups whose business models rely on the collection of consumer data.[445] Following that line of reasoning, one could contend that prohibitions on the disclosure and sale of consumer data to third parties exacerbates this problem.

One response to this critique is that although large companies may have vast quantities of consumer data and significant influence, the privacy and security concerns posed by data collection and disclosure in the IoT setting outweigh these matters, or at the very least, justify restrictions on the sale and assignment of certain types of consumer data. Additionally, over the last few years there has been a consistent stream of new start-up companies entering the IoT market despite the dominant role of large Internet companies. This suggests that assignment and transfer restrictions may not necessarily prevent start-up companies from successfully entering the IoT market. A detailed evaluation of the long-term viability of such new companies in light of the perceived dominance of large "data titans" must await further consideration.

e. Alternative Notice and Choice Methods

Despite many privacy law scholars' notable criticisms of the notice and choice model, at least one scholar has suggested that "emerging strategies of 'visceral' notice [that] leverage a consumer's very experience of a product or service to warn or inform . . . [are] worthy of further study before we give in to calls to abandon notice as a regulatory strategy in privacy and

---

[443] Kees Jan Kuilwijk, *Big Data, the Internet of Things and Competition Law*, LINKEDIN (June 7, 2016), https://www.linkedin.com/pulse/big-data-internet-things-competition-law-kees-jan-kuilwijk [https://perma.cc/5AYH-4GYA].

[444] *The World's Most Valuable Resource Is No Longer Oil, but Data*, THE ECONOMIST (May 6, 2017), http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource [https://web.archive.org/web/20180104231109/http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource].

[445] Kuilwijk, *supra* note 443.

elsewhere."[446] Thus, one could contend that rather than imposing explicit transfer and assignment restrictions, alternative and improved notice techniques, such as concise privacy policies, privacy icons, and "notice that rel[ies] on consumer experience rather than entirely on words or symbols," could sufficiently protect consumers.[447]

A potential response to this critique is that consumers may continue to ignore privacy notices regardless of their length or form. Several studies suggest that the use of shorter policies, tables, or icons to provide privacy notices do not significantly avoid the pitfalls of traditional privacy policies.[448] Additionally, although in some settings there may be some advantages to using visceral privacy notices when compared to standard privacy policies, there are limits to the effectiveness of visceral notice.[449] For instance, visceral no-

---

[446] M. Ryan Calo, *Against Notice Skepticism in Privacy (And Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1027 (2012) [hereinafter Calo, *Notice Skepticism*].

[447] *Id.* at 1047; FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURE: BUILDING TRUST THROUGH TRANSPARENCY 17 (2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf [https://perma.cc/3EEX-GR3B] ("Icons, if appropriately designed and implemented, offer the ability to communicate key terms and concepts in a clear and easily digestible manner.").

[448] *See, e.g.*, Calo, *Notice Skepticism*, *supra* note 446, at 1033 ("Studies show only marginal improvement in consumer understanding where privacy policies get expressed as tables, icons, or labels, assuming the consumer even reads them."); Mike Hintze, *In Defense of the Long Privacy Statement*, 76 MD. L. REV. 1044, 1044 (2017) (contending that "short-form approaches" to providing notice of privacy policies, such as "standardized short-form notices" and icons "inevitably leave out important details, gloss over critical nuances, and simplify technical information in a way that dramatically reduces transparency and accountability"); Aleecia Mcdonald et al., *A Comparative Study of Online Privacy Policies and Formats*, *in* PRIVACY ENHANCING TECHNOLOGIES 37, 38 (Ian Goldberg & Mikhail Atallah eds., 2009) (a study finding inadequacies in various privacy notice formats and contending that "translating an entire privacy policy into a grid that conveyed information by icons and colors did not improve comprehension"); Lauren E. Willis, *Why Not Privacy by Default?*, 29 BERKELEY TECH. L.J. 61, 127 (2014) (discussing the ineffectiveness of a "behavioral advertising privacy icon" and contending that "[t]his simple, universal, and widely-used icon leads to an explanation of how to opt out of receiving behavioral advertising, but although most consumers have received advertising with this icon attached, very few consumers know what the icon means, and even fewer have clicked on it"); Joshua Gluck et al., *How Short Is Too Short? Implications of Length and Framing on the Effectives of Privacy Notices*, USENIX ASS'N 321 (2016), https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-gluck.pdf [https://perma.cc/V683-WF67] (finding that although "short-form privacy notices can inform users about privacy practices . . . removing expected privacy practices from notices sometimes led to less awareness of those practices, without improving awareness of the practices that remained in the shorter notices"); PEDRO GIOVANNI LEON ET AL., CARNEGIE MELLON U. CYLAB, WHAT DO ONLINE BEHAVIORAL ADVERTISING PRIVACY DISCLOSURES COMMUNICATE TO USERS? (Apr. 2, 2012), https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12008.pdf [https://perma.cc/AG6Y-LU3J] (finding that consumers continued to misunderstand the purpose and implications of privacy "icons and taglines").

[449] Shara Monteleone, *Addressing the "Failure" of Informed Consent in Online Data Protection: Learning the Lessons from Behaviour-Aware Regulation*, 43 SYRACUSE J. INT'L L. & COM. 69, 111 (2015) (discussing studies on visceral notices and contending that "a relevant finding of these

tice (as well as other traditional forms of privacy notice) may not eliminate the negative consumer consequences associated with use of "big data," such as discrimination.[450] Moreover, as one scholar has noted,

> privacy warnings are more difficult to translate into visceral terms because the consequences are much more abstract . . . [and] improved notice, whether simplified or more visceral . . . neglect a fundamental dilemma of notice: making it simple and easy to understand conflicts with fully informing people about the consequences of giving up data, which are quite complex if explained in sufficient detail to be meaningful.[451]

Thus, in the privacy setting, visceral notice is unlikely to be "a panacea to protect privacy."[452] As a result, alternative and complementary consumer protection methods, such as transfer and assignment restrictions, are still needed. To be clear, this Article does not contend that companies should no longer provide consumers with any form of privacy notice. Rather, it highlights the limits of depending excessively on the notice and choice model and privacy policies to safeguard consumers, and ultimately argues for the implementation of solutions to ameliorate the impact of, and correct, this overreliance.

Lastly, one could posit that IoT voice controlled "two-way" speaker devices, such as the Amazon Echo, could provide consumers with key summaries of privacy policies and conditions of use. However, it is unclear whether

---

studies is that a visceral notice represented by an informal interface ('informal condition') to be employed, for instance, in children's websites, prove to reduce privacy concerns, but also to increase data disclosure by users, making the informal design problematic for data protection and privacy policy"); Barbara Sandfuchs & Andereas Kapsner, *Coercing Online Privacy*, 12 I/S: J.L. & POL'Y FOR INFO. SOC'Y 185, 200 n.65 (2016) (describing Calo's visceral notice approach as "a nudge rather than a notice"); Yang Wang et al., *A Field Trial of Privacy Nudges for Facebook*, *in* PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 2367 *passim* (2014), http://repository.cmu.edu/cgi/viewcontent.cgi?article=1341&context=heinzworks [https://perma.cc/FP58-4SVD] (evaluating the advantages and disadvantages of "privacy nudges"); Victoria Groom & M. Ryan Calo, Reversing the Privacy Paradox: An Experimental Study (Sept. 25, 2011) (unpublished manuscript) (on file with authors) (finding that "visceral notice strategies prove more effective at modulating consumer privacy concern than traditional notice in certain instances" but noting concerns with "informal websites").

[450] Philip Hacker & Bilyana Petkova, *Reining in the Big Promise of Big Data: Transparency, Inequality, and New Regulatory Frontiers*, 15 NW. J. TECH. & INTELL. PROP. 1, 5–6 (2017) (contending that although "proposed smart disclosure policies such as 'visceral notice' can help consumers make better-informed choices about services powered by data . . . transparency [cannot] work on its own to combat troublesome discriminatory uses of Big Data [and therefore] regulatory strategies that couple transparency with some substantive protections" are needed).

[451] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1885 (2013).

[452] Monteleone, *supra* note 449, at 116–17 (contending that visceral notice alone cannot correct all privacy related problems and advocating for the use of other "coercive measures").

privacy notices provided via an interactive IoT device will truly improve consumer understanding of the implications of consenting to a company's privacy policy. Further, even if such notice improves some consumers' understanding of privacy policies it does nothing to impact companies' subsequent, use, disclosure and transfer of consumer data once consumers consent to the policy. Stated differently, IoT personal assistants could inform consumers that their data could be transferred to third parties in the event of bankruptcy or a sale of the company or its assets, yet the result for consumers is potentially the same: the company continues to be the primary arbiter of how and when consumer data is used and disclosed, and once the consumer consents to the company's privacy policy after receiving notice through the IoT device, their data can continue to be transferred and disclosed through the financial frameworks of Article 9 and the Bankruptcy Code. Thus, the potential effectiveness of relying solely or primarily on alternative notice and choice techniques to safeguard consumers is questionable.

B. Require CPOs in Article 9 Foreclosures

Article 9's scope, attachment, and other provisions discussed in Part IV.A above could remain as they are to alleviate concerns related to the ability of IoT companies that rely primarily on health-related and biometric data to obtain financing.[453] Instead, Part 6 of Article 9 could be amended to explicitly provide that when a customer database containing consumer information is subject to a secured party's security interest, judicial intervention is the only method by which the secured party can obtain and dispose of the collateral.

Article 9 could be revised to provide that a CPO must be appointed to provide guidance to the court in deciding whether to issue an order requiring the debtor to provide the collateral (customer data) to the secured party. CPOs could: (1) consider whether the debtor's privacy policy permits a sale upon an event of default under a security agreement, (2) recommend that the secured party be prohibited from selling the data in a piecemeal manner to buyers so that the data cannot be disassociated from the business, (3) recommend that the secured party be permitted to operate the debtor's business as a "going concern,"[454] and (4) to the extent that the debtor's privacy poli-

---

[453] *See supra* notes 405–436 and accompanying text.

[454] This approach could be viewed as fitting within a "downstream data protection model" which "[p]rohibits data disclosure by data custodian or limits disclosure to certain persons or for certain purposes." Terry, *Regulatory Disruption*, *supra* note 394, at 153; *see also* PARRISH & MORGAN, *supra* note 257, at 3-6 (discussing the differences between a section 363 Chapter 11 sale and sales under Chapter 7 of the Bankruptcy Code and Article 9, and contending that "for sellers, the 363 sale process provides a way for substantially all of a chapter 11 debtor's assets to

cy does not adequately protect consumer interests, determine whether the party that wants to acquire the data is willing to adopt a more consumer-friendly privacy and data protection policy that limits disclosures and transfers after data acquisition.

The major critiques of this approach are that it limits the remedies available to secured parties in the event of default, requires parties to go to court in the event of default, imposes additional costs associated with hiring and appointing a CPO, and may make such assets less attractive to lenders. Either the debtor or the secured party must bear the cost of a CPO's appointment. Additionally, as with the transfer and assignment restrictions discussed in Part IV.A, the consumer protection effect of this approach may be negated if parties elect to engage in regulatory arbitrage by structuring a transaction as a direct sale of IoT data to avoid the application of Article 9. As noted earlier, the adoption of statutes prohibiting such activities may alleviate this concern.

Despite these criticisms, the various data disclosure moments authorized by Article 9 support the imposition of restrictions on the transfer and disclosure of consumer data in the IoT context. It is clear that companies use privacy policies to authorize the monetization of consumer data, and that "notice and choice" has largely failed consumers. Thus, as noted earlier, more notice and choice (including simplified disclosures) is unlikely to be the most effective solution.[455]

The expected proliferation and widespread use of new types of IoT data about consumers, warrants movement away from an overreliance on companies' privacy policies. Further, in contrast to explicit restrictions prohibiting a transfer or assignment of rights in customer data (or databases), this solution balances the interests of debtors that would like to use IoT data as a source of credit with the concerns of consumers that may arise when Article 9's regime permits data disclosures and transfers upon foreclosure. Such a solution may be preferable for companies whose primary or most valuable asset is their customer database. As a practical matter, currently a

---

be sold as a going concern, as opposed to ceasing the business and liquidating assets pursuant to Chapter 7 of the Bankruptcy Code or Article 9 of the Uniform Commercial Code").

[455] In a leading article on the creation of security interests in customer databases prior to the rise of the IoT, one scholar offered several valuable proposals to remedy consumer privacy concerns in the non-IoT setting. Nguyen, *Collateralizing*, *supra* note 19, at 599–602. These solutions include obligating companies to disclose in their privacy policies secured transactions involving customer databases as well as provide explanations regarding the implications of assignment; requiring clear references on financing statements to customer databases; and amending Article 9 to require that the security agreement obligates the secured party to comply with the debtor's existing privacy policy. *Id.* These proposals also emphasize reliance on the terms of a company's privacy policy as the primary vehicle of protecting consumers. Further, consumers may not review or understand detailed privacy policies. Thus, the imposition of more disclosure requirements may not sufficiently protect consumer interests.

creditor likely needs judicial intervention to obtain customer lists and customer databases that are subject to a security interest and controlled by or in the possession of the debtor. Thus, if a court is likely to already be involved in connection with the secured party's exercise of its rights under the security agreement, it is advisable to appoint a CPO to aid the court in its determinations when highly-sensitive consumer data may be up for sale. Congress has already recognized the dangers associated with the transfer of non-IoT consumer data in the bankruptcy context via the adoption of the BAPCPA. These concerns are also present in the Article 9 context and are even more disquieting given the new types, quality, and quantity of IoT data that are now available to companies. Although the appointment of a CPO does not mean all concerns related to consumer data transfers and disclosures will be automatically remedied, CPOs with expertise in the bankruptcy setting may provide valuable guidance to courts during the Article 9 foreclosure process.

C. Require CPOs in All Bankruptcy Transfers

Another approach to increasing the protection of consumer data in the bankruptcy setting is to require the appointment of CPOs whenever consumer data are offered for sale or lease in a bankruptcy proceeding. Thus, even if the sale of consumer data would be permissible under the debtor's existing privacy policy, the consumer has consented to the privacy policy, if no privacy policy is provided, or if the data does not qualify as personally identifiable information, a CPO would be appointed to provide guidance to the court on whether the sale of the data should be approved.[456] This would, of course, require amendments to the Bankruptcy Code. Given the increasing prevalence of section 363 sales, sections 332 and 363 of the Bankruptcy Code (containing the existing CPO and BAPCPA provisions discussed in this Article) are the first place to begin.[457] The definition of "personally identifiable information" could also be expanded to cover any type of consumer data regardless of whether it may lead to identification, or a separate and much broader definition of consumer data could be adopted.[458] Other

[456] One could of course contend that consumer advocates are also needed in other types of proceedings that deal with assets that affect consumers. Although this may be true, the impact of IoT data as discussed in this article and the various ways that it can be disclosed and misused to the detriment of consumers in accordance with Article 9 and the Bankruptcy Code suggest that special attention should be given to IoT data as an asset.

[457] 11 U.S.C. §§ 332, 363 (2012); PARRISH & MORGAN, *supra* note 257, at 3-6 ("[T]he use of 363 sales has become common, and many bankruptcy cases are now filed for the sole purpose of completing a 363 sale."); *see supra* notes 263–311 and accompanying text.

[458] *See* 11 U.S.C. § 101(41A) (defining personally identifiable information); Narayanan & Shmatikov, *supra* note 389 (critiquing use of the term "personally identifiable information" and

provisions of the Code may also need to be amended to give effect to such a proposal.[459]

Further, in light of privacy policies that attempt to skirt the buyer limitations established by the FTC in *Toysmart* and discussed in Part II.B above, in amending these provisions of the Bankruptcy Code consideration should be given to whether these limitations adequately protect consumers and whether some or all of these limitations should be expressly included in the code.[460]

As noted in Part III.A, if the debtor's privacy policy does not sufficiently protect consumers, this inadequacy will continue even if the buyer adopts the debtor's privacy policy.[461] Thus, in deciding if a sale or lease should be approved, whether the proposed buyer of the data consents to or assumes the debtor's existing privacy policy or agrees to use the data for similar purposes as the debtor should be irrelevant when the privacy policy does not adequately protect the data of consumers. Courts and CPOs should be willing to acknowledge that in many instances consumers' interests may be better served if health-related and biometric data are not transferred to purchasers. Rather than solely seeking to extract as much value as can be obtained from the debtor's assets for the benefit of creditors, courts must actively consider the implications of the transfer of consumer data in bankruptcy proceedings and must be willing to follow CPO recommendations that sufficiently protect consumers' interests. Further, the harms that consumers may suffer from the transfer of their data to third parties in bankruptcy proceedings supersede concerns about increased costs associated with CPO appointments.

The consistent stream of bankruptcy cases since *Toysmart* involving the sale of consumer data coupled with the documented inadequacies of the

---

contending that "[t]he versatility and power of re-identification algorithms imply that terms such as "personally identifiable" and "quasi-identifier" simply have no technical meaning").

[459] The sections of the Bankruptcy Code that authorize a transfer of the debtor's assets outside of the section 363 context may also need to be addressed to the extent that customer data can be (and are frequently) transferred to third parties in non-section 363 transfers. Some commentators contend that section 332 does not require the appointment of a CPO "in the context of a sale under a Chapter 11 plan" and therefore "[section] 1123(a) of the Bankruptcy Code continues to allow a plan to provide for a transfer or sale of the debtor's property '[n]otwithstanding any otherwise applicable nonbankruptcy law.'" Levin & Marinelli, *supra* note 311, at 627; *see also* PARRISH & MORGAN, *supra* note 257, at 3-8, 3-10 ("Sales under section 363 lack many of the protections that the Bankruptcy Code provides creditors as part of the plan process" and "courts generally agree that a trustee may sell all of the estate's assets through a 363 sale, rather than by a plan of reorganization, where the trustee demonstrates, among other things, a sound 'business justification' for the sale prior to a plan confirmation."); Karam, *supra* note 257, at 403–11 (discussing the differences between section 363 sales and sales under section 1123 of the Bankruptcy Code).

[460] *See supra* notes 312–321 and accompanying text.

[461] *See supra* notes 304–307 and accompanying text.

BAPCPA discussed in this Article, as well as courts' reluctance to appoint CPOs indicate that amendments to the Bankruptcy Code are needed.

CONCLUSION

By using IoT devices and services, consumers may unwittingly trade privacy in exchange for convenience and efficiency with dire consequences. Consumer IoT data are extremely valuable to IoT companies. The IoT holds perils for consumers if it is not effectively regulated. As such, renewed discourse and debate about how to effectively protect consumer privacy and data in the IoT era, while balancing other important goals of various legal frameworks, is needed.

Bankruptcy law and Article 9 can significantly impact privacy law issues. Currently, privacy policies, Article 9, and the Bankruptcy Code permit companies to opaquely disclose and transfer consumer data to third parties. Given the exponential growth in the types and volume of data that companies will collect and retain, Article 9's secured credit framework and the Bankruptcy Code should be revised to effectively address consumer privacy concerns. These amendments could take the form of specific assignment and transfer restrictions or revisions to enforcement mechanisms. The latter solution may alleviate some concerns associated with transfer and assignment restrictions.

The privacy and security harms posed by the IoT are significant. As a result, consumer interests may be more adequately protected when restrictions are imposed on the collection, transfer, and assignment of certain types of data under commercial frameworks and in other monetization settings. Movement away from an excessive dependency on the notice and choice model and the provisions of privacy policies is long overdue.