Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 29 *XXIX*
Number 2

Article 6

2019

The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector

Elias Wright
Fordham University School of Law, ewright26@law.fordham.edu

The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector

Cover Page Footnote

J.D. Candidate, Fordham University School of Law, 2020; B.A., Religion & Art History, Oberlin College, 2014. I would like to thank Olivier Sylvain, my advisor, for his guidance and feedback throughout the writing process. Additionally, I am greatly appreciative of N. Cameron Russell, Danielle Keats Citron, and all of the scholars who visited and contributed to the Civil Rights and Civil Liberties in the Digital Age seminar, as well as Sean Corrado and the editors and staff of the IPLJ for their advice and feedback. I would like to extend a special thank you to my family and friends for patiently suffering my incessant and rambling reveries.

The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector

Elias Wright*

In recent years, advances in facial recognition technology have resulted in a rapid expansion in the prevalence of private sector biometric technologies. Facial recognition, while providing new potentials for safety and security and personalized marketing by retailers implicates complicated questions about the nature of consumer privacy and surveillance where a "collection imperative" incentivize corporate actors to accumulate increasingly massive reservoirs of consumer data. However, the law has not yet fully developed to address the unique risks to consumers through the use of this technology.

This Note examines existing regulatory mechanisms, finding that consumer sensitivities and the opaque nature of the technology have resulted in over- and underinclusive regulatory regimes. This Note proposes that the broad implications of biometric privacy harms justify more extensive privacy regulation than a narrow focus on data security and self-regulation. It suggests that regulation predicated on consumer data self-management is inefficient in controlling the flow of information generated by facial recognition.

---

* J.D. Candidate, Fordham University School of Law, 2020; B.A., Religion & Art History, Oberlin College, 2014. I would like to thank Olivier Sylvain, my advisor, for his guidance and feedback throughout the writing process. Additionally, I am greatly appreciative of N. Cameron Russell, Danielle Keats Citron, and all of the scholars who visited and contributed to the Civil Rights and Civil Liberties in the Digital Age seminar, as well as Sean Corrado and the editors and staff of the IPLJ for their advice and feedback. I would like to extend a special thank you to my family and friends for patiently suffering my incessant and rambling reveries.

This Note finds that a regulatory approach based in collaborative governance may be better suited for regulating complex systems that create hard-to-calculate risks, change too quickly for traditional regulatory approaches, and involve technical and industry expertise that regulators and legislators are unlikely to have.

INTRODUCTION

> "Well, all information looks like noise until you break the code."[1]

In Steven Spielberg's 2002 science fiction film *Minority Report*, John Anderton's face is scanned as he walks into a futuristic version of the retail store Gap.[2] A hologram personally greets him and prompts him on his recent experience with purchasing "assorted tank tops."[3] What was considered science fiction seventeen years ago now rapidly approaches reality as retailers adopt commercial applications of facial recognition technology for functions including safety and security, secure payment, marketing, and customer service.[4] While the extent of current commercial use of biometrics

---

1 NEAL STEPHENSON, SNOW CRASH 74 (1992).

2 MINORITY REPORT (20th Century Fox 2002).

3 *Id.*

4 U.S. GOV'T ACCOUNTABILITY OFF., GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 6, 38 (2015).

is not fully known, this technology presents potential benefits and risks for both retailers and consumers.[5]

Use of facial recognition technology can identify customers, preventing fraud and providing "VIP services,"[6] as well as recognizing individuals with known shoplifting convictions.[7] While the prevalence of this technology may improve the retail experience by offering convenience and individualized service, these technologies are generating and storing vast amounts of sensitive information about individuals' movements, preferences, and associations.[8] Retailers, using biometric data for the aggregation of customer profiles, are creating valuable databases that are more sensitive to the risk of breach.[9] How this data is collected, stored, used, and shared may result in negative consequences for consumers walking into public retail establishments.

Privacy advocates and scholars have flagged the expanding use of biometric data as a concerning area for consumers.[10] As biometric techniques generate and use novel forms of information, scholars emphasize that there is presently little legal oversight covering techniques of collection, storage, and usage.[11]

---

5 *Id.* at 10.

6 Brenda Salinas, *High-End Stores Use Facial Recognition Tools to Spot VIPs*, NAT'L PUB. RADIO (July 21, 2013, 6:21 AM), https://www.npr.org/sections/alltechconsidered/2013/07/21/203273764/high-end-stores-use-facial-recognition-tools-to-spot-vips [https://perma.cc/9VGP-Q755].

7 Chavie Lieber, *Your Favorite Store Could Be Tracking You with Facial Recognition*, RACKED (May 22, 2018, 4:00 PM), https://www.racked.com/2018/5/22/17380410/facial-recognition-technology-retail [https://perma.cc/FL4Q-CNUL].

8 Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1127-28, 1131 (2015).

9 John Tengberg, *Inter-Organizational Information Sharing of Customer Data in Retail* 4, 7–9, 22–23 (Composite Info. Sys. Lab., Working Paper No. 2013-09), http://web.mit.edu/smadnick/www/wp/2013-09.pdf [https://perma.cc/3P4Y-QX3P].

10 *See, e.g.*, Woodrow Hartzog & Evan Selinger, *Facial Recognition Is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66 [https://perma.cc/47AP-JAXB].

11 *See, e.g.*, 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, 250–51, 255 (2007); Jenna Bitar & Jay Stanley, *Are Stores You Shop at Secretly Using Facial Recognition on You?*, ACLU (Mar. 26, 2018, 4:18 PM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/are-stores-you-shop-secretly-using-face [https://perma.cc/HL5L-V7GV].

This Note examines the way in which existing institutional structures and consumer anxieties have resulted in over- and underinclusive regulatory regimes when confronted with an emerging technology form. The failures and successes expose which measures in law and policy may best protect consumers from the collection and use of biometric information by commercial non-governmental actors in retail settings.

Part I of this Note describes the history, technological background, and unique privacy risks of surveillance from biometric facial recognition technologies. It outlines the development of private sector uses of facial recognition in brick-and-mortar retail settings. This Part then demonstrates the tension between consumer privacy sensitivities and the emerging utility of facial biometric data to retailors for structuring consumer demographics, habit, and preference data into a machine-readable format when collected from existing closed-circuit television cameras.

Part II explores current laws that protect consumer biometric data. This Part then discusses how current laws have been utilized to protect consumer privacy, alongside alternate regulatory enforcement mechanisms that could be used where an act or practice causes or is likely to cause substantial injury to consumers that is not reasonably avoidable by consumers, nor outweighed by countervailing benefits to consumers or to competition.

Part III considers the availability and shortcomings of current regulatory approaches for emerging facial recognition technologies. This Part examines the potential of an individual rights regime, using the example of Illinois' BIPA as a model of this approach. Part III then considers the FTC's managerial regime, in which a regulatory "light touch" serves as a backstop to industry self-regulation. Finally, this Part evaluates problems of the present incentive structures and market failures of self-regulatory regimes that may impede the development of an effective collaborative governance regime.

The final section, Part IV, considers that the incentive structures of the present regulatory regimes, emphasizing consumer data self-management and market self-correction, are inadequate in addressing the unique issues of facial recognition. This Part suggests

that the FTC's "light touch" approach alone is unlikely to develop enforceable norms and standards. However, this Part suggests that FTC's role as a "norm entrepreneur" makes it ideally situated to engage in collaborative governance process, which has the potential for meaningful regulation.

I. BACKGROUND: PRIVACY IN A LANDSCAPE OF PRIVATE BIOMETRIC SURVEILLANCE TECHNOLOGIES

In recent years, the rapid expansion in prevalence of private sector biometric technologies implicates complicated questions about the nature of consumer privacy and surveillance. As retailers target individual consumers and define them through classification systems according to a hierarchy of value, they subject consumers to new risks and potentials.[12] This Note considers how these potential harms should be conceptualized and what type of remedies best address and moderate consumer risks.

Section I.A traces the sociohistorical development of biometrics and then discusses the technological basis and relevant uses and risks of biometrics in the private-sector. Section I.B describes the specific risks inherent to the collection, aggregation, and profile creation using biometric data. Section I.C describes the present applications of biometrics in retail and unique issues with facial recognition databases.

A. The Current Technological Context

Biometric identifiers allow private-sector users to monitor individuals within a constrained space, noninvasively, from a distance, and without the consumer's knowledge. The incorporation of biometrics, such as facial recognition, into existing closed-circuit television (CCTV) devices, provides an additional layer of data to private surveillance technologies. This biometric overlay allows private-sector users to conduct a more comprehensive analysis of individuals within retail environments, linking new inputs to already existing reservoirs of data, such as past purchases, interests,

---

[12] *See* JOSEPH TUROW, THE AISLES HAVE EYES: HOW RETAILERS TRACK YOUR SHOPPING, STRIP YOUR PRIVACY, AND DEFINE YOUR POWER 194 (2017).

immediate family members, or criminal records, collected by the retailer or purchased from data aggregators.[13]

1. A Brief Sociotechnical History of Biometrics

The conceptual underpinnings of identifying individuals using biometric markers emerged with the development of the new communications technologies in the nineteenth century, such as telegraphy, photography, and telephony.[14] Visual reproduction technologies were developed that could analyze, classify, and identify the structure of human faces.[15] New photography technologies transformed social perceptions of identity and privacy.[16] The nineteenth-century pseudoscience of physiognomy believed, for example, that people's faces bore the signs of their essential qualities and could be visually analyzed as a means of measuring their moral worth.[17]

With the development of computerization, facial recognition in the United States was developed as a public-private venture, funded and shaped to military priorities.[18] From the 1960s through the 1990s automated facial recognition research was primarily funded through the Defense Advanced Research Projects Agency (DARPA).[19] The goal of automated facial recognition was assisting the military to identify, at a distance, specific individuals among

---

13 *See id.* at 109.

14 KELLY A. GATES, OUR BIOMETRIC FUTURE: FACIAL RECOGNITION TECHNOLOGY AND THE CULTURE OF SURVEILLANCE 12, 18–19 (2011).

15 *Id.*

16 *See* ARI EZRA WALDMAN, PRIVACY AS TRUST 15–16 (2018) (discussing the advent of the Kodak instantaneous camera as a basis for Samael Warren & Louis Brandeis' *Right to Privacy*); Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) ("Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life.").

17 Blaise Agüera y Arcas, Margaret Mitchell & Alexander Todorov, *Physiognomy's New Clothes*, MEDIUM (May 6, 2017), https://medium.com/@blaisea/physiognomys-new-clothes-f2d4b59fdd6a [https://perma.cc/6CJF-VW6X] (discussing the dangers of applying physiognomy through AI due to its historically deeply prejudiced applications in the criminal law where "primitive type[s] of people" were more "prone to crime" and applications by Nazi "race scientists" to suggest evolutionary inferiority).

18 GATES, *supra* note 14, at 29.

19 *Id.*

enemy ranks and surrounding sensitive locations, such as military bases.[20]

Private sector interest in facial recognition has focused on adapting the technology to CCTV.[21] CCTV, while a low-cost method for expanding the surveillance capabilities of public and private actors, poses a problem of high labor costs in both the quantity of staff and time needed for monitoring footage.[22] From the 1990s to the early 2000s, DARPA and the National Institute of Standards and Technology (NIST) sponsored testing aimed at solving issues with integrating facial recognition to CCTV.[23] The organizations, by resolving technological limitations and creating uniformity across systems, ultimately hoped to encourage the creation of a private-sector commercial market for biometric technologies.[24] The resultant "Smart CCTV" would integrate automated facial recognition with video surveillance, creating new "algorithmic" forms of surveillance that could automatically manage the enormous amount of video imagery, providing accurate identification at a low labor cost.[25] In short, though the private-sector use of biometrics is nominally detached from the implications of governmental total-surveillance, similar sociological risks permeate the technology's development and the resulting effects on consumers.

Facial recognition's use of the face as the source of code influences the sociological response to its incorporation into private-sector systems.[26] Contemporary cultural meanings associated with

---

20 *Id.*

21 *Id.* at 66.

22 *Id.* at 64.

23 *Id.* at 71; *see also Face Recognition Technology (FERET)*, NIST (Jan. 25, 2011), https://www.nist.gov/programs-projects/face-recognition-technology-feret [https://perma.cc/7Y85-N7XV]. The Department of Defense (DoD) Counterdrug Technology Development Program Office sponsored the Face Recognition Technology (FERET) program, started in 1993. *Id.* The goal of the FERET program was to develop automatic face recognition capabilities that could be employed to assist security, intelligence, and law enforcement personnel in the performance of their duties. *Id.*

24 GATES, *supra* note 14, at 58–59, 71.

25 *Id.* at 64.

26 *See, e.g.*, Luke Dormehl, *Facial Recognition: Is the Technology Taking Away Your Identity?*, THE GUARDIAN (May 4, 2014, 3:00 PM), https://www.theguardian.com

the face are multivalent and dynamic—all individuals have faces and those faces are understood as inherently unique and a source of "identity."[27] This tracks with an enduring conception of the face as the "window to the soul"[28]—a location of centralized and concentrated significance for identity in the cultural imagination. Human societies are predicated on evolutionary abilities to individually recognize and track people in social networks.[29] The face functions as a site of judgment, where community members can assess features and movements—facial expressions—for similarities and differences, providing a tool for assessing a known or unknown individual's perceived mental state or threat level.[30] The Oxford English Dictionary recognizes many different meanings of "face," including: "[o]utward show; artificial or assumed expression or appearance; pretence"[31] but also "[r]eputation, credit; honour, good name."[32] Simultaneously, the face has the symbolic qualities of an impermeable "image," separating an individual's internal thoughts and processes from an exterior world of interpreters.[33] Symbolism is itself a dynamic force; as philosopher Bruno Latour suggests, "[h]umans are not the ones who arbitrarily add the 'symbolic dimension' to pure material forces."[34] Understood this way, the face—when used as code in computer-mediated technology—is an interface between cultural perceptions and physically apparent markers.[35] The use of facial recognition as a

---

/technology/2014/may/04/facial-recognition-technology-identity-tesco-ethical-issues [https://perma.cc/K2PG-JVJJ].

27 *See generally* Michael J. Sheehan & Michael W. Nachman, *Morphological and Population Genomic Evidence that Human Faces Have Evolved to Signal Individual Identity*, 5 NATURE COMM. 1 (2014).

28 *See* Stephen Porter et al., *Is the Face a Window to the Soul? Investigation of the Accuracy of Intuitive Judgments of the Trustworthiness of Human Faces*, 40 CAN. J. OF BEHAV. SCI. 171, 176 (2008).

29 Sheehan & Nachman, *supra* note 27, at 2.

30 *See* GATES, *supra* note 14, at 11.

31 *Face*, OXFORD ENGLISH DICTIONARY, http://www.oed.com/viewdictionaryentry/Entry/67425 [https://perma.cc/H6GQ-BXAA] (last visited Mar. 7, 2019).

32 *Id.*

33 *Cf.* VILEM FLUSSER, TOWARDS A PHILOSOPHY OF PHOTOGRAPHY 8 (1983). *See also* Tom Gunning, *In Your Face: Physiognomy, Photography, and the Gnostic Mission of Early Film*, 4 MODERNISM/MODERNITY 25 (1997).

34 BRUNO LATOUR, WE HAVE NEVER BEEN MODERN 128 (1993).

35 *See* ALEXANDER R. GALLOWAY, THE INTERFACE EFFECT 18–22 (2012).

networked surveillance technology degrades an already unstable division between embodied-space and "cyberspace."[36] Transcoding that results in a transformation from the depth of meanings expressed in the face to a machine-readable format reagitates a dormant "boundary anxiety" of reducing human uniqueness into deterministic binary.[37] As a result, the latent symbolic and cultural value of the face used as a technological piece of code is impossible to disentangle from the mobile and multifaceted history of meanings, making its use and interpretation a site of heightened agitation and sensitivity.[38] This latent cultural conception of the powers of facial recognition then colors the use and regulation of the technology.

2. The Technology: How Does It Work and What Data is Being Generated

Biometrics are technologies that allow for the automated recognition of individuals based on their behavioral and biological characteristics.[39] Biometrics, as a tool,[40] establishes confidence that one is dealing with individuals who are already known (or unknown)—and consequently that they belong to a group with certain rights (or to a group to be denied certain privileges).[41] Biometric data may be acquired from any source that visually documents an individual or that observes identifiable characteristics such as heart rate or odor.[42] For consumers, biometric data may be collected in various contexts such as automated photo tagging on sites such as Facebook, activity and health monitoring through

---

36 *See generally* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF 40–50 (2012).

37 *See* GALLOWAY, *supra* note 35, at 18–22; Laura Shanner, *Boundary Anxiety*, 26 CAN. MED. ASS'N J. 1273, 1273 (2002).

38 *See* GATES, *supra* note 14, at 11–12.

39 NATIONAL RESEARCH COUNCIL, BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES 1 (Joseph N. Pato & Lynette I. Millett, eds. 2010).

40 By a "tool" this Note considers Foucault's notion of "technologies of power" where the activity of exercising a technical goal generates information beyond the technical task and asserts control over how a subject is defined. *See* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 195–228 (1995).

41 NATIONAL RESEARCH COUNCIL, *supra* note 39, at 1.

42 Anil K. Jain et al., *An Introduction to Biometric Recognition*, 14 IEEE TRANSACTIONS ON CIR. SYS. VIDEO TECH. 4, 4 (2004).

wearable technologies such as Fitbit, and even the gestures used when individuals interact with their phones and computers.[43]

The private sector has adopted facial recognition as a commonly used biometric identifier.[44] Automatic facial recognition methods collect biometric data on the characteristics of individuals faces through a step-by-step process.[45] First, the system extracts patterns in an image and compares them against a model of a face, establishing the presence of a face.[46] Second, a facial recognition algorithm registers the face and places it in a preset position, allowing for standardization of the image, so it is in the same format as the images in the database.[47] The resultant data is referred to as a "faceprint."[48] The faceprint measurements and other collected information are "biometric data," which are compiled into a database.[49] Using the biometric database, faceprints may then allow for: (1) facial classification, by classifying the face into categories such as an estimation of gender, age or race; (2) verification, by comparing the similarity of previously stored faceprint of any particular individual to a new faceprint and establishing a confidence score that the two individuals are the same; and (3) identification, by comparing a person's facial image to a database of stored faceprints.[50]

In the past several years, underlying biometric technologies have consistently improved following increased investment and research in facial recognition systems.[51] Newer systems have enhanced accuracy by incorporating neural networks, a machine-learning AI technique that is used to find an optimal function to solve a task from

---

43 *See, e.g.*, Stacy Cowley, *Hold the Phone! My Unsettling Discoveries About How Our Gestures Online Are Tracked*, N.Y. TIMES (Aug. 15, 2018), https://www.nytimes.com/2018/08/15/business/behavioral-biometrics-data-tracking.html [https://perma.cc/RQ9B-FF7B].

44 *See* COMMERCIAL USES, *supra* note 4, at 7; *see also* Jain, *supra* note 42, at 9.

45 COMMERCIAL USES, *supra* note 4, at 3–4.

46 *Id.*

47 *Id.*

48 *Id.*

49 HANDBOOK OF FACE RECOGNITION 2–3, 11 (Stan Z. Li & Anil K. Jain eds., 1st ed. 2005).

50 FED. TRADE COMM'N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES 4–5 (2012).

51 COMMERCIAL USES, *supra* note 4, at 3.

a large number of inputs.[52] As a result, facial recognition technologies available for private sector actors are more accurate, less expensive, and readily available from cloud software providers like AWS.[53]

How faceprints in databases are compiled, structured, and stored may implicate privacy concerns. Using facial recognition requires accessing reference material through a multimedia database.[54] A multimedia database is a database that contains one or more types of information such as text, image, video clip, sound, diagram, and graphical animation.[55] The material in multimedia databases may be generated by the system and populated from a variety of sources. Various websites have collected facial images in the form of mug shots from an estimated seventy-eight million Americans with criminal records from police departments and sheriffs' offices across the country.[56] Even individuals who are arrested but never charged have their photos on these sites.[57] The increasing public availability of facial images, especially as companies like Facebook pursue "real identity" policies, may result in an immense searchable multimedia database for previously unidentified individuals.[58]

Face recognition systems are capable of matching faceprints with individuals' names at times when consumers' identities are

---

[52] Yana Welinder & Aeryn Palmer, *Face Recognition, Real-Time Identification, and Beyond*, *in* CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY, 3–4 (2018).

[53] *See, e.g.*, *Amazon Rekognition*, AWS, https://aws.amazon.com/rekognition/ [https://perma.cc/5792-B4G2]; *see also* Justin Lee, *Credence Research Report Forecasts Biometrics Market to Reach $34.5B by 2022*, BIOMETRIC UPDATE (May 8, 2016), http://www.biometricupdate.com/201605/credence-research-report-forecasts-biometrics-market-to-reach-34-5b-by-2022 [https://perma.cc/T59D-4Q4J].

[54] N. Tsapatsoulis et al., *Facial Image Indexing in Multimedia Databases*, 4 PATTERN ANALYSIS & APPLICATIONS 93, 93–94 (2001).

[55] *Id.* at 93.

[56] Rebecca Beitsch, *Fight Against Mugshot Sites Brings Little Success*, PEW RES. CTR. (Dec. 11, 2017), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2017/12/11/fight-against-mugshot-sites-brings-little-success [https://perma.cc/R9E9-XNF5].

[57] *Id.*

[58] *See* Alessandro Acquisti et al., *Face Recognition and Privacy in the Age of Augmented Reality*, 6 J. PRIVACY & COMM. 1, 1 (2014) (demonstrating through research the capability to reliably reidentify individuals offline using Facebook reference photos); *see also* FED. TRADE COMM'N , *supra* note 50, at 8 ("[The FTC] is not aware of companies currently using data in these ways, if they begin to do so, there would be significant privacy concerns.").

known, such as when using CCTV to monitor store checkouts or returns when credit cards are used.[59] Additionally, geo-fencing and passive Wi-Fi tracking may allow identification by matching a smartphone's Device ID with a face scan.[60] By collecting signals from a smartphone's Wireless Positioning System (WPS) and Global Positioning System (GPS) connecting with a Wi-Fi network access point, a system may identify a user profile that has been created using the same phone.[61] The system then could identify an individual's faceprint by combining automated CCTV data with device information from Wi-Fi positioning.[62] While this field is still developing, as facial recognition gains more widescale adoption, market forces likely will improve and expand upon automated identification techniques.[63]

B. Privacy and Compounding Consumer Risks

Biometrics provide a technology capable of real-time automated constant surveillance, exposing consumers to new privacy risks. The collection of data exposes consumers to the risk of their private information being shared with unintended recipients through the sale to third parties or data breaches.[64] Consumers are already experiencing a "new normal," in which companies routinely suffer from cyber-attacks that reveal the sensitive data of millions of consumers.[65] Unlike financial information, biometric data is "more

---

[59] Evan Schuman, *What's the Truth Behind Walmart's Failed Facial Recognition Trial?*, COMPUTERWORLD (Nov. 11, 2015, 3:05 AM), https://www.computerworld.com/article/3004166/retail-it/whats-the-truth-behind-walmarts-failed-facial-recognition-trial.html [https://perma.cc/G3D4-P6YA].

[60] Stephanie Clifford & Quentin Hardy, *Attention, Shoppers: Store Is Tracking Your Cell*, N.Y. TIMES (July 14, 2013), https://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html?pagewanted=all&_r=0 [https://perma.cc/2WAS-4WMF].

[61] Dmitry Namiot & Manfred Sneps-Sneppe, *Geofence and Network Proximity*, *in* INTERNET OF THINGS, SMART SPACES, AND NEXT GENERATION NETWORKS AND SYSTEMS: 17TH INTERNATIONAL CONFERENCE 117, 118 (Olga Galinina et al. eds., 2017).

[62] *Cf. id.*

[63] *See generally* TUROW, *supra* note 12.

[64] *See generally* FED. TRADE COMM., PRIVACY & DATA SECURITY UPDATE (2016), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2016/privacy_and_data_security_update_2016_web.pdf [https://perma.cc/E22Y-7AXK].

[65] *See,* Stacey-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C.L. REV. 423, 425–26 (2018).

vulnerable as a data set," because you can't "replace [it] like you can a credit card."[66] Additionally, biometric data is not subject to existing regulatory liabilities associated with using sensitive consumer financial information.[67] The transfer of information between collecting companies and the compiling of user databases with aggregated profiles of consumers may compound the risks of sensitive information and creates an increased potential for substantial harm to consumers.[68] While the collection of biometrics may provide new functions to business, it also presents privacy risks for consumers. Section I.B.1 outlines biometric privacy concerns involving locational data and surveillance, Section 1.B.2 discusses the privacy risks of data breaches, and Section I.B.3 discusses how aggregation by data brokers may compound privacy risks.

1. Privacy and Surveillance

Biometric data presents privacy risks due to its dual nature— as a digital record of automated and remote surveillance on one hand, and an irreplaceable and privately held password to consumers' sensitive accounts on the other.[69]

Biometrics, especially through facial recognition, are surveillance technologies—identifying and tracking individuals and collecting information about user's lifestyles, habits, preferences, and associations.[70] In *Carpenter v. United States*,[71] the Supreme Court held that cell site location information (CSLI), automatically generated location information capable of tracking an individual when they used their cell phone, was protected private information as it "provide[d] an intimate window into a person's life, revealing

---

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

67 For example, the FTC has enforcement powers under the Gramm-Leach Bliley Act, 15 U.S.C. §§ 6801–6803, and FACT Act 15 U.S.C. §§ 1601–1616, when the information collector is a financial or credit reporting institution.

68 *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1703, 1768–79 (2010).

69 Ohm, *supra* note 8, at 1131.

70 *See, e.g.*, Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591, 1593 (2017).

71 *See generally* 138 S. Ct. 2206 (2018).

not only [their] particular movements, but . . . familial, political, professional, religious, and sexual associations."[72] While Justice Roberts opinion does not directly implicate private actors,[73] the collection of biometrics by private parties raises similar privacy concerns.

Research suggests that Americans are increasingly sensitive about the data collected from them by private actors.[74] A 2015 Pew Research Center study suggested that contrary to assertions that people increasingly "don't care" about privacy,[75] Americans value their personal information and freedom from surveillance in daily life.[76] The study found that 63% of participants felt it is important to be able to "go around in public without always being identified."[77] In an earlier study, Pew found that a majority—81%—of participants agreed that surveillance cameras are hard to avoid and that physical location over time was a sensitive category.[78] These observations are coherent with a sense that the proliferation of

---

72 *Id.* at 2217 (citing *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

73 *See generally* 138 S. Ct. 2206 (2018).

74 Vindu Goel, *Survey Finds Americans Don't Trust Government and Companies to Protect Privacy*, N.Y. TIMES (May 20, 2015, 10:00 AM), https://bits.blogs.nytimes.com/2015/05/20/survey-finds-americans-dont-trust-government-and-companies-to-protect-privacy/ [https://perma.cc/KX9S-5V47].

75 *See generally* Claire Cain Miller, *Americans Say They Want Privacy, but Act as if They Don't*, N.Y. TIMES (Nov. 13, 2014), https://www.nytimes.com/2014/11/13/upshot/americans-say-they-want-privacy-but-act-as-if-they-dont.html [https://perma.cc/494V-CURB]. This phenomenon has been described in online behavior as the "privacy paradox" where users claim to be very concerned about their privacy yet undertake very few steps to protect their personal data. *See generally* Susanne Barth & Menno D.T. de Jong, *The Privacy Paradox- Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review*, 34 TELEMATICS & INFORMATICS 1038 (2017).

76 Mary Madden & Lee Rainie, *Americans' Views About Data Collection and Security*, PEW RES. CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-views-about-data-collection-and-security/ [https://perma.cc/9LRA-3E95].

77 *Id.*

78 *Id.* (noting that many participants mentioned the presence of cameras of various kinds, stating, for example, that "*CCTV [c]ameras are all over the place*" and "*[w]e are always on video. We leave [an] imprint as soon as we leave our house.*").

privacy-degrading devices leaves consumers uncomfortable and "fatigued," but disempowered to meaningfully act in response.[79]

Studies addressing consumer sentiments towards biometrics emphasize specific sensitivity to use of the technology in commercial settings.[80] In a study by the Consumer Technology Association (CTA), consumers were less comfortable with biometric screening in malls and open public places than in areas like airports, which were perceived as more secure.[81] The study found that the use of biometrics for commercial purposes produced the lowest comparative levels of comfort, with only 40% of participants being comfortable with its use.[82] Additionally, the CTA study found that consumers trusted commercial organizations such as retail the least—15%—in terms of biometric information.[83] The CTA study found that commercial consumers were more comfortable with some activities like authenticating transaction at retail stores, but were less so for commercial service personalization such as serving special offers in physical retail stores.[84] Similarly, a 2018 study by the Brookings Institutive found that 50% of participants found the use of facial recognition in retail settings to prevent theft unfavorable, with 42% of those surveyed stating that facial recognition was an invasion of personal privacy.[85] Within

---

[79] In explaining the ''privacy paradox," Hargittai and Marwick emphasize pragmatism as a central component. This is the paradox that emerges from a prominent concern with privacy in the digital environment that is not manifested in actual online behavior. Focusing on young people in particular, they outline how people experience ''privacy fatigue" and confusion about the data-driven systems in place, which leads to an acceptance of their data being collected as a pragmatic response in the negotiation with digital infrastructures and a sense of disempowerment to fundamentally challenge the nature of data collection. *See* Eszter Hargittai & Alice Marwick, *What Can I Really Do? Explaining the Privacy Paradox with Online Apathy*, 10 INT'L J. OF COMM'N 3737, 3738–41, 3752–53 (2016).

[80] *See generally* CONSUMER TECH. ASS'N, BIOMETRIC TECHNOLOGIES: UNDERSTANDING CONSUMER SENTIMENTS (2016).

[81] *Id.* at 16.

[82] *Id.* at 23.

[83] *Id.* at 53.

[84] *Id.* at 49.

[85] Darrell M. West, *Brookings Survey Finds 50 Percent of People Are Unfavorable to Facial Recognition Software in Retail Stores to Prevent Theft*, BROOKINGS (Oct. 8, 2018), https://www.brookings.edu/blog/techtank/2018/10/08/brookings-survey-finds-50-percent-of-people-are-unfavorable-to-facial-recognition-software-in-retail-stores-to-prevent-theft/ [https://perma.cc/34N4-5C8A].

identification, facial recognition is generally perceived as more concerning to privacy than other biometric techniques.[86] In a University of Texas study, respondents most often ranked facial recognition as the biometric technique with which they were least comfortable.[87]

Consumer mistrust and sensitivity towards surveillance techniques informs legal scholarship suggesting that the constant surveillance of individuals' activities leads to privacy harms and the "chilling" of social interactions.[88] Scholarship from social science research demonstrates that—when watched—individuals change their activities, avoiding "experiment[ing] with new, controversial, or deviant ideas."[89] Jonathan Penney has shown empirically that online surveillance causes "chilling," where individuals self-censor, avoiding perceived risks about activities being leaked or disclosed where they would cause embarrassment or be used for nefarious purposes.[90] Julie E. Cohen argues this effect homogenizes social interaction where the "pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream."[91] Daniel Solove has theorized that the monitoring-induced mainstreaming of identity inhibits freedom of choice, resulting in pervasive forms of social control that are anti-democratic.[92] Joel Reidenberg emphasizes that anonymity in public is a critical feature for an open society, by protecting individuals from stalking and violence and enabling them to hold and advocate

---

86 *See generally* Jamie Condliffe, *Facial Recognition Is Getting Incredibly Powerful—and Ever More Controversial*, MIT TECH. REV. (Sept. 8, 2017, 10:16 AM), https://www.technologyreview.com/the-download/608832/facial-recognition-is-getting-incredibly-powerful-and-ever-more-controversial/ [https://perma.cc/MZV9-K96G].

87 RACHEL L. GERMAN & K. SUZANNE BARBER, CONSUMER ATTITUDES ABOUT BIOMETRIC AUTHENTICATION: A UT CID REPORT 7 (May 2018).

88 *See, e.g.*, Jonothan W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKLEY TECH. L.J. 117, 121–23 (2016).

89 Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013).

90 Penney, *supra* note 88, at 126–27.

91 Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000).

92 *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 494 (2006); *see* FOUCAULT, *supra* note 40, at 195–228 (theorizing that in a "panoptic society," where individuals are under constant surveillance, the surveillance does not need to be "perfect" for individuals to behave as though they are under perfect surveillance).

unpopular ideas.[93] These possible negative effects, while more problematic in governmental surveillance, are replicated in part through private sector surveillance.[94] As a result, facial recognition may frustrate the ability to blend into the "obscurity" of a crowd, by lowering the transaction costs of finding and identifying people and ultimately restricting individuals expressive and social capacities.[95]

While much scholarship has focused on direct governmental surveillance, the increasing scope of surveillance data collection from private actors implicates similar risks. Kiel Brennan-Marquez explains that existing voluntary data-sharing of surveillance material between private-sector actors and the government increases the potential of privacy harms.[96] Private-sector actors already compile information on specific individuals' locations and repackage it for police departments.[97] Biometrics may increase the potential for harm as locational information is not limited to geo-tags drawn from social media posts.[98] Private actors' direct access to increasingly large quantities of data on individuals' informal data-sharing, along with a lack of constraint by the constitutional safeguards of the Fourth Amendment, may result in the amplification of harms.[99]

2. Data Breach Risks

Biometric information is based on a unique physiological characteristic making it naturally stable and hard to artificially alter.[100] For this reasons device developers, app developers, and

---

93 Joel Reidenberg, *Privacy in Public*, 69 U. MIAMI L. REV. 141, 153 (2014).

94 *See* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1031 (2014) (noting that coercive tendencies of private actors with a profit-maximizing motive is more acceptable than "the dangers that attend tyranny").

95 WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 234 (2018). Hartzog defines "obscurity" as "the state of information or people being hard or unlikely to be found or understood." *Id.*

96 Kiel Brennan-Marquez, *The Constitutional Limits of Private Surveillance*, 66 KAN. L. REV. 485, 486, 488–89 (2018).

97 *Id.* at 486.

98 *See id.*

99 *Id.* at 498.

100 Margaret Rouse, *Biometric Verification*, TECHTARGET.COM (May, 2008), https://searchsecurity.techtarget.com/definition/biometric-verification [https://perma.cc/Z2UY-N6LZ].

businesses are creating products which utilize this uniqueness of biometrics for password authentication, similar to the use of Social Security Numbers in the financial sector.[101] The expanding collection of data increases the risk of data breaches, which have been ever increasing.[102] Large biometric databases, including the fingerprint database of the Office of Personnel Management, have already been hacked.[103] Other biometric databases such as those containing face-shape data are susceptible to hacking.[104] Stolen biometric identifiers then can be used to impersonate consumers, gaining access to personal information.[105] The use of biometrics for accessing sensitive personal information creates an increased risk of tangible and substantial harm if the information is stolen.[106]

The privacy risks of data breach may lead to potential harms even where stolen consumer data is not used to directly harm

---

[101] *See, e.g.*, Arielle Pardes, *Facial Recognition Tech Is Ready for Its Post-Phone Future*, WIRED (Sept. 10, 2018, 7:00 AM), https://www.wired.com/story/future-of-facial-recognition-technology/ [https://perma.cc/MW75-RS6T]; *see also* Ohm, *supra* note 8, at 1144.

[102] *See, e.g.*, KROLL, BUSINESSES REPORT ALL-TIME HIGH LEVELS OF FRAUD, CYBER, AND SECURITY INCIDENTS DURING 2017 (2018), https://www.kroll.com/-/media/kroll/pdfs/news/business-report-fraud-cyber-and-security-incidents-2017.ashx?la=en [https://perma.cc/2G2U-SL5G].

[103] *See, e.g.*, Anish Malhotra, *The World's Largest Biometric ID System Keeps Getting Hacked: The Personal Data of Many Indians Is For Sale on WhatsApp For Less Than $10*, VICE: MOTHERBOARD (Jan. 8, 2018, 10:07 AM), https://motherboard.vice.com/en_us/article/43q4jp/aadhaar-hack-insecure-biometric-id-system [https://perma.cc/UPS9-Z87U]; *see also US Government Hack Stole Fingerprints of 5.6 Million Federal Employees*, THE GUARDIAN (Sept. 23, 2015, 5:44 PM), https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints [https://perma.cc/2P5G-KXWQ].

[104] Kaveh Waddell, *When Fingerprints Are as Easy to Steal as Passwords*, THE ATLANTIC (Mar. 24, 2017), https://www.theatlantic.com/technology/archive/2017/03/new-biometrics/520695/ [https://perma.cc/TL79-L4JF].

[105] *Id. But see* Andy Greenberg, *We Tried Really Hard To Beat Face ID—And Failed (So Far)*, WIRED (Nov. 3, 2017, 7:00 AM), https://www.wired.com/story/tried-to-beat-face-id-and-failed-so-far/ [https://perma.cc/29BQ-4CBA] (discussing how Wired magazine spent thousands of dollars on expensive masks and enlisted experienced biometric hackers in an attempt to trick Face ID following the release of the iPhone X, but still failed to beat the system).

[106] FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/N8DJ-FNDL].

consumers. Daniel Solove and Danielle Citron theorize that consumers, anxious to the risks following a data breach, will act more cautiously as they become aware of the ongoing threats of their data in the possession of hackers.[107] The heightened risk of harm following a data breach creates an additional harm in the form of a lost opportunity cost as individuals take actions to mitigate expected loss, resulting in "chilling a person's ability to engage in life's important activities."[108]

3. Big Data Aggregation and Algorithmic Bias

Biometrics exists within a landscape of the large-scale creation, collection, and analysis of consumer data.[109] 2.5 quintillion bytes of data are created each day at our current pace, with 90% of the data in the world generated in the past two years.[110] The dramatic increase in networked technologies combined with advancing trends in data analytics technology has opened the door to a new approach to understanding the world and making decisions—big data analysis.[111] "Big data" are algorithmic information techniques that process large volume datasets and provide insights.[112] Using predictive models, big data facilitates the analysis of large data sets and provides summaries that support consumer evidence-based decision-making, and captures nuanced pictures of consumers, which reveal "unexpected inferences about our habits, predilections, and personalities."[113] Shoshana Zuboff describes this process as "surveillance capitalism" where data extraction greatly diminishes

---

[107] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 759 (2018).

[108] *Id.*

[109] *See, e.g.*, Madden & Rainie, *supra* note 76.

[110] Bernard Marr, *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*, FORBES, (May 21, 2018, 12:42 AM), https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#469bbaaa60ba [https://perma.cc/VT7N-DNLW].

[111] Steve Lohr, *The Age of Big Data*, N.Y. TIMES (Feb. 11, 2012), https://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html [https://perma.cc/EW4B-M323].

[112] Amir Gandomi & Murtaza Haider, *Beyond the Hype: Big Data Concepts, Methods, and Analytics*, 35 INT'L J. INFO. MGMT. 137, 140 (2015).

[113] Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 90 (2014).

the information costs of corporate actors, redistributing privacy rights away from consumers and towards corporate actors.[114]

Consumer behavioral insights are a valuable commodity across various business sectors including marketing and ecommerce.[115] As a result, big data analysis has become an industry worth hundreds of billions of dollars.[116] In the present data economy, consumer data is routinely shared, sold, or made available to third parties.[117] The ecosystem of big data analysis is served by data brokers—third parties that aggregate consumer information across sources and use it to create highly detailed profiles about individuals.[118] One of the largest data brokers, Acxiom reportedly has 1500 data points on over 700 million individuals.[119] Data brokers do not have a direct relationship with the individuals they are collecting data on, and individuals are often unaware that their information is being transferred, shared, or sold to third parties.[120] This process occurs in a landscape with almost no restrictions on the transferal of information collected by a first party to third party actors, with consumers having no way of identifying which parties hold their information.[121]

---

[114] Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75, 83 (2015).

[115] Alex Romanov, *Putting a Dollar Value on Data Insights*, WIRED, https://www.wired.com/insights/2013/07/putting-a-dollar-value-on-big-data-insights/ [https://perma.cc/M32R-2G7Z] (last visited Sept. 24, 2018) (noting that Walmart was able to use big data analysis to drive a 10–15% increase in completed online sales for $1 billion in incremental revenue).

[116] *Data, Data Everywhere*, ECONOMIST (Feb. 25, 2010), https://www.economist.com/special-report/2010/02/25/data-data-everywhere [https://perma.cc/V89V-UZ6P].

[117] *Id.*

[118] *See* Julie Brill, *Demanding Transparency from Data Brokers*, WASH. POST (Aug. 15, 2013), http://www.washingtonpost.com/opinions/demanding-transparency-from-data-brokers/2013/08/15/00609680-0382-11e3-9259-e2aafe5a5f84_story.html [https://perma.cc/37TX-2SRL].

[119] *Id.*

[120] Yael Grauer, *What Are "Data Brokers," and Why Are They Scooping Up Information About You?*, VICE: MOTHERBOARD (Mar. 27, 2018, 10:00 AM), https://motherboard.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection [https://perma.cc/59TR-XGJN].

[121] Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321, 337 (2013).

Biometrics are a potential solution to an industry issue of "data [being] worthless in a vacuum."[122] Insights from data may only be extracted where data is structured,[123] allowing analytic processes to turn the high volume of "meaningless" raw data into "meaningful insights."[124] Some data, like purchase records, may be collected in structured form. By one estimation structured data accounts for only 5% of all existing collected data.[125] Large quantities of data collected in formats such as video, image, and audio, on the other hand, cannot be leveraged for insights without an intermediate process to structure the data.[126] Facial recognition, when used as a unique persistent identifier in a data management system, enables organizations to structure previously unstructured video data, associating an identity with other raw data such as previous purchases, emotional response, age, gender, and in-store movement patterns, and increasing the value of the customer profile.[127] When analyzing consumer decision-making, consumer engagement that does not result in a conversion or purchase may be as significant as those transactions that are recorded in financial data.[128] Biometric identification techniques, when shared across data collectors, then dramatically expand the sources from which consumer data may be drawn, increasing the accuracy and invasiveness of aggregate profile creation.

The effects of biometric data's utility—identifying specific individuals—compound privacy risks from data aggregation. Consumer profiles assembled using biometrics are more valuable to data brokers as they provide greater profile accuracy.[129] In a

---

122 Gandomi & Haider, *supra* note 112, at 140.

123 Structured data, unlike unstructured data, has predefined metadata and can be stored in relational databases making it searchable by human or algorithm.

124 Gandomi & Haider, *supra* note 112, at 140.

125 *Id.* at 138.

126 *Id.*

127 *Id.*

128 Sam Ransbotham & David Kiron, *Using Analytics To Improve Customer Engagement*, MIT SLOAN MGMT. REV. (Jan. 30, 2018), https://sloanreview.mit.edu/projects/using-analytics-to-improve-customer-engagement/ [https://perma.cc/4YLL-DLJ7].

129 *See* MCKINSEY, THE AGE OF ANALYTICS COMPETING IN A DATA-DRIVEN WORLD 65 (2016), https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Analytics/Our%20Insights/The%20age%20of%20analytics%20Competin

marketplace where aggregate consumer data often contains incorrect and erroneous information,[130] increasing the accuracy of information is highly lucrative for data brokers.[131] More accurate data allows for higher confidence in insights, which allows for a competitive advantage to the data's users in predicting consumer's actions.

The wide availability of facial biometric identity allows corporations to use previously unstructured locational and choice-based data to tailor marketing based on the specific identity, compounding the invasive harmful effects of behavioral marketing.[132] As Ryan Calo has observed, increased accuracy of personal information profiles can allow for "digital market manipulation" by being leveraged for the "mass production of bias," "disclosure ratcheting," and "means-based targeting."[133] Calo explores how big data analysis, using insights derived from behavioral economics, permits firms to delineate the specific ways each individual consumer "deviates from rational decisionmaking, however idiosyncratic, and leverage that bias to the firm's advantage."[134] Calo identifies the economic and privacy costs from digital market manipulation.[135] The technique results in increased transaction costs when "consumer[s] spend time and money hiding their identity or browsing the same website at different times or with different browsers in order to compare price or even to avoid creepy ads."[136] Simultaneously, "the unanticipated or coerced use of

---

g%20in%20a%20data%20driven%20world/MGI-The-Age-of-Analytics-Full-report.ashx [https://perma.cc/9N54-YAQ9].

130 Melanie Hicken, *Find Out What Big Data Knows About You (It May Be Very Wrong)*, CNN: MONEY (Sept. 5, 2013, 2:02 PM), https://money.cnn.com/2013/09/05/pf/acxiom-consumer-data/ [https://perma.cc/9N7Q-PDUZ].

131 *Facial Recognition Market is Expected to Reach $9.6 Billion, Worldwide by 2022*, CISION: PRNEWSWIRE (June 29, 2016), https://www.prnewswire.com/news-releases/facial-recognition-market-is-expected-to-reach-96-billion-worldwide-by-2022-584841741.html [https://perma.cc/6YK3-RJY4].

132 Ashley Deeks & Shannon Togawa Mercer, *Facial Recognition Software: Costs and Benefits*, LAWFARE (Mar. 27, 2018, 9:00 AM), https://www.lawfareblog.com/facial-recognition-software-costs-and-benefits [https://perma.cc/6NJX-D8L6].

133 *See* Calo, *supra* note 94, at 995–96.

134 *Id.* at 1003.

135 *Id.* at 1027.

136 *Id.*

personal information" may disadvantage individuals through rent extraction, such as raising prices for those who visit a product page multiple times.[137]

Citron and Pasquale have further noted that analysis of data to create individuals' scores may be harmful by "turn[ing] individuals into ranked and rated *objects*" that control individuals opportunities but may be based in inaccurate information or algorithmic bias with little transparency or input by scored parties.[138] Additional risks occur where bias inherent to algorithms results in replicating "cross-race effect[s]," where historically disenfranchised groups are disproportionally misidentified.[139] This outcome can result in replication of discriminatory practices, such as misidentifying individuals as shoplifters in a retail setting.[140] Where privacy is at risk from the types, use, and quantity of information collected, the effects of facial recognition in this data environment require more precise analysis.

C. Biometrics in Retail

Facial recognition is a rapidly growing biometric technology used in the retail sector.[141] A recent study found that facial recognition is likely to generate revenue of $9.78 billion by 2023, growing at a compounded annual growth rate of 16.81% between 2017 and 2023.[142] The market for facial recognition is increasing, with large investments of up to $1.6 billion in start-ups from China, a country that has been an open environment for testing the

---

137 *Id.* at 1029–30.

138 Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 3–5 (2014).

139 Rod McCullom, *Facial Recognition Is Both Biased and Understudied*, UNDARK (May 17, 2017), https://undark.org/article/facial-recognition-technology-biased-understudied/ [https://perma.cc/3WGM-29PC]; *see also* Steve Lohr, *Facial Recognition Is Accurate, If You're a White Guy*, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html [https://perma.cc/7LM2-NRQG] (noting that each company's error rates were significantly higher for non-white non-male individuals).

140 McCullom, *supra* note 138.

141 Lieber, *supra* note 7.

142 *Global Facial Recognition Market Report 2018*, CISION: PR NEWSWIRE (June 5, 2018), https://www.prnewswire.com/news-releases/global-facial-recognition-market-report-2018-300660163.html [https://perma.cc/24AT-F9ST].

technology.[143] Intel, and Chinese internet company Tencent, have announced a collaboration on products that use AI and facial recognition to "gain new insights about their customers to both elevate the users' experience and drive business transformation."[144] Decreases in the associated costs of the technology have made facial recognition software a viable tool for retailers.[145] Services such as FaceFirst offer facial recognition specifically targeted to retailers using "surveillance . . . and an underlying software platform that leverages artificial intelligence to [prevent] theft, [fraud,] . . . and . . . violence."[146] Additionally, facial recognition can be used by retailers to connect online with offline behaviors, provide more in-depth demographics, and track in-store product engagement.[147] This Section discusses the specific uses of facial recognition technologies in the retail sector and the potential legal questions that arise from data collection, use, and sharing.

The idea of retailers tracking customers is not new.[148] Neither is the premise of using images of customers to provide personalized

---

143 Jamie Condliffe, *Big Investors are Placing Bets on China's Facial Recognition Start-Ups*, N.Y. TIMES (July 24, 2018), https://www.nytimes.com/2018/07/24/business/dealbook/china-facial-recognition.html [https://perma.cc/A6NN-B2JS]; *see also* Rachel Change, *China is the World's Retail Laboratory*, BLOOMBERG BUS. (Oct. 18, 2018, 12:01 AM), https://www.bloomberg.com/news/features/2018-10-18/china-is-the-world-s-retail-laboratory [https://perma.cc/7GTV-VLLC].

144 Jonathan Chadwick, *Tencent Teams Up with Intel for Retail Surveillance Camera and "AI Box,"* COMPUTER BUS. REV. (Nov. 2, 2018), https://www.cbronline.com/news/ai-box [https://perma.cc/5DUX-BZMA]; *see also* Ashley Armstrong, *Chinese Online Retailer JD Plans to Open Hundreds of Unmanned Shops, Ahead of Amazon*, TELEGRAPH (Dec. 14, 2017, 12:10 PM), https://www.telegraph.co.uk/business/2017/12/14/chinese-online-retailer-jd-plans-open-hundreds-unmanned-shops/.

145 Nick Coult, *Facial Recognition Software: Coming Soon to Your Local Retailer?*, CRIME REP. (Apr. 23, 2018), https://thecrimereport.org/2018/04/23/facial-recognition-software-coming-soon-to-your-local-retailer [https://perma.cc/9C9A-TPQA].

146 *FaceFirst Launches Fraud-IQ to Solve $9.6B Retail Return Fraud Problem with Facial Recognition*, CISION: PRWEB (June 11, 2018), https://www.prweb.com/releases/2018/06/prweb15550963.html [https://perma.cc/NE4U-7MBJ].

147 Bryan Pearson, *3 Ways Retailers Can Use Facial Recognition To Create Better Experiences*, FORBES (Mar. 15, 2018, 3:47 PM), https://www.forbes.com/sites/bryanpearson/2018/03/15/3-ways-retailers-can-use-facial-recognition-to-express-better-experiences/#4e87d12c1766 [https://perma.cc/DKP3-K2HR].

148 *See* TUROW, *supra* note 12, at 87 (discussing the use of reward cards to track specific customers purchases and send unique promotions). Building customer loyalty through memory of specific clients and shaping a retail experience to their habits and needs are at

white glove service.[149] A central premise in the historical development of retail has been providing "personalized service" and creating customer loyalty.[150] What is new is the expanded accuracy and range of collection beyond a point of sale or loyalty programs.[151] "True personalization," through individual-level relevance has been the most difficult marketing tactic, because it requires both responsiveness and highly accurate data, which is difficult to collect, analyze, and apply to messages in real time.[152] Facial recognition may allow for other consumer benefits including an enhanced customer service experience,[153] greater operational efficiency,[154] better advertising quality,[155] and most importantly convenience.[156] Additionally, facial recognition may allow for greater competition

---

the root of what is considered good customer service. *See* Leigh Buchanan, *A Customer Service Makeover*, INC. (Mar. 1, 2011), https://www.inc.com/magazine/20110301/a-customer-service-makeover_pagen_2.html [https://perma.cc/E5YG-75EC].

149 *See, e.g.*, Drew Limsky, B*usiness Travel; Hotels Are Doing Business on a Last-Name Basis*, N.Y. TIMES (Oct. 1, 2002), https://www.nytimes.com/2002/10/01/business/business-travel-hotels-are-doing-business-on-a-last-name-basis.html [https://perma.cc/7GDH-4C3Z] (discussing upscale hotel chains' guest recognition programs where "photographs of V.I.P.'s are distributed by e-mail to the hotel staff" emphasizing personalized service and identity recognition); *see also* Julie Weed, *Checking in After Checkout*, N.Y. TIMES (May 27, 2013), https://www.nytimes.com/2013/05/28/business/hotels-work-harder-to-collect-customer-responses.html [https://perma.cc/KPL8-4SV3] (describing the use of internal customer feedback to tailor service to the specific customer).

150 *See* TUROW, *supra* note 12, at 29–30 (discussing early twentieth century retailers trust-based relationships with consumers and the ability to recognize patterns of transactions).

151 *Id.* at 3.

152 *Id.* at 186.

153 *See, e.g.*, Hayley Peterson, *Walmart Is Developing a Robot That Identifies Unhappy Shoppers*, BUS. INSIDER (July 19, 2017, 11:39 AM), https://www.businessinsider.com/walmart-is-developing-a-robot-that-identifies-unhappy-shoppers-2017-7 [https://perma.cc/NLS7-H2WS].

154 *See, e.g.*, Annie Lin, *Facial Recognition Is Tracking Customers as They Shop in Stores, Tech Company Says*, CNBC (Nov. 23, 2017, 11:23 PM), https://www.cnbc.com/2017/11/23/facial-recognition-is-tracking-customers-as-they-shop-in-stores-tech-company-says.html [https://perma.cc/8P3Y-4A2C].

155 *See, e.g.*, MARK BARTHOLOMEW, ADCREEP: THE CASE AGAINST MODERN MARKETING 73 (2017).

156 *See, e.g.*, Will Knight, *Paying with Your Face*, MIT TECH. REV., https://www.technologyreview.com/s/603494/10-breakthrough-technologies-2017-paying-with-your-face/ [https://perma.cc/P3SS-SXSC] (last visited Oct. 16, 2018); *see also* Andrea Felsted, *From Amazon to Alibaba Grocers' Agony Is Endless*, BLOOMBERG (Aug. 6, 2018, 1:00 AM), https://www.bloomberg.com/view/articles/2018-08-06/from-amazon-to-alibaba-grocers-agony-is-endless [https://perma.cc/2EYH-S74H].

in the "war" between brick-and-mortar retailers and ecommerce retailers like Amazon.[157] Out of a need to compete for consumers, stores are becoming physical websites, as retailers invest in in-store technologies that can replicate the types of information collected by cookies and other markers online.[158] The goal is to exceed the types and quantity of information collected online, providing a competitive advantage for retailers that maintain physical presences.[159] This strategy is described in the industry as "omnichannel," where a physical retailer can meld various points of information from online and mobile phone capabilities with its physical resources.[160] Facial recognition can be incorporated into omnichannel as a persistent identifier.[161] This can solve an existing issue of "identity resolution," which requires retailers to connect customers' many identifiers across channels (like email addresses, cookies, phone numbers, mobile device ad IDs and home addresses)

---

[157] *See* TUROW, *supra* note 13, at 142 (discussing the use of reward cards to track specific customers purchases and send unique promotions). This creates a situation in which retailors must adapt to new expectations and pressures of consumers or face failure. *See* Matt Townsend et al., *America's "Retail Apocalypse" Is Really Just Beginning*, BLOOMBERG (Nov. 8, 2017), https://www.bloomberg.com/graphics/2017-retail-debt/ [https://perma.cc/8N9S-Q64X].

[158] *See* TUROW, *supra* note 12, at 107–43. Retailers have adopted technologies for monitoring customers in stores and constructing unique shopper profiles which combine social characteristics, behaviors, and engagement with products to increase the likelihood of conversion—a sale or other desired action. *Id.* at 148–50.

[159] *See* Marc Vermut, *Why Omnichannel Is the Future of Retail for Millennials (and Everyone Else, Too)*, ADAGE (Sept. 27, 2018), https://adage.com/article/neustar/omnichannel-future-retail-millennials/315054/ [https://perma.cc/5AYG-BDST] (describing in a "publishing partner" article, in coordination with marketing intelligence brand Neustar, the potential of omnichannel to build a competitive advantage using data analytics gathered from various sources); *see also* Eric Nyquist, *How to Make the Most of Omnichannel Retailing*, HARV. BUS. REV., https://hbr.org/2016/07/how-to-make-the-most-of-omnichannel-retailing [https://perma.cc/3259-CYTM] (last visited Oct. 18, 2018) ("The more profitable play is to coax online shoppers to come into your stores, where the environment can induce them to spend more.").

[160] TUROW, *supra* note 12, at 108; *see also* Michael Corkery, *Hard Lessons (Thanks Amazon) Breathe New Life into Retail Stores*, N.Y. TIMES (Sept. 3, 2018), https://www.nytimes.com/2018/09/03/business/retail-walmart-amazon-economy.html [https://perma.cc/8RDN-TV3U].

[161] *See* Peter Messmer, *Why Is Identity Resolution so Valuable for Retailers with Physical Locations?*, ADDSHOPPERS (July 9, 2018), https://www.addshoppers.com/blog/why-is-identity-resolution-so-valuable-for-retailers-with-physical-locations [https://perma.cc/RF9P-JXWV].

into a single useful customer profile.[162] Efficiently solving issues of identity resolution efficiently is seen as a lucrative goal of various marketing services companies aimed at customizing customer interactions on a micro-level.[163]

Facial recognition is viewed as an important tool in the toolbox of "the future of shopping," with retailers already experimenting with its potential.[164] In 2015, Walmart tested a system that scanned the faces of all individuals entering several of its stores; the system could identify suspected shoplifters, and instantly alerted store security on their mobile devices.[165] Use of facial recognition is not limited to large national retailers, however.[166] In March of 2018, the ACLU reached out to twenty of the biggest stores in the United States to ask if they use facial recognition technology: the resulting report stated that "of the 20 companies . . . contacted, only one was willing to tell [the ACLU] that they don't use it."[167]

Many facial recognition products presently on the market focus on increasing security through automated facial recognition technology.[168] However, as some independent experts have noted, the technology may be less effective as a security measure for private businesses because they lack access to databases held by law enforcement agencies.[169] Rather, customer engagement and

---

162 *Id.*

163 *See generally* SIGNAL, THE FUTURE OF RETAIL: IDENTITY IS THE NEXT COMPETITIVE BATTLEGROUND (2017), https://cdn2.hubspot.net/hubfs/370829/ABM%20Retail%20Q2%202018/ABM_Q22018_Future-of-Retail_eBook-Digital_11Jun2018.pdf [https://perma.cc/AB3W-U4LB].

164 TUROW, *supra* note 12, at 227.

165 Jeff John Roberts, *Walmart's Use of Sci-Fi Tech to Spot Shoplifters Raises Privacy Questions*, FORTUNE (Nov. 9, 2015), http://fortune.com/2015/11/09/wal-mart-facial-recognition/ [https://perma.cc/ZF4E-ZB67].

166 Susan Campbell, *Local Stores Use Artificial Intelligence to Catch Shoplifters*, WPRI (Apr. 23, 2018, 6:02 PM), https://www.wpri.com/target-12/local-stores-use-artificial-intelligence-to-catch-shoplifters/1136106605 [https://perma.cc/J4XX-9W7S].

167 Bitar & Stanley, *supra* note 11.

168 *See* Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, N.Y. TIMES (Mar. 13, 2018), https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html [https://perma.cc/5A4A-LRBU].

169 Chris Frey, *Revealed: How Facial Recognition Has Invaded Shops—and Your Privacy*, GUARDIAN (Mar. 3, 2016), https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto [https://perma.cc/L48S-ETEF].

marketing capabilities of facial recognition are the projected valuable commodity for retailers.[170] Facial recognition as part of an omnichannel approach can track "all those aggregated bits of data collected through loyalty programs, point of sale records and other sources."[171]

Various products and services already exist in the market offering the utility of facial recognition to retailers.[172] FaceFirst, which is a major player in the field, offers a product and application programming interface (API) plug-in that allows for integrating face recognition into "virtually any third-party software."[173] Peter Trepp, the CEO of FaceFirst, told BuzzFeed News that "hundreds of [retail] locations, growing to thousands very soon" were incorporating the company's facial recognition system.[174] FaceFirst's software is designed to scan faces from a distance of fifty to one hundred feet.[175] As consumers enter a store, a CCTV camera captures multiple images of each shopper.[176] The software then analyzes that image and compares it to a database of "dishonest customers" provided by retailers or third-parties.[177] Other software developers have created technology allowing retailers to match consumer facial scans with a database of "valued customers," identifying their shopping profile.[178]

---

170 *Id.*

171 *Id.; see also* Sapna Maheshwari, *Stores See a Future Without "May I Help You?" (They'll Already Have Your Data),* N.Y. TIMES (Mar. 10, 2019), https://www.nytimes.com/2019/03/10/business/retail-stores-technology.html [https://perma.cc/Z8BF-PBN6] (discussing that through facial recognition "stores could send automatic text messages and receive theirs profiles to assist them better[,]" allowing stores to "immediately know customers' identities and personal preferences when they arrived").

172 *See, e.g.*, *Company Overview,* FACEFIRST, https://www.facefirst.com/ [https://perma.cc/GP2Y-HEZ5] (last visited Sept. 18, 2018).

173 *Sentinel-IQ Face Recognition Surveillance*, FACEFIRST, https://www.facefirst.com/solutions/surveillance-face-recognition/ [https://perma.cc/3JUS-8WHJ] (last visited Sept. 18, 2018).

174 Leticia Miranda, *Thousands of Stores Will Soon Use Facial Recognition, and They Don't Need Your Consent*, BUZZFEED NEWS (Aug. 17, 2018, 10:28 AM), https://www.buzzfeednews.com/article/leticiamiranda/retail-companies-are-testing-out-facial-recognition-at [https://perma.cc/5ZE5-A3AP].

175 *Id.*

176 *Id.*

177 *Id.*

178 Salinas, *supra* note 6.

Legal questions arise from the divergence of customers' expectations and the extent of information made available for collection and use through biometric facial recognition. Legal scholars have argued that there is no privacy in public,[179] and CCTV has been found not to violate any traditional privacy torts.[180] Many places that appear public, like retail establishments, are in fact privately owned, making visual surveillance difficult to avoid.[181] Private areas are often surveilled and it is difficult to argue that a face is truly private.[182] Even if consumers assume they will be under some form of video surveillance, facial recognition likely exceeds their expectations that store camera feeds are not actively monitored, and that if monitored, that the video footage is not used unless an altercation of some kind occurs.[183] Although biometric collection may enable new functionalities for retailers, the prospect of data being used for divergent purposes such as being shared or sold raises important legal questions.[184] It also exposes consumers to targeted advertising, by their faceprint being captured, retained, connected to their real-world identity, and combined with information about their income, education, demographics, and other data.

Biometric data collected and used by retailers presents unique problems to regulation. A consumer leaving his or her home and entering a brick-and-mortar retailer may be identified. The consumer may not even see the camera that captures their faceprint. He or she is likely unaware that their collected data is subject to the risk of breach or that their habits or demographics may be employed to deliver hyper-targeted advertising. There is little opportunity to clearly notify consumers and less to obtain consent, written or otherwise. Facial recognition facilitates and furthers the reach of a "collection imperative," extending and connecting the constant

---

179 *See, e.g.*, Heidi Reamer Anderson, *The Mythical Right to Obscurity: A Pragmatic Defense of No Privacy in Public*, 7 I/S J.L. & POL'Y FOR INFO. SOC'Y 543, 544 (2012).

180 *See* Robert D. Bickel, Susan Brinkley & Wendy White, *Seeing Past Privacy: Will the Development and Application of CCTV and Other Video Security Technology Compromise an Essential Constitutional Right in a Democracy or Will Courts Strike a Proper Balance?*, 33 STETSON L. REV. 299, 342–43 (2003).

181 COHEN, *supra* note 36, at 165–66.

182 *Id.*

183 Bitar & Stanley, *supra* note 11.

184 *Id.*

surveillance of networked devices to "real" space while increasing the value of the data collected.[185] The disproportionate power over information by private entities increases the potential for abuse. For this reason, legal scholars have called for an outright ban on the technology.[186] Consideration of these legal questions requires an understanding of how the United States addresses issues of consumer data privacy. The next Part discusses the current approach to consumer data privacy in the United States.

II. PUBLIC AND PRIVATE ORDERING

This Part explores present federal, state, and private sector approaches to privacy protections for consumer biometric information collected in commercial settings. Section II.A discusses existing state privacy statutes that recognize individual-rights in facial recognition information as well as recent litigation trends. Section II.B describes the sectoral approach to federal privacy statutes and the absence of individual rights at the federal level. Section II.C then explain a managerial approach through the FTC's authority under Section 5 to take enforcement action against companies that engage in unfair or deceptive trade practices and the goals of facilitating self-regulation. Finally, Section II.D describes a multi-stakeholder approach employed by the National Telecommunications and Information Administration (NTIA) to develop industry-wide facial recognition standards.

A. State Legislation

At the state level, there is some movement towards regulating biometric data, including facial recognition. States have followed differing strategies in addressing the issues of biometric data. Connecticut, Iowa, Nebraska, North Carolina, Oregon, Wisconsin, and Wyoming have included biometric information in their statutory definitions of "personal information" in data security breach

---

185 *See* Danielle Keats Citron, *A Poor Mother's Right to Privacy*, 98 B.U.L. REV. 1139, 1141 (2018); *See also* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 87 (2019) (discussing a similar notion of the "extraction imperative").

186 Hartzog & Selinger, *supra* note 10.

notification laws.[187] Other states, including New York, Connecticut, and Alaska, have proposed legislation seeking to regulate biometric data, but have yet to enact legislation.[188]

Only three states have enacted statutes directly governing biometric information privacy.[189] In 2009, Texas enacted a statute governing biometric information: the "Capture or Use of Biometric Identifier" (CUBI).[190] CUBI permits collection of biometrics for a commercial purpose based on informed consent, as well as for the sale or disclosure of biometric data under certain limited circumstances.[191] CUBI does not provide a private right of action, but the Texas Attorney General can bring an action to recover against a company for up to $25,000 per violation.[192]

In 2017, Washington enacted legislation applicable to biometrics.[193] The Washington law includes a broad definition of biometric identifiers, including any "data generated by automatic measurements of an individual's biological characteristics . . . that is used to identify a specific individual."[194] Companies are required to provide notice of collection for a commercial purpose, and, to obtain consent.[195] The law's text states that consent is "context-dependent."[196] The Washington and Texas laws, while generating

---

187 *See* Daveante Jones, *Protecting Biometric Information in Arkansas*, 69 ARK. L. REV. 117, 132 (2016) (quoting Phil Ross, *Biometrics: A Developing Regulatory Landscape for a New Era of Technology*, GENOMICS L. REP. (2014), http://www.genomicslawreport.com/index.php/2014/05/21/biometrics-a-developing-regulatory-landscape-for-a-new-era-of-technology [https://perma.cc/WEV4-PW23]).

188 John T. Wolak, Mitchell Boyarsky & Randy A. Gray, *The Biometric Standards: How New York Measures Up in the Face of Biometric Use Regulations*, N.Y.L.J. (June 1, 2018, 3:10 PM), https://www.law.com/newyorklawjournal/2018/06/01/the-biometric-standard-how-new-york-measures-up-with-regulations/?slreturn=20180825134641 [https://perma.cc/TB2Q-9FZ7]; *see also* N.Y. Assemb. A9793, 2017–18 Leg. Sess. (2018) (replicating the language of Illinois BIPA); H.B. 5522, 2017 Leg. (Conn. 2017) (prohibiting "retailers from using facial recognition software for marketing purposes").

189 Hannah Zimmerman, *The Data of You: Regulating Private Industry's Collection of Biometric Information*, 66 U. KAN. L. REV. 637, 648 (2018).

190 TEX. BUS. & COM. CODE § 503.001 (2009).

191 *Id.*

192 *Id.*

193 WASH. REV. CODE § 19.375.010 (2017).

194 *Id.* § 19.375.010(1).

195 *Id.* § 19.375.010(2).

196 *Id.*

new corporate compliance objects, have been described as "lack[ing] teeth," as they do not include a private right of action and have not resulted in enforcement by attorneys general.[197]

The main source of recent biometrics lawsuits is the Illinois Biometric Information Privacy Act of 2008 (BIPA).[198] While BIPA was enacted over ten years ago, over the past two years there has been a marked increase in the quantity of BIPA lawsuits, with plaintiffs suing more than thirty companies across a range of industries, including large tech companies Google and Facebook, for alleged violations.[199] BIPA regulates the collection, use, and storage of biometric information by private entities, covering "biometric identifiers"—including "face geometry"—which covers information created through the facial recognition process.[200] Under BIPA, before collecting biometric information, any private entity must provide the individual with notice that the information is being collected, including the duration of the period for which the information will stored, and used; the individual must also consent through a written release.[201] Biometric information must be destroyed when the initial purpose for collecting the information has been satisfied, or within three years of the individual's last interaction with the private entity.[202]

BIPA, like the Washington and Texas laws, relies on a notice-and-choice framework.[203] This approach originates from FTC privacy policy guidance.[204] Notice requires that consumers be given "clear and conspicuous notice of an entity's information before any personal information is collected from them."[205] Choice requires

---

197 Paul Shukovsky, *Washington Biometric Privacy Law Lacks Teeth of Illinois Cousin*, BLOOMBERG: BNA (July 18, 2018), https://www.bna.com/washington-biometric-privacy-n73014461920/ [https://perma.cc/3PQH-92SL].

198 Charles N. Insler, *Understanding the Biometric Information Privacy Act Litigation Explosion*, 106 ILL. B.J. 34, 35 (2018).

199 *Id.*

200 740 ILL. COMP. STAT. 14/10 (2008).

201 *Id.*

202 740 ILL. COMP. STAT. 14/15 (2008).

203 *See, e.g.*, 740 ILL. COMP. STAT. 14/15(d) (2008).

204 Joel R. Reidenberg et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 J.L. INFO. POL'Y 485, 489 (2015).

205 FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 14 (2000), https://www.ftc.gov

"giving consumers options as to how any personal information collected from them may be used . . . beyond those necessary to complete a contemplated transaction."[206] As discussed infra, there is debate among scholars as to whether this approach is workable.[207] Under BIPA, failure to provide notice-and-choice can subject a company to a private right of action, with recovery of up to the greater of actual damages or $5,000 per reckless violation.[208] Private litigants can also recover attorney fees, costs (including expert fees and litigation expenses), and additional relief at the discretion of the court.[209] Negligent violations of the statute permit recovery of the greater of actual damages or $1,000 per violation.[210] BIPA sets a high standard for corporate compliance, with the requirement for written consent having been described as "really, really burdensome."[211] This, however, has not limited plaintiffs from bringing suit alleging violations of BIPA.

Most suits have focused on BIPA's notice-and-consent requirement.[212] The main hurdle for the sustainability of lawsuits under BIPA has been alleging harm to confer standing following *Spokeo v. Robbins*,[213] which requires a plaintiff to allege an injury-in-fact that is both concrete and particularized.[214] In a class action suit, the plaintiffs in *Patel v. Facebook*,[215] alleged that Facebook unlawfully collected and stored biometric data derived from their faces. A district court in California found that a state statute could establish standing in federal court for an alleged privacy harm.[216]

/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf [https://perma.cc/YP2R-9PZS].

206 *Id.* at 15.

207 *See generally* Reidenberg, *supra* note 203.

208 740 ILL. COMP. STAT. 14/20 (2008).

209 *Id.*

210 740 ILL. COMP. STAT. 14/15(1).

211 Shukovsky, *supra* note 196.

212 *See, e.g.*, Rosenbach v. Six Flags Entertainment, 2017 WL 6523910, at *7 (Ill. App. Ct. 2017).

213 136 S. Ct. 1540 (2016).

214 For a discussion of the implications of *Spokeo* for alleging privacy harms see Mathew DeLuca, *The Hunt for Privacy Harms After* Spokeo, 86 FORDHAM L. REV. 2439 (2018).

215 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018) (cases consolidated at *In re Facebook Biometric Information Privacy Litig.*, No. 15-03747 (N.D. Cal. 2018)).

216 *Id.* at 953.

The court found that "provisions [of BIPA], along with the plain text of BIPA as a whole, leave little question that the Illinois legislature codified a right of privacy in personal biometric information."[217] However, cases in Illinois federal court have found plaintiffs did not demonstrate "concrete injuries" that violated a statutory right.[218]

The fate of recent BIPA cases is yet to be determined.[219] The still-pending lawsuits demonstrate the possible implications of a verdict, specifically for Facebook, which could lead to damages in the billions of dollars.[220] Finding liability for companies like Facebook under BIPA would shift the trend away from unsuccessful consumer lawsuits against large corporations for privacy related activities that do not include data breach.[221] Additionally, various states with proposed BIPA-style private action legislation will be interested in the outcome.[222] The effects of a verdict against

---

[217] *Id.* This interpretation was affirmed at the state level by the Illinois Supreme Court in Rosenbach v. Six Flags, 2019 IL 123186 (2019).

[218] *See, e.g.*, Matthew Boesler, *Google Wins Dismissal of Suit Over Facial Recognition Software*, BLOOMBERG (Dec. 29, 2018, 2:57 PM), https://www.bloomberg.com/news/articles/2018-12-29/google-wins-dismissal-of-suit-over-facial-recognition-software-jq9w1mws [https://perma.cc/FJN9-C68F].

[219] The status of challenges to standing under BIPA have been complicated by the Supreme Court of Illinois in Rosenbach v. Six Flags, 2019 IL 123186 (2019) finding that the construction and "unambiguous" language of the statute confer standing to sue in the absence of a breach in contradiction of Illinois federal courts interpretations of the requirements of *Spokeo*. *See, e.g.*, McGinnis v. United States Cold Storage, Inc., No. 17 C 08054, 2019 WL 95154, at *1 (N.D. Ill. Jan. 3, 2019).

[220] Joel Rosenblatt, *Facebook Photo-Scanning Suit Is a Multibillion-Dollar Threat*, BLOOMBERG (Apr. 16, 2018, 10:06 PM), https://www.bloomberg.com/news/articles/2018-04-16/facebook-must-face-group-suit-claiming-it-stole-biometric-data [https://perma.cc/T9DP-76N4].

[221] *See, e.g.*, Joel Rosenblatt, *Facebook Users Can't Sue as a Group Over Advertisers' Data Use*, BLOOMBERG (Sept. 2, 2016, 9:21 PM), https://www.bloomberg.com/news/articles/2016-09-02/facebook-users-ruled-too-varied-to-pursue-group-privacy-lawsuit [https://perma.cc/MW55-Z3GR].

[222] Torsten M. Kracht et al., *Biometric Information Protection: The Stage Is Set for Expansion of Claims*, LEXIS NEXIS (Feb. 28, 2018), https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/archive/2018/02/28/biometric-information-protection-the-stage-is-set-for-expansion-of-claims.aspx [https://perma.cc/2WL4-LYKW] (noting that Michigan, New Hampshire, Alaska, and Montana have proposed biometric legislation that includes a private right of action for violations). Additionally, California passed a sweeping consumer privacy law with the potential to rework compliance regimes across a variety of sectors including retail use of biometrics. Dipayan Ghosh, *What You Need to Know About California's New Data Privacy Law*, HARV. BUS. REV. (July 11, 2018),

Facebook could be dramatic, "caus[ing] other companies to think they could be subject to [] massive damages."[223] Similarly, class action plaintiffs' lawyers are likely to ramp up BIPA related litigation as more companies begin to use the technology.[224] This may serve as a significant financial incentive to compliance with biometric statutes, or discontinuance of the technique altogether.[225] As this Note discusses below, regulation that functionally prevents use of a technology removes any consumer choice and may be disproportionate to the privacy harm of the regulated activity.[226] Present state law, while trending towards the inclusion of some protections of biometric data, has not yet defined a clear set of practical norms or expressed a preference for private litigation or public enforcement.

B. Federal Legislation

Federal privacy law in the United States follows a sectoral approach, where a patchwork of statutes regulate different industries and economic sectors.[227] This approach differs from many other industrialized nations, where a centralized "omnibus" statute protects all personal data.[228] Under federal law, statutes differentiate between specific types of data and the context of that data's collection or use.[229] For example, financial data is regulated through

---

https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law [https://perma.cc/8SRJ-HCLU].

[223] Ben Kochman, *5 Cybersecurity and Privacy Cases to Watch: Midyear Report*, LAW360 (July 30, 2018, 8:24 PM), https://www.law360.com/articles/1067733/5-cybersecurity-and-privacy-cases-to-watch-midyear-report [https://perma.cc/7469-8RLL].

[224] Steven Grimes & Eric Shinabarger, *Biometric Privacy Litigation: The Next Class Action Battleground*, BLOOMBERG L.: BIG L. BUS. (Jan. 17, 2018), https://biglawbusiness.com/biometric-privacy-litigation-the-next-class-action-battleground/ [https://perma.cc/X5B9-XX6C].

[225] *Cf.* Ally Marotti, *Google's Art Selfies Aren't in Illinois. Here's Why*, CHICAGO TRIB. (Jan. 17, 2018, 7:00 AM), http://www.chicagotribune.com/business/ct-biz-google-art-selfies-20180116-story.html [https://perma.cc/AA2N-6HA2] (discussing how Google does not offer specific features and products in Illinois in response to the requirements and litigation risk of BIPA).

[226] *See also id.*

[227] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014).

[228] *Id.*

[229] *See id.* ("There is a law for video records and a different law for cable records.").

the Fair Credit Reporting Act (FCRA), which protects the privacy of credit information and prescribes reporting requirements for credit companies,[230] and the Gramm-Leach-Bliley Act (GLBA), which applies to companies that provide financial products.[231] Different laws regulate medical information, such the Health Insurance Portability and Accountability Act (HIPAA),[232] which protects the privacy of health data.

The sectoral approach leaves large areas unregulated, with no federal law that directly protects the privacy of data collected by retailers such as Macy's or Amazon.[233] As a result, there is no federal statute that specifically regulates biometrics in the private sector.[234] In the absence of a federal statute regulating the general collection of consumer data, the large quantities of data collected by biometric facial recognition will be addressed at the state level or through regulatory agencies.[235] The apparent downside of the sectoral approach, as opposed to an omnibus approach, is that the regulations are context-specific and may not address specific types of data such as biometrics.[236] The sectoral approach may be advantageous, however, as it avoids federal preemption, incentivizes narrowly tailored legislative strategies, and allows for organic development of regulatory tactics for emerging technologies.[237]

C. Federal Trade Commission

The Federal Trade Commission (FTC) has played a central role in regulating consumer data.[238] In 1914, Congress created the FTC through the Federal Trade Commission Act (FTCA) to protect

---

230 15 U.S.C. § 1681 (2012).

231 15 U.S.C. §§ 6801–09, 6821–27.

232 Pub L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, 42 U.S.C.).

233 Solove & Hartzog, *supra* note 226, at 587.

234 Michael Monajemi, *Privacy Regulation in the Age of Biometrics that Deal with the New World Order of Information*, 25 U. MIAMI INT'L & COMP. L. REV. 371, 397 (2018).

235 *Id.*

236 *Id.*

237 *See generally* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2009).

238 Solove & Hartzog, *supra* note 226, at 585.

consumers and promote competition.[239] Section 5 of the FTCA authorizes the FTC to identify, and enforce against, "unfair or deceptive acts or practices" that affect commerce.[240] In the absence of a federal law that directly protects the privacy of biometric data collected and used by retailers the FTC may regulate under its Section 5 authority.[241]

The FTC has largely focused its approach to privacy interests on its "deceptiveness authority," bringing actions against companies found to mislead consumers on control or collection of user data.[242] The FTC may regulate retailers based on representations in their privacy policies. However, this approach is of limited utility for biometrics in retail settings as the FTC cannot mandate that companies have privacy policies, privacy policies have inherent incentives for vagueness, and biometric collection and use is remote and often facilitated by third parties with no direct relationship with consumers. Where companies do not make privacy policy misrepresentations, the FTC may bring regulatory adjudication under its "unfairness" jurisdiction.

Under the FTCA, the FTC can declare an act or practice to be "unfair" if it: (1) "causes or is likely to cause substantial injury to customers;" (2) the injury "is not reasonably avoidable by consumers themselves;" and (3) the injury is "not outweighed by countervailing benefits to consumers or competition."[243] Additionally, Section 45(n) clarifies that "the [FTC] may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination."[244] The FTC's policy statement on unfair practices suggests that the extent to which a

---

239 *Id.* at 598.

240 FEDERAL TRADE COMMISSION ACT SECTION 5: UNFAIR OR DECEPTIVE ACTS OR PRACTICES, FED. RESERVE (2016), https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf [https://perma.cc/6948-RL96].

241 *Id.* at 587.

242 *See, e.g.*, Press Release, Federal Trade Commission, FTC Approves Final Order in Nomi Technologies Case (Sept. 3, 2015), https://www.ftc.gov/news-events/press-releases/2015/09/ftc-approves-final-order-nomi-technologies-case [https://perma.cc/FTJ7-RSYL].

243 15 U.S.C. §§ 45(a), (n) (2012).

244 15 U.S.C. § 45(n).

practice violates recognized public policy, is "unethical or unscrupulous," as well as whether consumers suffer substantial injury that is not "outweighed by any offsetting consumer or competitive benefits" and "which consumers could not reasonably have avoided" are all relevant in assessing the unfairness of a practice.[245] The FTC has stated that "[a]n injury may be sufficiently substantial . . . if it does a small harm to a large number of people, or if it raises a significant risk of concrete harm."[246]

The FTC has limited substantive Magnuson-Moss rulemaking authority under the FTCA, however, the restrictive procedural requirements of this approach make it functionally ineffective.[247] Courts have recognized that the FTC may use adjudication for regulating activities that relate to privacy.[248] With the emergence of internet commerce and new networked technologies, the FTC's main role has been as a "backstop" to industry promulgated self-regulatory regimes.[249] The FTC's actions in the privacy space have been constrained, bringing only cases with a high likelihood of success, and settling the vast majority of cases.[250] Hartzog and Solove argue that the FTC therefore essentially acts as a norm setting body, incrementally developing a body of law through complaints and settlements that then serve as pseudo-precedent for practitioners.[251]

The FTC's norm-setting "soft law" function is solidified by its issuing of interpretive statements, policy guidance, and press releases.[252] In 2012 the FTC issued a staff report following public comment on private sector use of facial recognition technology.[253] The FTC suggests that private actors should follow approaches that

---

245 Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1432–33 (2017).

246 FED TRADE COMM'N, COMM'N STATEMENT OF POLICY ON THE SCOPE OF THE CONSUMER UNFAIRNESS JURISDICTION (1980), *as reprinted in* Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984).

247 Solove & Hartzog, *supra* note 226, at 620–21.

248 *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 246 (3d Cir. 2015).

249 Solove & Hartzog, *supra* note 226, at 598–99.

250 *Id.* at 613.

251 *Id.* at 620.

252 *Id.* at 625.

253 *See generally* FED. TRADE COMM'N, *supra* note 50.

"implement privacy by design," "simplify consumer choice," and emphasize "transparen[cy]."[254] While this approach provides an additional emphasis on data security, it fundamentally mirrors the notice-and-choice regimes used in other FTC regulation.[255] As discussed below, a notice-and-choice framework remains tenuous for biometric data collection. Notably, FTC Commissioner Rosch dissented from the 2012 staff report.[256] He emphasized that no harm occurred with the collection and use of biometrics as "[t]here is nothing to establish that this misconduct has occurred or even that it is likely to occur in the near future."[257] The FTC has never clearly articulated which parts of its recommendations are mandatory and which parts are best practices.[258] Against a backdrop of shifting metrics of substantial consumer harm, it remains unclear what is the appropriate amount of protection that should be provided to this data.

D. NTIA Multistakeholder Process

In December of 2013 the National Telecommunications and Information Administration (NTIA) announced that it would convene a multistakeholder process regarding the commercial use—specifically use in retail—of facial recognition technology starting in early 2014.[259] The goal of the process was to "develop a voluntary, enforceable code of conduct that . . . applies to facial recognition technology."[260] The NTIA referenced work by the FTC, industry organizations, and scholars suggesting "that the facial recognition topic is a strong opportunity for stakeholders to reach consensus on a code of conduct in a reasonable timeframe."[261] However, after several meetings consumer privacy advocates

---

254 *Id.*

255 *See, e.g.*, FED. TRADE COMM'N, *supra* note 204, at 14.

256 FED. TRADE COMM'N, *supra* note 50, at A2 (Dissenting Opinion of Commissioner J. Thomas Rosch).

257 *Id.*

258 Solove & Hartzog, *supra* note 226, at 626.

259 NAT'L TELECOMM. & INFO. ADMIN., PRIVACY MULTISTAKEHOLDER MEETINGS REGARDING FACIAL RECOGNITION TECHNOLOGY: FEBRUARY–JUNE 2014 (2013), https://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-meetings-regarding-facial-recognition-technology-feb [https://perma.cc/7E4W-SRMM].

260 *Id.*

261 *Id.*

withdrew from the proceedings, citing a lack of guidance for business or protection of individuals under a standard of enforceability of "encouragement" rather than "requirement" for any adopted standards.[262] The NTIA ultimately published a consensus document of the remaining stakeholders.[263] While the utility of the finalized NTIA standards remains unclear,[264] its results inform policy discussions on voluntary self-regulation of private sector facial recognition.[265] The tension between consumer anxiety and the value of facial recognition to industry suggests that regulatory action may be necessary to set boundaries of permissible collection and usage. The following Part compares approaches from Illinois state law with the utility of the FTC's present "unfair and deceptive practices" norm-setting regime under Section 5.

III. "THE FULL RAMIFICATIONS OF BIOMETRIC TECHNOLOGY ARE NOT FULLY KNOWN"[266]

This Part considers the availability and shortcomings of current regulatory approaches for emerging facial recognition technologies. This Part first evaluates the potential of an individual rights regime, where public law recognizes a new right in individuals to informational privacy, limiting how biometric information may be collected and creating a right of action to enforce the right. Using the example of Illinois' BIPA regime as a model of this approach, Section III.A considers the autonomy value of this approach, but also discusses the inherent problems with individual rights as a way

---

262 Press Release, Consumer Federation of America, Statement on NTIA Privacy Best Practices Recommendations for Commercial Recognition Use (June 15, 2016), https://consumerfed.org/press_release/statement-ntia-privacy-best-practice-recommendations-commercial-facial-recognition-use/ [https://perma.cc/B9RX-9Q95].

263 *Id*.

264 *See NTIA Facial Recognition Best Practice Guidelines Meet Mixed Reception*, BIOMETRIC TECH. TODAY at 1 (2016).

265 Additionally, it is worth considering what the regulatory validity of a document issued through a multistakeholder process is after the withdrawal of stakeholders. For a more in-depth discussion of the implications of multistakeholder processes and techno-policy see generally Nick Doty & Deirdre K. Mulligan, *Internet Multistakeholder Processes and Techno-Policy Standards*, 11 J. TELECOMM. & HIGH TECH. L. 135 (2013).

266 740 ILL. COMP. STAT. 14/5(g) (2008).

to regulate complex systems out of a widening information gap between consumers and private actors. This Section concludes that individual rights can serve only as a limited tool for fixing a system-wide problem, because rights-bearing individuals and the statutory basis of those rights suffer from technical, behavioral, judicial expertise, and economic limitations. Section III.B then considers the potential of an FTC managerial regime, in which a regulatory "light touch" serves as a backstop to industry self-regulation. This Section finds that while the managerial regime benefits from the flexibility to develop policy gradually in response to rapidly changing technology, the present emphasis on user control may be ineffective when dealing with the unique issues presented by facial recognition. Finally, Section III.C considers the problems of the present incentive structures and market failures of self-regulatory regimes that may impede the development of an effective collaborative governance regime.

A. The Problems of Statutory Individual-Rights

To understand what individual-rights in information are created by biometric statutes, it is helpful to understand the history of BIPA's enactment following the failure of the startup, Pay By Touch. In the early 2000s, Pay By Touch promised to "change the way the world pays" with a biometric authentication and payment system.[267] The system enabled consumers to link various accounts (credit cards, checking accounts, loyalty programs, etc.) to their fingerprints, and then access those accounts or make payments with the touch of a finger, rather than by using cash or swiping a card.[268] However, when Pay by Touch filed for bankruptcy in 2007 its primary asset was an extensive collection of consumer fingerprints.[269] BIPA was introduced into the Illinois Senate in

---

[267] Blaire Briody, *We're Getting Closer Than Ever to Paying with Our Fingerprints*, BUS. INSIDER (Feb. 28, 2013, 4:22 PM), https://www.businessinsider.com/forget-credit-cards-2013-2 [https://perma.cc/HR52-VJY5].

[268] Shubha, *Failure Story: What Happened to Pay By Touch?*, LET'S TALK PAYMENTS (Apr. 20, 2015), https://letstalkpayments.com/failure-story-what-happened-to-pay-by-touch/ [https://perma.cc/2WDV-FZ3F].

[269] *See* Lucy L. Thomson, *Sensitive Personal Data for Sale in Bankruptcy—An Uncertain Future for Privacy Protection*, 2017 ANN. SURV. BANKR. L. 12 (2017). The history of the rise and fall of Pay By Touch is a fascinating story of a freewheeling, overfunded and

February 2008.[270] During hearings on the bill in the Illinois House, Representative Kathy Ryg directly referenced the Pay By Touch bankruptcy, noting that it left "thousands of customers . . . wondering what will become of their biometric and financial data."[271] When the Illinois legislature passed BIPA, this sentiment was incorporated into the law's preamble,[272] emphasizing that the law targeted future harms that may arise from the use of the technology and stating that the "full ramifications of biometric technology are not fully known."[273]

While there was uncertainty surrounding the fate of data maintained by Pay By Touch, in 2008, the harms the Illinois Legislature addressed where predominantly speculative or based in perceived discomforts.[274] In the absence of specific harm to address, BIPA's approach codified an arguably arduous notice-and-choice regime requiring written consent. This was not the first occurrence of media coverage resulting in a reactive public law to address a nascent problem.[275] However, passing laws based on technological potentialities risks miscalculating the harms and benefits of emerging technology, impeding development and creating disproportionate compliance costs.[276]

---

under-supervised start up, for more information see Lance Williams, *How 'Visionary' Raised – and Lost – a Fortune*, SFGATE (Dec. 7, 2008, 4:00 AM), https://www.sfgate.com/news/article/How-visionary-raised-and-lost-a-fortune-3181454.php [https://perma.cc/U2BD-SN9C].

270 Insler, *supra* note 197, at 35.

271 95th ILL. GEN. ASSEM., H. PROCEEDINGS, at 249 (May 30, 2008) (statement of Representative Ryg). It is worth noting that Representative Ryg's singular statement represents the dearth of any legislative discussion prior to the bill's passage.

272 740 ILL. COMP. STAT. 14/5(d) (2008) ("An overwhelming majority of members of the public are wary of the use of biometrics when such information is tied to finances and other personal information.").

273 § 14/5(f).

274 *See* Elvy, *supra* note 65, at 432; *see also* Citron, *supra* note 11, at 250.

275 *See generally* CASS SUNSTEIN, LAWS OF FEAR: BEYOND THE PRECAUTIONARY PRINCIPLE 1–5, 35–61 (2005) (arguing that fear-based lawmaking is faulty because fear is inherently faulty).

276 *See* Cary Coglianese et al., *Seeking Truth For Power: Informational Strategy and Regulatory Policymaking*, 89 MINN. L. REV. 277, 284 (2004).

This Section analyzes the implications of BIPA and potential individual-rights models for regulating facial recognition.[277] This Section starts by considering whether a rights-based statutory regime grounded in notice-and-choice appropriately protects privacy interests for emerging technologies. This Section then discusses the problem of statutory ossification, where static law fails to address how a unique technology develops and changes. Finally, this Section addresses the limitations of legislative reactions to consumer sensitivities in emerging technologies.

1. Notice-and-Choice as an Ineffective Approach in Biometric Statutes

BIPA requires that companies collecting biometric information provide notice to consumers, so they may choose to opt-out from the activity where collection occurs.[278] This regime, however, is ineffective at protecting consumers from the privacy harms associated with facial recognition.

Notice-and-choice in American law is based in the Fair Information Practice Principles (FIPPs). The FIPPs are a self-regulatory regime promulgated by the FTC, requiring corporations to provide consumers with "notice," "choice," "access," and "security."[279] The FIPPs of "notice" and "choice" have become the backbone of the federal and state self-regulatory approach since their introduction in 1973.[280] However, the resilience of the FIPPs as a method for lawmakers to implement concepts of control, notice, and consent to protect privacy may suggest limitations in lawmakers abilities to conceptualize privacy—valuing libertarian notions of autonomy over consumer protection.[281]

---

[277] While the Washington and Texas law may provide some clarification on alternate legislative approaches, this Note views BIPA as the most significant approach, because of its provision including a consumer right of action, pending litigation, and that states like New York have legislation in committee which directly replicates its language and scope.

[278] See *supra* Section II.A

[279] FED. TRADE COMM'N, *supra* note 204.

[280] John A. Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (Or Anywhere Else)*, 66 CLEV. ST. L. REV. 559, 585 (2018).

[281] *See* HARTZOG, *supra* note 95, at 60–61.

The current regulatory regime presumes that when companies provide accurate information to consumers, consumers will make an informed choice to accept or reject the service, allowing effective self-regulation.[282] The FTC has identified "notice" as "[t]he most fundamental principle."[283] Accordingly, privacy policies—the mechanism for providing notice—are essential to this model.[284] However, privacy policies are generally non-contractually enforceable[285] statements of companies data practices, which are supposed to inform consumers what information platforms collect, how and for what purpose they collect it, and with whom they share it.[286] This approach assumes that consumers then will have the opportunity to opt out of the service, avoiding any collection of their data.[287] Proponents argue that notice-and-choice is an effective substitute for regulations because it is more flexible, inexpensive to implement, and easy to enforce.[288] A wide range of legal critics suggest that in practice, this approach is ineffective because, no one reads privacy policies[289] they are often long,[290] difficult to understand,[291] use legal jargon inaccessible to the average consumer,[292] and even privacy experts finding them misleading.[293]

---

[282] Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39, 41 (2015).

[283] *See* Reidenberg et al., *supra* note 204, at 489 (2015).

[284] *See* Solove & Hartzog, *supra* note 226, at 594.

[285] *See* 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, 189–90 (2016) (discussing that individual consumers cannot sue for breach of contract based on privacy policies because courts do not find cognizable harm that is required in a contract claim).

[286] Solove & Hartzog, *supra* note 226, at 592.

[287] *Id.* at 592.

[288] Reidenberg et al., *supra* note 204, at 489.

[289] *See, e.g.*, George R. Milne & Mary J. Culnan, *Strategies For Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices*, 18 J. INTERACTIVE MARKETING 15 (2004).

[290] *See, e.g.*, T.J. Ortenzi, *Facebook Privacy Policy Explained: It's Longer than the Constitution*, HUFFINGTON POST (May 25, 2011), https://www.huffingtonpost.com/2010/05/12/facebook-privacy-policy-s_n_574389.html [https://perma.cc/7JLH-ZXA2].

[291] Reidenberg et al., *supra* note 204, at 491.

[292] *Id.* at 491.

[293] Reidenberg et al., *supra* note 281, at 87–88.

In a 2014 report on big data, the U.S. President's Council of Advisors on Science and Technology stated that "the framework of notice and consent is also becoming unworkable as a useful foundation for policy."[294] Woodrow Hartzog emphasizes that at best the notice-and-choice model of individual "control" is an illusion.[295] This result stems from an inherent power imbalance between uninformed consumers and companies capable of using adversarial design choices that wear down consumer resistance, manufacturing permissive consumer consent.[296] Such an imbalance results in a lack of ability for meaningful privacy self-management, where individuals can do very little to effectuate their preferences.[297] This is not a new realization.[298] Ultimately, notice-and-choice may be an unworkable model for consumer control and self-management of data collection practices.

The collection of facial recognition biometrics by retailers is uniquely problematic under a notice-and-choice regime. Use of facial recognition for identity verification or payment systems typically involves use of an application or preregistration of an account on a website.[299] Upon downloading a required application, the collection of facial recognition for identity verification can

---

294 PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH. REPORT TO THE PRESIDENT, BIG DATA AND PRIVACY: A TECH. PERSPECTIVE (May 2014).

295 HARTZOG, *supra* note 95, at 64.

296 *Id.* at 64–67.

297 *See generally* Daniel Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013). In part, this is because the dominant model offered by civil society organizations for individuals to push back against mass data collection advances an individualized understanding of resistance in which the onus is on the individual to change their behavior. This means that challenging data collection becomes an individualized act based on perceived skill and ability to engage in privacy-enhancing digital practices, such as downloading encrypted software, using anonymized browsers, and changing security settings. Lobbying for policy reform and engaging in litigation activism, meanwhile, is often bounded by technical and issue-specific expertise that confines the debate to a small constituency of experts. *See* Arne Hintz & Ian Brown, *Enabling Digital Citizenship? The Reshaping of Surveillance Policy After Snowden*, 11 INT'L J. COMM'N 782, 796 (2017).

298 In 1967, Arthur R. Miller presciently warned a Senate subcommittee that "[e]xcessive reliance should not be placed on what too often is viewed as a universal solvent—the concept of consent." Hearings Before the Subcomm. on Admin. Practice and Procedure of the S. Comm. on the Judiciary, 90th Cong., First Session 78 (1967).

299 BIPA defines "Written release" as "informed written consent." 740 ILL. COMP. STAT. 14/10 (2008).

readily be incorporated into a browse-wrap privacy policy,[300] or in the case of BIPA's more rigorous written consent requirement,[301] a clickwrap agreement.[302] While courts have not articulated if a browsewrap agreement could satisfy BIPA,[303] in litigation on whether clickwrap satisfies BIPA's notice and consent, courts appear to suggest that a clickwrap agreement will satisfy BIPA's written notice and consent requirement.[304] Given the asymmetry of information between corporations and consumers it is unlikely that consumer control through BIPA's individual-rights will accomplish more than increased corporate reliance on contractual terms that are adhesive in practice.[305]

The higher degree of consumer awareness of the technology's use may alleviate some privacy risk of collection, but the lack of restrictions on "function creep"[306] likely results in situations where

---

[300] Browsewrap agreements are visible on a separate webpage accessible via a hyperlink on the main webpage; a website user may click that link to visit, view, and read the site's terms. *See* Ian Rambarran & Robert Hunt, *Are Browse-Wrap Agreements All They Are Wrapped Up to Be?*, 9 TUL. J. TECH. & INTELL. PROP. 173, 174 (2007).

[301] *See supra* Section II.A.

[302] Under the clickwrap model, a website or application presents a user with the applicable terms and requires that the user assent to those terms by clicking an icon. *See* Norton, *supra* note 284, at 191.

[303] *See, e.g.*, Patel v. Facebook, Inc., 290 F. Supp. 3d 948, 954–56 (N.D. Cal. 2018).

[304] *See, e.g.*, In re Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1166–67 (N.D. Cal. 2016) (finding that plaintiffs agreed to the user agreement through a clickwrap that stated "I have read and understood the Terms of Use, and I agree to them," for choice of law purposes and allowing claim to proceed); *see also* Vigil v. Take-Two Interactive Software, Inc., 235 F. Supp. 3d 499, 505–07, 510 (S.D.N.Y. 2007) *aff'd in part, vacated in part, remanded sub nom. Santana v. Take-Two Interactive Software Inc.*, 717 F. App'x 12 (2d Cir. 2017).

[305] For an interesting discussion on the question of whether the nature of a contract of adhesion creates a duty in the corporation to avoid harming the consumer as an information fiduciary see Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS. L. REV. 1183 (2016) (discussing the concept of fiduciary "duties of trust" for information collectors); *see also* Danielle Keats Citron, *Big Data Brokers as Fiduciaries*, CONCURRING OPINIONS (June 19, 2012), https://concurringopinions.com/archives/2012/06/big-data-brokers-as-fiduciaries.html [https://perma.cc/5VMZ-65CH] (discussing the use of fiduciary law to address the imbalance between consumers and corporations).

[306] A "function creep" occurs when "databases created for one discrete purpose, despite the initial promises of their creators, eventually take on new functions and purposes." Tania Simoncelli & Barry Steinhardt, *California's Proposition 69: A Dangerous Precedent for Criminal DNA Databases*, 33 J.L. MED. & ETHICS 279, 283 (2005); *see also* BRETT

consumer expectations do not match the scope of how consumer information will be used. Given movement to an omnichannel approach by retailers, consumers may provide consent to facial recognition for purposes of the statute by agreeing to clickwrap terms while using retailer website or applications.

Surveillance is additionally problematic under a rights-based regime. A main selling point of using facial recognition for remote surveillance is its "frictionless" ability to collect information without consumer awareness.[307] Using facial recognition in retail settings complicates how a notice-and-choice regime could work effectively. Any posted notice would likely be ignored, and there is no practical way to obtain written consent that would not be unduly burdensome on a retailer.[308] While it has not been litigated, under a biometric statute like Washington's that does not require written consent, entry into a location with a clearly posted notice stating "warning by entering into this store you may be subjected to facial recognition" could qualify as consent.[309]

The lack of clear obligations creates uncertain liabilities, resulting in a lose-lose situation where, due to information asymmetries, consumers readily negotiate away their privacy entitlements or businesses avoiding using the technology altogether.[310] While it is debatable where the latter result is

---

FRISCHMANN & EVAN SELINGER, RE-ENGINEERING HUMANITY 20–21 (2018) (discussing "surveillance creep").

[307] *See, e.g.*, *The Frictionless Future of Face Recognition*, NEC https://www.nec.com/en/global/highlights/safety/campaign/pdf/airport_wp.pdf [https://perma.cc/XVS5-K5B3] (last visited Nov. 16, 2018). The technology is "frictionless" in that it is designed to avoid consumer interaction with the technology or recognition that they are being subjected to a technological process. *Id.*

[308] The possibility of using geofencing to send consumer phones a notice for acceptance when they enter a location using the technology is interesting but likely unworkable as not all consumers use or carry phones. *See* Sarah K. White, *What Is Geofencing? Putting Location to Work*, CIO (Nov. 1, 2017, 12:43 PM), https://www.cio.com/article/2383123/geofencing-explained.html [https://perma.cc/7RRE-TYUJ].

[309] *See, e.g.*, WASH. REV. CODE § 19.375.020(2) (2017). Washington's law states that "notice" is "given through a procedure reasonably designed to be readily available to affected individuals" and is "context-dependent." *Id.*

[310] Masooda Bashir et al., *Online Privacy and Informed Consent: The Paradox of Information Asymmetry, Proc.* ASIST 78th Ann. Meeting (2015), https://www.asist.org/files/meetings/am15/proceedings/submissions/papers/97paper.pdf [https://perma.cc/F4JA-9UQ6]; *Ally Marotti, Google's Art Selfies Aren't Available in Illinois. Here's Why,*

ultimately more beneficial to consumers,[311] this outcome is antithetical to the argument of proponents of notice and choice that it avoids the overregulation of legitimate business interests.[312]

2. The Risks of Statutory Ossification

Legislation of emerging technologies runs the risk of miscomprehending future implications and codifying technical knowledge and potential harms at a static point. While this risk occurs to some degree in all legislation, because technological development is inherently fluid, regulatory interventions may result in heightened risks of inadequately addressing new uses or, as discussed above, corporate actors routing uses around regulations. How BIPA defines and uses terms relating to biometrics provides an example of the predictive limitations of public law and corresponding "ossification" risks. [313]

An example of this tendency in BIPA is the lack of a definition for "collection." Section 15(b) states that "[n]o private entity may collect, capture, purchase, receive through trade, or otherwise obtain [biometric information]." While there are situations in which a corporation is clearly storing faceprints in a database, the process of transcoding information that occurs when generating faceprints does

Chi. Trib., Jan. 17, 2018, https://www.chicagotribune.com/business/ct-biz-google-art-selfies-20180116-story.html [https://perma.cc/YGD4-8BML] (last viewed Mar. 16, 2019). *See also* Erica Gunderson, *Biometric Data: Are We Safer in Illinois, or Just Having Less Fun?*, WTTW (Jan. 22, 2018, 5:07 PM), https://news.wttw.com/2018/01/22/biometric-data-are-we-safer-illinois-or-just-having-less-fun [https://perma.cc/V8PP-LRBU] (mentioning Google's choice to geoblock access in Illinois and Texas to its Arts and Culture application to avoid any possible liability under BIPA).

311 *See* Hartzog & Selinger, *supra* note 10 (discussing a need for a moratorium on all usage of facial recognition).

312 *See* M. Ryan Calo, *Against Notice Skepticism in Privacy (And Elsewhere)*, 87 NOTRE DAME L. REV 1027, 1049–50 (2012); *see also* Kenneth A. Bamberg & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 303 (2011) ("The shortcomings of command-and-control governance . . . are well recognized.").

313 In Justice Scalia's dissent in *United States v. Mead Corp.*, he discusses the risk of "ossification" where procedural requirements in administrative rulemaking limit the ability to change policy or interpretation. 533 U.S. 218, 247 (2001) (Scalia, J. Dissenting). As discussed further below, this Note uses "ossification" to describe situations where privacy entitlements created by legislation increase the political capital required to amend a law, limiting the flexibility of enacted statutes.

not clearly delineate when "collection" has occurred.[314] With products on the market such as those provided by FaceFirst, it is unclear if scanning a face and then comparing it to a database would constitute collection if the faceprint is not retained after comparison.[315] These statutory gaps for growing uses of the technology then force judicial interpretation in ways that may exceed their institutional competence.

When BIPA was enacted, the Illinois legislature could not predict all future commercial uses of biometrics.[316] Present state approaches lack institutional guidance with technical expertise in facilitating the development of the statute.[317] While Washington's law incorporates more nuanced definitions, there is a need for flexibility in adjusting statutes for evolving risks and presently unknown problems.[318] In addition, because judges often lack substantive expertise in matters of a highly technical nature, they should assert caution and deference in construing statutes pertaining to nascent technologies.[319]

The risk of statutory misinterpretation is compounded by heightened resistance to legislative amendment. Two attempts to amend BIPA resulted in contentious negotiation breakdowns between civil society organizations, technology lobbyists, and Illinois legislators.[320] This legislative neutralization may be inherent to individual-rights regimes. BIPA creates a limited entitlement in consumers of controlling their biometric data and a resulting duty in corporations to follow certain procedural requirements.[321] However, after the entitlement is defined, consumers assign a higher value to

---

314 *See supra* Section I.A.2.

315 *See supra* Section I.C.

316 *See supra* notes 197–217 and accompanying text.

317 *See supra* Section II.A.

318 *See supra* Section II.A.

319 *See* Olivier Sylvain, *Disruption and Deference*, 74 MD. L. REV. 715, 761–68 (2015) (noting in *Sony v. Universal Studios* that the Supreme Court stated that judges are generally less capable of "accommodat[ing] fully the varied permutations of competing interests that are inevitably implicated by such new technology").

320 *See* Jeffrey D. Neuburger, *Illinois Considering Amendments to Biometric Privacy Law (BIPA) That Would Create Major Exemptions to its Scope*, NAT'L L. REV. (Apr. 17, 2018), https://www.natlawreview.com/article/illinois-considering-amendments-to-biometric-privacy-law-bipa-would-create-major [https://perma.cc/MEZ9-2XTK].

321 *See* Cohen, *supra* note 91, at 1391.

the right and are likely more resistant to any activities perceived as displacing or removing the right.[322] As Julie E. Cohen has noted control oriented privacy rights that function as a limited property right reinforce persistent inequalities, by raising the social capital cost of amendment and incentivizing corporations to negotiate and consolidate consumer rights through contractual terms.[323] Cohen emphasizes that the fixation on consumer "control" through a libertarian notion of "autonomy," is itself a market failure that gives undue power to adhesive contractual relationships.[324] This suggests an incongruence between the present level of resistance by entrenched parties and the corresponding amount of protection the law provides consumers.[325] Rights-based statutes' tend to ossify results in delegating interpretation to narrow litigation interests, and in creating ambiguity between the statute's terms, the technology it regulates, and a consumer-centric interests without any organization tasked with interpretation.

3. The Problem of Regulating Anxiety

An added complexity of legislation is the disconnect between consumer anxieties and technological expertise. In a recent survey of American fears, participants were far more fearful of corporate tracking of personal information than loneliness, theft, or death.[326] Consumer discomfort with facial recognition suggests a similar underlying trend.[327] The introduction of new technologies often generates anxiety.[328] In the early 1980s, the introduction of the

---

322 *See id.* at 1397–98.

323 *See id.* at 1391 ("Recognizing property rights in personally-identified data risks enabling more, not less, trade and producing less, not more, privacy.").

324 *Id.* at 1399–1402.

325 *See, e.g.*, Neuburger, *supra* note 319.

326 *See* Cari Romm, *Americans Are More Afraid of Robots than Death*, THE ATLANTIC (Oct. 16, 2015), https://www.theatlantic.com/technology/archive/2015/10/americans-are-more-afraid-of-robots-than-death/410929/ [https://perma.cc/4Y7Q-UL83].

327 *See supra* notes 79–86 and accompanying text.

328 Romm, *supra* note 325 ("People tend to express the highest level of fear for things they're dependent on but that they don't have any control over, and that's almost a perfect definition of technology."). However, it shouldn't be overlooked as Thomas Pynchon noted in 1984—the year of the release of the "disruptive" Macintosh personal computer—that these "Luddite" anxieties are actually a proxy of the fear and negative consequences of sociological and economic changes that accompany technological shifts, rather than fear

personal computer led to instances of "computerphobia," where sufferers experienced "a range of resistances, fears, anxieties, and hostilities," including "feeling that you can be replaced by a machine, [or] become a slave to it."[329] The history of BIPA's passage reflects similar anxiety around new technology.[330] While all public law addresses speculation of future harms but limits recovery by requiring standing,[331] the more prescient question is whether anxieties about emerging technologies should be incorporated into a cost-benefit analysis of legislative interventions.

Cass Sunstein argues that individuals' cognitive biases towards the immediacy of perceived new risks lead to "probability neglect," where legal institutions may overcompensate to address consumer concerns leading to "costly expenditures for little or no gain."[332] Due to the latent cultural significance of the face, the technology may cause a heightened emotional response, where "people tend to focus on the adverse outcome, not on its likelihood."[333] While the harms relating to facial recognition carry the potential of both subjective and object harms, legislation that overcompensates for short-term fears may fail at assessing an appropriate normative balance in light of individuals' capacity to adjust.[334]

This is not to suggest that the potential harms of facial recognition are inconsequential, only that setting an entitlement based on the most sensitive parties at a point of heightened anxiety creates an incongruent valuation.[335] It is, however, difficult for legislatures to account for the adjustment of public perception where harms that are intangible (or at minimum difficult to assess based on

---

of the technology itself. Thomas Pynchon, *Is It O.K. To Be a Luddite?*, N.Y. TIMES, (Oct. 28, 1984) ("The word 'Luddite' continues to be applied with contempt to anyone with doubts about technology, especially the nuclear kind.").

329 ANNA FRANCES GRUNDY & JOHN GRUNDY, WOMEN AND COMPUTERS 20 (1996).

330 *See* 740 ILL. COMP. STAT. 14/5 (d), (f) (2008) ("An overwhelming majority of members of the public are wary of the use of biometrics . . . . The full ramifications of biometric technology are not fully known.").

331 *See* Solove & Citron, *supra* note 107, at 750 (discussing judicial limitations on "speculative harms" as not conferring standing).

332 Cass R. Sunstein, *Probability Neglect: Emotions, Worst Cases, and the Law*, 112 YALE L.J. 61, 62–63 (2002).

333 SUNSTEIN, *supra* note 275, at 5.

334 *See* Sunstein, *supra* note 331, at 62–63.

335 *See id.*

costs and benefits) and information asymmetry strongly favor corporate interests. Sunstein suggests that because representative institutions are susceptible to error, responding to public anxieties will create pressures to act in ways that may not ultimately respond to individual's "reflective values."[336] As a result, providing consumers with a right in facial recognition, even with the capacity of class action litigation, likely will not lead to norm-setting.[337]

In such a context, identifying infringement upon an individual privacy right as the core harm produced by mass data collection may mitigate the power structures that shape digital infrastructures. Individual privacy self-management may do little to overcome or change them. The subsequent Section discusses authority available to the FTC and considers if and how agencies or may mediate between consumer anxieties and technological development.

B. The FTC and the Problems of Regulating Opaque and Hidden Usage

As described above, an individual-rights model suffers from the erroneous conception of the consumer as a fully autonomous individual with the capacity to make informed privacy enhancing decisions.[338] Recognizing this limitation suggests that managerial methods may provide more effective control of highly informationalized processes that require governance institutions capable of responding with expertise and discretion.[339] This Part discusses the capabilities of the FTC and managerial regulation of facial recognition, considering the degree to which the FTC can facilitate consumer protective norms as a "privacy norm entrepreneur."[340] Section B.1 finds that the FTC's present regulatory posture may overemphasize notice-and-choice and incentivize corporate behavior antithetical to an effective self-regulatory

---

336 *Id.* at 102–03.

337 As discussed *supra* Section III.A.1, rights that can be contractually negotiated away will likely lead to a result where the interests of the most sensitive (or litigious) parties are protected, with little residual benefit to consumers who can negotiate away their protections.

338 *See* COHEN, *supra* note 36, at 9, 32–33.

339 *See* JULIE COHEN, BETWEEN TRUTH AND POWER 38 (forthcoming 2019).

340 *See generally* Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041 (2000).

regime. Ultimately, Section B.2 considers the value of the underutilized "unfairness" authority, but recognizes that likely obstructions may encumber the emergence of consumer protection norms under the current regime.

1. Deceptive Practices Actions May Undermine Transparency Norms

In states that have biometric laws requiring notice, or that mandate privacy policies for consumer-facing companies,[341] the FTC may bring enforcement actions for misrepresentations within privacy policies.[342] The FTC's action against Nomi Technologies provides an example of how this authority may be used and its relative strengths and weaknesses as a regulatory mechanism for facial recognition in retail.

In 2015, the FTC brought an enforcement action against Nomi Technologies, a company in the retail technology sector that offered brick-and-mortar clients the ability to analyze aggregate data about consumer traffic in the merchants' stores.[343] The FTC alleged that Nomi misled consumers with promises that it would provide an in-store mechanism for consumers to opt out of tracking and that consumers would be informed when locations were using Nomi's tracking services.[344]

In dissenting statements on the action, Commissioner Maureen Ohlhausen reflected the tension between the goals of consumer control and the desire for corporate participation and transparency norms.[345] Commissioner Ohlhausen stated that the action fails to balance consumer harms with the FTC's goal of "transparency" as it "imposes a penalty far out of proportion to . . . consumer harm," because Nomi "went beyond its legal duty" by offering a consumer-facing design intervention in its product "with an easy and effective

---

341 *See, e.g.*, Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 PENN. ST. L. REV. 777, 793 (2016).

342 *See supra* Section II.C.

343 Complaint at ¶¶ 3–5, *In re* Nomi Techs., 2015 FTC Lexis 213 (F.T.C. Aug. 28, 2015) (No. C-4538).

344 *Id.* at ¶¶ 15–17.

345 Dissenting Statement of Comm'r Maureen K. Ohlhausen, In re Nomi Techs, Inc., (F.T.C. Aug. 28, 2015) (Matter No. 132-3251).

global opt-out."[346] Commenters on the action have noted that by pursuing Nomi, the FTC is creating an implicit incentive where companies are subjected to higher liability where they are more transparent than when they are vague or "not offering an opt-out mechanism at all."[347]

The problem may be inherent to the FTC's "deceptive practices" power where situations under which the FTC can file a complaint are relatively limited[348] and the FTC lacks the explicit authority to generally protect online consumer privacy.[349] In the absence of this authority, the FTC cannot mandate that companies have privacy policies, creating a "curious situation whereby a company without a privacy policy is arguably less likely to be punished for privacy-invasive practices than a company with a privacy policy."[350] This situation leads to an implicit incentive where companies that are vague about their commitments to privacy or that have a general privacy policy utilizing boilerplate language typically will be immune from action under Section 5 authority.[351]

The shortcomings of this approach may suggest a shifting status of the influence of technology on consumers' everyday lives. When the central approach of the FTC was incentivizing disclosure through privacy policies, noncompliance was obvious, and the FTC could serve a more disengaged and entrepreneurial role.[352] However, where facial recognition practices in retail are inherently nontransparent and involve complex systems with multiple actors and hard-to-calculate risks, this approach may incentivize market

---

346 *Id.*

347 James S. DeGraw et al., *Nomi Highlights Risks of Publicizing Privacy Policies*, LAW360 (May 27, 2015, 8:21 AM), http://www.law360.com/articles/659398/nomi-highlights-risks-of-publicizing-privacy-policies [https://perma.cc/A8BK-FJGV].

348 *See* Reidenberg et al., *supra* note 203, at 509.

349 *See id*.

350 *See Federal Trade Commission: Overview of Statutory Authority to Remedy Privacy Infringements*, ELEC. PRIVACY INFO. CTR., http://epic.org//privacy/internet/ftc/Authority.html [https://perma.cc/Q64A-RHBW] (last visited Nov. 6, 2018).

351 *See* CHRIS HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 216 (2016) ("The FTC's deceptive power is not a perfect tool for policing information security problems.").

352 *See generally* Hetcher, *supra* note 340.

failure in self-regulation.[353] The incentive structure towards opaque practices that evade regulatory friction is already apparent in companies that use facial recognition.[354] While deceptive practices could serve as a regulatory mechanism for FTC enforcement of data privacy norms for facial recognition in retail, this approach may have the inadvertent result of reinforcing lack of transparency by companies that use the technology.[355] This outcome is especially problematic because low-compliance obligations do not meaningfully displace or regulate practices, while the high value of consumer information incentivizing collection cannot be meaningfully regulated by optimistic notions of corporate responsibility.[356] As a result, the FTC's present posture may ultimately facilitate continued market failure rather than effective self-regulatory behavior.[357]

2. Unfair Practices Authority May Enable Limited Norm Development

The Wheeler-Lea Amendments to the FTCA provide broad regulatory latitude to the FTC for defining new practices as "unfair."[358] The FTC has historically understood the unfairness standard as "the result of an evolutionary process. . . . deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not

---

353 *See* Margot E. Kaminski, *Binary Governance: A Two-Part Approach to Accountable Algorithms* 4, 17–19 (forthcoming 2019).

354 *See, e.g.*, *Our Privacy Commitment*, FACEFIRST, https://www.facefirst.com/privacy-commitment/ [https://perma.cc/JV3V-6FMV] (last visited Nov. 10, 2018). FaceFirst's website only includes a privacy policy for its website, which does not discuss the use of its products by retailers. *See id.* FaceFirst's representations in its website section titled "Commitment to Privacy" contain language such as "*we encourage* customers to post signage alerting customers when that biometric surveillance is being used" that creates no enforceable commitment in FaceFirst as the technology provider. *Id.*

355 Shawn A. Johnson, *A Law and Economics Approach to Privacy Policy Misstatements: Considering the Need for a Cost-Benefits Analysis in the FTC's Deception Framework*, 18 COLUM. SCI. & TECH. L. REV. 79, 98–99 (2016) ("The true harm implicated in *Nomi* is the market failure that occurs when consumers are deprived of accurate information with which to make informed choices.").

356 *See* COHEN, *supra* note 338, at 44.

357 *See* Cohen, *supra* note 91, at 1395.

358 *See supra* Section II.C.

quickly become outdated or leave loopholes for easy evasion."[359] Notably, the FTC can find a practice unfair even when it is otherwise legally permissible.[360] This vagueness in definition creates value in the FTC's flexibility to address new problems.[361] This flexibility is valuable in regulating new information flows—like facial recognition—where market forces have power to route around inconvenient regulatory resistance by redefining or obscuring the regulated process.[362]

The FTC is an appropriate body to regulate emerging technologies through the historical expertise of the agency in technological matters.[363] Additionally, the agency's history of action, allowing regulation of consumer harms that fall outside the scope of traditional torts and regulatory efforts, affords a more deferential posture by the courts to the agency's expanding definitions of its own authority.[364] This Part discusses available FTC authority under Section 5 unfair powers and the possibility of direct enforcement actions against facial recognition in retail settings.

3. Enforcing Data Security Norms

For the FTC to act the harm must be substantial.[365] While the most dominant kind of substantial harm asserted by the FTC has been monetary, notions of harm under unfairness have been steadily evolving over the past twenty years.[366] In *FTC v. Wyndham Worldwide Corp.*[367] the court found that "non-monetary harm" may

---

359 FED. TRADE COMM'N POLICY STATEMENT ON UNFAIRNESS, App. to *Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

360 Spiegel v. FTC, 540 F.2d 287, 292 (7th Cir. 1976) ("[T]he Supreme Court left no doubt that the FTC had the authority to prohibit conduct that, although legally proper, was unfair to the public.").

361 HOOFNAGLE, *supra* note 350, at 30.

362 *See* Julie E. Cohen, *The Regulatory State in the Information Age*, 17 THEOR. INQ. L. 369, 385–87 (2016).

363 *See* HOOFNAGLE, *supra* note 350, at 30 (discussing the FTC's pivots to the emerging technologies of radio and television to regulate unfair and deceptive practices).

364 *See* Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 MD. L. REV. 785, 814 (2015).

365 *See supra* Section II.C.

366 *See generally* Solove & Hartzog, *supra* note 226.

367 10 F. Supp. 3d 602 (D.N.J. 2014).

support an action.[368] The Third Circuit did not clarify this point, and this authority is not yet stable.[369] Nonetheless, the FTC likely has the authority to address data security failings that lead to breach and theft of facial recognition information.

In *Wyndham* the court found that the agency could bring an adjudicatory action where reasonable notice was provided through industry guidance sources, the FTC's guidance, and consent orders from previous FTC enforcement actions.[370] The increasing quantity of information available to businesses through the FTC and internal trade groups on reasonable data security approaches likely indicates that a failure on the level of *Wyndham* by a retailer or facial recognition software provider would justify an FTC action especially where facial recognition data is particularly "sensitive."[371]

This pattern suggests that the FTC could bring adjudication actions to mandate encryption of facial recognition data at rest and transmission.[372] Considered under the policy statement on

---

[368] *Id.* at 623 n.15 (noting, however, that "the Court need not reach this issue given the substantial analysis of the substantial harm element above").

[369] *See* LabMd, Inc. v. FTC, 776 F.3d 1275 (2015); *see also* Ava Farshidi, *The New Retail Experience, and its Unaddressed Privacy Concerns: How RFID and Mobile Location Analytics Are Collecting Customer Information*, 7 CASE W. RES. J.L. TECH. & INTERNET 15, 25–26 (2016). *But see* Daniel Solove, *Did the LabMD Case Weaken the FTC's Approach to Data Security?*, LINKEDIN (June 8, 2018), https://www.linkedin.com/pulse/did-labmd-case-weaken-ftcs-approach-data-security-daniel-solove/ [https://perma.cc/A5C9-SXUW] (stating that the Eleventh Circuit opinion focuses on the particulars of the order the FTC sought against LabMD, not on the underlying theory of unfairness or on the use of negligence as a standard to find unfairness and therefore does not create a split with the Third Circuit).

[370] *Wyndham*, 10 F. Supp. 3d at 616–17.

[371] This Note suggests that it would be within the scope of the FTC's evolutionary process to include faceprints within definitions of "sensitive personal information" information that poses heightened privacy concerns that require heightened restrictions. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUS. AND POLICYMAKERS, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/T4KB-N576]; *see also* Jon L. Mills & Kelsey Harclerode, *Privacy, Mass Intrusion, and the Modern Data Breach*, 69 FLA. L. REV. 771, 805–06 (2017).

[372] Encryption is the process of transforming information so that only the person (or computer) with the key can read it. Encryption technology for sensitive data "at rest" refers to information while it is on a server, while "in transit" refers to transferring information

unfairness cost-benefit analysis framework, the unique harms of not encrypting faceprints likely meets the standard of an unfair practice. Even if individual harm to consumers is low and predominantly subjective, in the aggregate, the harms are substantial.[373] While a company not using encryption reduces its own compliance costs, this practice does not increase market competition as a whole, and, it is highly unlikely that the costs avoided outvalue the net harm of taking no action.[374] Where the facial recognition information was collected remotely and without active consumer knowledge, there is little likelihood of avoiding the harm caused.[375] Analogous to Justice Marshall's dissenting opinion in *Smith v. Maryland*,[376] the "risk of surveillance" here is unavoidable even if some form of notice is provided because "[i]t is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternate."[377] Suggesting that consumers can choose to not go to brick-and-mortar retailers is not a realistic policy position. Because the unfairness balancing test has the flexibility to incorporate public policy considerations in situations of nominal "consent" that the deceptive test cannot,[378] regulators may balance the inefficiency of consumer attempts to avoid retail establishments for fear of future breach or surveillance harms as a harm for both consumers and retailers.[379]

---

across websites, on devices, or in the cloud. Thomas B. Paul, *Stick with Security: Store Sensitive Personal Information Securely and Protect It During Transmission*, FED. TRADE COMM'N (Aug. 18, 2017, 8:59 AM), https://www.ftc.gov/news-events/blogs/business-blog/2017/08/stick-security-store-sensitive-personal-information-securely [https://perma.cc/BCL6-589C].

373 *See supra* Section I.B.

374 Johnson, *supra* note 354, at 115–16 (2016).

375 *See supra* Section I.B.1; *see also* Hartzog, *supra* note 363, at 798 (noting that in a spyware case under the unfair authority the FTC noted that substantial harm was caused to consumers from invasive surveillance and recognized concerns that "[c]onsumers cannot reasonably avoid these injuries because [the surveillance] is invisible to them").

376 442 U.S. 735, 748–52 (1979).

377 *Id.* at 750 (Marshall, J., dissenting).

378 *See supra* Section III.A.1.

379 While it could be argued that this approach could result in a competition benefit that incentivizes privacy markets where consumers choose to go to stores that do not use facial recognition, as discussed *supra* Section I.B.1, the incentives inherent for nondisclosure of practices presently makes this model unrealistic.

Whether the FTC can take prospective actions relating to perceived data security failings in the absence of breach is a more tenuous question. While the *Wyndham* court and the unfairness guidance leaves this possibility open, this action would run contrary to the agency's historical pattern of enforcement.[380] The FTC frames this deference to industry as a strength by promoting coregulatory regimes.[381] Through enforcing industry-specific consumer protection measures the FTC uses its limited resources towards setting norms on the margins of industry practice, setting the boundary of acceptable behavior.[382] However, while this "soft touch" approach generally benefits industry by limiting compliance obligations, the practical success of this approach requires the FTC to take action when a violation occurs, particularly by a prominent industry player or a particularly egregious violation.[383] However, as discussed infra, passive deference to industry activities and "corporate responsibility" may result in consumer harms in the absence of breach.

4. Enforcing Use, Data Minimization, and Transparency Norms

The FTC's unfairness power is more attenuated for harms relating to unexpected use or those exceeding expected use, where no breach has occurred. This is likely due to multiple factors: (1) a practical complexity in the economics of accurately balancing harm and benefit where harms are difficult to quantify the loss of privacy and the benefits of increased data collection is a quantifiable market good;[384] (2) agency aversion to judicial reversal;[385] (3) an

---

380 *See supra* Section III.B.1.

381 *COMMISSION STATEMENT MARKING THE* FTC'S *50TH DATA SECURITY SETTLEMENT*, FED. TRADE COMM'N (Jan. 31, 2014), www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf [https://perma.cc/PVF8-G8M6].

382 *See* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2262 (2015).

383 David A. DeMarco, *Understanding Consumer Information Privacy in the Realm of Internet Commerce: Personhood and Pragmatism, Pop-Tarts and Six-Packs*, 84 TEX. L. REV. 1013, 1037 (2006).

384 HOOFNAGLE, *supra* note 350*,* at 337–38.

385 *See id.* 334.

information gap between the regulators and industry;[386] (4) general deference to industry interests;[387] and (5) a historical tendency to enter into new areas using its deceptive power first.[388] However, the unfairness authority may be a more appropriate tool for balancing consumer privacy interests against information accumulation business models.[389]

Enforcement of facial recognition under the unfairness authority is difficult precisely because the balancing test for unfairness requires accounting for benefits to consumers and competition conferred through use of the technology. In the absence of a breach, subjective consumer harms may not outweigh retailors benefits of increasing information flows or proving convenient services. The FTC's action against Negotiated Data Solutions (N-Data) provides a framework of how to shift the agency's reliance from deceptive to unfairness authority using standards-based governance. In 2008, the FTC alleged that N-Data violated Section 5 of the FTCA by engaging in unfair acts or practices related to a promise not to enforce its patents to an essential Ethernet standard for local area networks (LAN).[390] The FTC alleged that N-Data's unfair practices were unfair reneging on a license agreement with the IEEE based on a standard that had been set by the industry.[391] The FTC found that "the type of behavior engaged in by N-Data harms consumers," because "[t]he process of establishing a standard displaces competition; therefore, bad faith or deceptive behavior that undermines the process may also undermine competition in an entire industry, raise prices to consumers, and reduce choices."[392] In N-Data, the FTC signaled an intention to expand its Section 5

---

386 *See, e.g.*, Rory Van Loo, *Helping Buyers Beware: The Need for Supervision of Big Retail*, 163 U. PA. L. REV. 1311, 1379 (2015).

387 *See supra* Section II.C.

388 HOOFNAGLE, *supra* note 350, at 347.

389 *Id.* (arguing that the failure of communication and customer relationship that lead to the Nomi enforcement was an "unfairness case[] dressed in a deception theory").

390 Theresa R. Stadheim, *Rambus, N-Data, and the FTC: Creating Efficient Incentives in Patent Holders and Optimizing Consumer Welfare in Standards-Setting Organizations*, 19 ALBANY L.J. SCI. & TECH. 483, 499 (2009)

391 *Id.*

392 THE CAMBRIDGE HANDBOOK OF TECHNICAL STANDARDIZATION LAW: COMPETITION, ANTITRUST, AND PATENTS 233 (Jorge L. Contreras ed. 2018).

enforcement in the context of high-tech markets based on participation in standards set by private standard-setting organizations.[393] In doing so, the FTC suggested an interpretation of the unfairness authority where a standard may be used both as the norm to be enforced and the mechanism for enforcement.

While N-Data has not yet proven to be the inflection point in the FTC's shift to this approach, the unfairness power's ability to facilitate and enforce norms created by private actors is coherent with the FTC's authority and history.[394] However, shifting to reliance on standard setting organizations creates new complexities to traditional enforcement models.[395] Julie E. Cohen argues that the shift to a standards-based governance structure reshapes modes of lawmaking and enforcement, where traditional modes of authority are "being outpaced by sociotechnical change."[396] Standards may compensate for the market failure in self-regulation that occurs from "information asymmetries that preclude the exercise of informed choice."[397] Additionally, standards may allow for a correction to the competitive structures, which ultimately result in the collection imperative as industry members search for any and all new sources of data out of a need to compete with the substantial advantages held by large players like Amazon, who already collect massive amounts of consumer data accumulation across platforms. A multistakeholder approach, where interest holders mandate standards for FTC enforcement, would be a beneficial alternative to direct and reactive participation by the public, due to a lack of expertise in understanding the ways in which technical commitments "implicate, reflect, reinforce, and sometimes predetermine policy commitments."[398]

---

393 Amy Marshak, *The Federal Trade Commission on the Frontier: Suggestions for the Use of Section 5*, 86 N.Y.U. L. REV. 1121, 1137–38 (2011).

394 *See supra* Section II.C.

395 COHEN, *supra* note 338, at 16.

396 *Id.*

397 Cohen, *supra* note 91, at 1395.

398 COHEN, *supra* note 338, at 38–39 (noting that "network organization under mandated standardization creates a paradox" where the need to effectively govern opaque organizations results in an agency that is itself opaquer and less accountable to the broader public.).

5. Systemic Failures in Negotiations at the NTIA

The problem, however, of an FTC mandated standard regime for facial recognition in retail is that this approach was already attempted by the NTIA and failed in achieving its goal of creating a clear, voluntary, and actionable policy.[399] The draft document produced after the walk-out of privacy advocates created a lower level of obligations than the FTC's own recommendations.[400] As Margot E. Kaminski notes, "the NTIA failure indicates that the current backdrop of potential FTC enforcement is not enough to get the industry to the table."[401] FTC enforcement of the codes of conduct themselves may drive the industry to view both the negotiation and adoption of codes of conduct as "leading to more likely enforcement by the FTC."[402] This scenario creates an incentive scheme that is "backwards" because, "industry views the NTIA codes of conduct as potentially creating a penalty, not avoiding one."[403]

The increased possibility of FTC enforcement creates an implicitly collusive free rider problem where the industry is discouraged from adopting codes of conduct once they have been created. Furthermore, the industry is averse to negotiating, out of fear that completed codes might be viewed as actual industry standards by the FTC, therefore driving FTC enforcement even without explicit adoption of the codes by particular players.[404] Such an outcome is exacerbated by civil society stakeholders, responding to the lack of negotiation, by hardening a demand for a rights-based regime.[405] While the FTC can "more visibly play the hammer" by entering directly into the regulation of facial recognition, Kaminski notes a paradox of this approach where new industries without

---

399 *See supra* Section II.D.

400 Margot E. Kaminski, *When the Default Is No Penalty: Negotiating Privacy at the NTIA*, 93 DENV. L. REV. 925, 935 (2016).

401 *Id.* at 946–47.

402 *Id.*

403 *Id.*

404 *Id.*

405 *See, e.g.*, Jennifer Lynch, *EFF and Eight Other Privacy Organizations Back Out of NTIA Face Recognition Multi-Stakeholder Process*, ELECTRONIC FRONTIER FOUND. (June 16, 2015), https://www.eff.org/deeplinks/2015/06/eff-and-eight-other-privacy-organizations-back-out-ntia-face-recognition-multi [https://perma.cc/62DT-BQ5K].

standards make FTC enforcement more difficult, reducing the leverage of their ability to encourage real negotiations in new technological space.[406] The next Part considers what actions the FTC and Congress can take to resolve this impasse, providing a forum for stakeholder negotiations that facilitates new norms and standards that can benefit both retailers and consumers.

IV. PROPOSAL: COLLABORATIVE GOVERNANCE AS A REGULATORY APPROACH

This Note has highlighted specific privacy harms that may befall consumers from the collection of personal data through facial recognition in retail settings. This Note recognizes that the use of facial recognition is still relatively new in the consumer sector and, as such, comprehensive industry norms and standards have yet to emerge. While there are privacy risks inherent as the technology develops, there are also potential benefits for consumers.[407] Even with increased media coverage and consumer anxiety towards the invasiveness of facial recognition, few consumers have changed their behavior, boycotted invasive tech firms, or exercised the nominal digital rights they possess.[408] Where applicable, right-based regimes, like BIPA, are ill-suited to address the massive information gap between individuals' knowledge and that of corporate actors.[409] Ongoing emphasis on autonomy and control ultimately requires individual-level data management that is time-consuming and complex especially where facial recognition technology is designed to be obscure.[410] This asymmetry becomes easily exploitable by consent-oriented approaches that have tendencies towards rent extraction and illusory choices rather than meaningful protections.[411] These potential limitations are especially relevant given the interest of various states and municipalities—including New York City—in creating biometric privacy laws enforceable by

---

406 Kaminski, *supra* note 399, at 948–49.

407 *See supra* Section I.C.

408 *See supra* Section III.A.

409 *See supra* Section III.A.1.

410 *See* Woodrow Hartzog, *Opinions: The Case Against Idealising Control*, 4 EUR. DATA PROTECTION L. REV. 423, 426-31 (2018).

411 *See supra* Section III.A.

private rights of action, with the potential for expansive (and expensive) litigation.[412] Facial recognition presents an issue of systemic management, making individual-rights regimes inadequate to take up demands that are impossible to vindicate by individuals.

Managerial frameworks and industry-based governance have thus far failed to keep up with the emerging technology, and often fail to fully consider various stakeholders impacted by ubiquitous data gathering and use.[413] Heightened information asymmetries require careful policy interventions to prevent the technology's realizing of only nominal benefits while degrading significant privacy interests.[414] These potential difficulties require facilitating the development of appropriate norms for governing a new information flow.[415] Instead, approaches have focused on regulating through a conservative "light touch" approach designed to give maximum freedom to corporate entities pursuant to a neoliberal conception of self-correcting markets.[416] While scholars have argued that the FTC's emphasis on self-regulation is "more than rubber stamp" on corporate interests,[417] the overall emphasis on consent and privacy policies as the key mechanisms for consumer protection have resulted in an incentive structure of selective transparency and strategic corporate social responsibility rather than market-based regulation.[418] While expanded use of the unfair power may serve important consumer interests, it is likely inadequate as a sole mechanism due to political aversion to a shifting definition of

---

412 *See, e.g.,* Stephanie Kapinos*, New York City Considers Facial Recognition Bill — Will New York Be the Next Forum for Biometric Privacy Litigation?,* PROSKAUER: NEW MEDIA & TECH. BLOG (Jan. 31, 2019), https://newmedialaw.proskauer.com/2019/01/31/new-york-city-considers-facial-recognition-bill-will-new-york-be-the-next-forum-for-biometric-privacy-litigation/ [https://perma.cc/TEE5-GJAF] (discussing Bill Int. No. 1170, a bill introduced by City Council member Ritchie Torres that would regulate the use of biometric technology in New York City, amending Section 1, Chapter 5 of Title 20 of the Administrative Code of the City of New York and requiring businesses to give notice to customers if they are collecting "biometric identifier information").

413 *See* Anjanette H. Raymond, *Information and the Regulatory Landscape: A Growing Need to Reconsider Existing Legal Frameworks*, 24 WASH. & LEE J. CIV. RTS. & SOC. JUST. 357, 358–60 (2018).

414 *See supra* Section I.C.

415 *See supra* Section III.B.

416 *See supra* Section II.C.

417 Solove & Hartzog, *supra* note 226, at 676.

418 *See supra* Section III.B.1.

"unfairness," lacking agency resources, and the difficulty of balancing non-monetizable surveillance effects of facial recognition against known and valuable data extraction benefits to businesses.[419]

A substantial response is required. As Microsoft president Brad Smith, emphasized in December, facial recognition is currently a "commercial race to the bottom, with tech companies forced to choose between social responsibility and market success."[420] While it may be warranted to be skeptical of Smith's professed desire to regulate out of social responsibility rather than the capability of a large corporation like Microsoft to compete in a regime with higher compliance costs, his diagnosis is likely apropos.[421] Until an enforceable industry standard emerges, consumers experience the ongoing risks of regressive technological governance.

A. Experimental Regulating Through the FTC

These signals from industry have been received in part on Capitol Hill. In December of 2018, Senator Brian Schatz introduced a bill into the Senate that would cover biometric information.[422] The proposed Data Care Act (DCA) would attempt to update the relationships of consumers and data collectors by creating a fiduciary obligation in the data collector as a "duty of care," providing the FTC with enforcement mandate under Section 5, expanding the FTC's enforcement toolkit with Administrative Procedure Act (APA) rulemaking authority, and making the created duties nonwaivable.[423] Approaches like the DCA, which deemphasize consumer data self-management and emphasize incremental interpretative development through FTC participation, suggest a trend in the right direction.[424] However, the DCA may be

---

419 *See supra* Section III.B.2.

420 Jay Greene & Douglas MacMillan, *Microsoft Pushes Urgency of Regulating Facial-Recognition Technology*, WALL ST. J., Dec. 6, 2018, https://www.wsj.com/articles/microsoft-pushes-urgency-of-regulating-facial-recognition-technology-1544129253 [https://perma.cc/4YSP-AMUY] (internal citation omitted).

421 *See* Kaminski, *supra* note 352, at 28.

422 Data Care Act, S.R. 3744, 115th Cong. § 2 (2018).

423 *Id.*

424 See Woodrow Hartzog & Neil Richards, *It's Time to Try Something Different on Internet Privacy*, WASH. POST, Dec. 20, 2018, https://www.washingtonpost.com/opinions/its-time-to-try-something-different-on-internet-privacy/2018/12/20/bc1d71c0-

limited without accounting for additional factors, such as the FTC's own expertise limitations in making appropriate rules.[425]

This Note proposes that addressing the instrumental concerns about facial recognition require a systemic shift in regulatory approach. Collaborative governance, through carefully calibrated public-private partnerships, may be better suited for regulating complex systems that create hard-to-calculate risks, change too quickly for traditional regulatory approaches, and involve technical and industry expertise that regulators and legislators are unlikely to have.[426] This approach may solve a "pacing problem" because "the pace of technological and market change [have] accelerated, both rule-based and purely self-regulatory approaches have become increasingly less relevant to the protection of privacy."[427] The goal of collaborative governance is to exist in a space between command-and-control and private ordering.[428] As a result, the shift to collaborative governance is coherent with the FTC's historical relationship to business and facilitation of information exchanges as a "norm entrepreneur."[429] What is required for this mechanism to work is twofold: expanded authority by Congress to directly regulate the facial recognition sector and an agency shift greater involvement allowing for the engagement and retention of industry participation. This can include using direct regulatory measures such as negotiated rulemaking, codes of conduct with required agency approval of terms, using legal safe harbors to encourage the adoption of industry codes of conduct, audited self-regulation with certification standards, and filing and disclosure obligations.[430] Incentive systems can be designed that encourage monitoring and

---

0315-11e9-9122-82e98f91ee6f_story.html?utm_term=.ee18fb158f19 [https://perma.cc/4ZXQ-4F6J].

425 Additionally, the DCA as drafted may not restrict uses that result in subjective harms discussed above, because even if surveillance uses "benefit the online service to the detriment of an end user," they may not satisfy the heightened standard of "unexpected and highly offensive to a reasonable end user." S. 3744 § 3 (b) (2) (A–B).

426 Kaminski, *supra* note 352, at 4–5.

427 Kenneth A. Bamberger & Deirdre K. Mulligan, *New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry*, 33 L. & POL'Y 477 (2011).

428 Kaminski, *supra* note 352, at 19.

429 *See* Bamberger & Mulligan, *supra* note 311, at 308, 314.

430 Kaminski, *supra* note 352, at 20.

allow for benefits to be recognized by those that are compliant and that more immediately sanction non-compliance.[431]

While there is some suggestion that the US should shift to an omnibus GDPR solution,[432] this Note finds that the sectoral approach applies a clearer and more granular approach for regulator engagement with stakeholders in the retail sector that does not risk displacing or confounding consequences of preempting present federal and state law.[433] An FTC-centric collaborative governance approach would build on existing relationships and patterns of governance, while shifting the incentive structure of regulated entities towards norm realization rather than a deregulatory obfuscation. The FTC, by shifting its regulatory focus towards a collaborative role, can become a greater facilitator of information exchanges, supplying the incentives for the design of ethical technologies that enhance consumer privacy.

B. Outline for a Collaborative Process

This Note suggests that the NTIA process is not conclusive that a collaborative governance approach is unworkable for facial recognition. While the NTIA's failure may have been a result of the dissonance between the agencies perceived role as a "neutral forum" and creation of a "voluntary" best practices, the FTC's involvement in a collaborative process would be as a direct regulator. [434] This Note suggests a multi-step proposal for recalibrating the FTC's regulatory approach.

Initially, the FTC requires a Congressional statutory grant for addressing private sector facial recognition.[435] As discussed supra,

---

[431] *See* Scott J. Shackelford et al., *When Toasters Attack: A Polycentric Approach to Enhancing the "Security of Things,"* 2017 U. ILL. L. REV. 415, 472 (2017).

[432] *See, e.g.*, Ohm *supra*, note 68, at 1764. *Cf.* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 922, 927-29 (2009) (discussing the drawbacks of embracing an omnibus privacy regime in the U.S.).

[433] *See* Bamberger & Mulligan, *supra* note 311, at 309.

[434] Kaminski, *supra* note 399, at 948.

[435] While some scholars argue that a state-oriented approach following BIPA is appropriate, this Note finds that these approaches provide inadequate protections, while potentially resulting in a balkanized compliance regime, a lack of cohesion between federal and state requirements for standing, and extensive legal fees for class action attorneys.

the Magnuson-Moss rulemaking procedure imposed by Congress in 1980, due to perceived abuses of the agency's rulemaking authority, may too greatly limit the agency's effectiveness at addressing issues of emerging technology.[436] This Note suggests that political reservations towards a more expansive administrative state may be diffused by crafting legislation that requires: (1) preliminary reporting to Congress clarifying the status and potentials of facial recognition technology; (2) a statutory mandate of negotiated rulemaking; (3) a modified safe harbor provision; and (4) delegated supplemental enforcement through state attorneys general.

1. Preliminary Reporting

The FTC's present employment of technologists suggests internal competencies for filling a role similar to the Office of Technology Assessment (OTA), prior to its 1995 defunding—providing nonpartisan advice on technical subjects.[437] The OTA's role was to ensure that sound scientific insight from the sciences guided Congressional policy choices.[438] Reports by the National Highway Traffic Safety Administration (NHTSA) as a requirement in the Moving Ahead for Progress in the 21st Century Act, suggest that reporting requirements can increase general publicly available technical knowledge in the contentious technological areas, such as the cybersecurity of self-driving cars, while offering prospective identification of regulatory hurdles.[439] Statutory reporting requirements could expand the FTC's informational role, while emphasizing non-partisan research goals.

Compare Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186 (2019), *with* Rivera v. Google, Inc., No. 16 C 02714, 2018 WL 6830332, (N.D. Ill. Dec. 29, 2018).

436 *See supra* Section II.C.

437 *See* Deirdre K. Mulligan & Kenneth A. Bamberger, *Saving Governance-by-Design*, 106 CAL. L. REV. 697, 734 (2018). The FTC is already filling this role in part through convening conferences, and other nonenforcement regulatory tools. *See, e.g.*, FED. TRADE COMM'N, *supra* note 50.

438 Mulligan & Bamberger, *supra* note 436, at 734.

439 *Id.* at 774–75 (noting that this enabled promulgation of a unique policy calling for procedural input and oversight of design implementation).

2. Negotiated Rulemaking

The Negotiated Rulemaking Act of 1990 (NRA) establishes a statutory framework for negotiated rulemaking under which agencies may bring together representatives of the affected parties in a negotiating committee for face-to-face discussions.[440] If the committee reaches a consensus, the agency can then issue the agreement as a proposed rule subject to normal administrative review processes.[441] While use of the NRA is typically discretionary,[442] historical reservations over FTC rulemaking may suggest political expediency in mandating a collaborative approach, with the fallback option of traditional APA rulemaking in the event of a negotiation breakdown.

While negotiated rulemaking has declined in usage since the 1990s,[443] this Note finds that it may have unique propensities for addressing facial recognition in retail. As David Thaw suggests, the success of negotiated rulemaking in creating an information security rule under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for entities managing individuals' sensitive health data, is an indicator of negotiated rulemaking's ability to address contentious privacy-related issues. [444] In creating the HIPAA rule, the Department of Health and Human Services (HHS), delegated substantial negotiated rulemaking authority to the National Committee on Vital Health Statistics (NCVHS), a committee composed of representatives of private interests and private experts. [445] NCVHS ultimately created a workable cybersecurity rule, generally considered successful.[446] Thaw suggests that the success of the NCVHS by "harness[ing] private expertise not at the expense of the public interest, but rather in support of it" was the result of several factors[447]: First, that members believed that if they failed to

---

440 *See* 5 U.S.C. § 561 (1992).

441 *See* 5 U.S.C. § 562(2) (1992).

442 *See* David Thaw, *Enlightened Regulatory Capture*, 89 WASH. L. REV. 329, 341 (2014).

443 *See* Jeffrey S. Lubbers, *Achieving Policymaking Consensus: The (Unfortunate) Waning of Negotiated Rulemaking*, 49 S. TEX. L. REV. 987, 989 (2008).

444 *See* Thaw, *supra* note 441, at 351–52.

445 *Id.* at 352.

446 *Id.*

447 *Id.* at 335, 355–66, 369.

act, other regulators or legislators would act, resulting in patchwork of inconsistent local rules that would both be inefficient and could lead to increased potential liability.[448] Next, that participants role having the "force of law" rather than "merely advisory" authority imposed a heighted sense of responsibility towards "the public interest" in the negotiation's outcome.[449] Finally, that highly technical and interconnected problems require nuanced solutions where participants' information sharing ultimately would benefit their future compliance.[450]

While some scholars suggest that negotiated rulemaking is no more successful than APA rulemaking and can undermine public accountability,[451] this Note argues that because of the normative nature of privacy as an allocation of power, regulating facial recognition requires the information sharing and collaboration emphasized through negotiated rulemaking to countervail information asymmetries.[452] The FTC, by initiating and maintaining a collaborative process with the flexibility to convene a larger committee on privacy and technology, and then creating stakeholder subcommittees on topics such as "the use of facial recognition in retail," can facilitate emerging norms with greater dexterity towards both the future development of the technology and granularity of the privacy risks and expectations in differing sectors.

Facilitating engagement from new and wider ranges of inter-disciplinary stakeholders can address the technological, ethical, and rights effects of decision-making, while simultaneously diminishing the hardening of negotiation positions occupied by trade groups, social media companies, and consumer advocates that are less susceptible to reputational pressures than brick-and-mortar retailers.

---

448 *Id.*

449 *Id.*

450 *Id.*

451 *See* William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 982 (2016).

452 *See* Cohen, *supra* note 91, at 1379–82; *see also* Thaw, *supra* note 441, at 353 (citing Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667, 667–68 (2013)) ("privacy is a normative exercise in making 'decisions about competing claims to legitimate access to, use of, and alteration of information.'"); *see also* Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S J.L. & POL'Y FOR INFO. SOC'Y 355, 413–14 (2011).

Imagining this as a generative and creative process with participation of technologists can result in use-oriented restrictions beyond notice-and-choice and include design-based solutions that balance consumer privacy and industry interest. Examples of such include temporary anonymized faceprint storage,[453] using sorted index numbers (SIN) of appearance based facial features that cannot be reidentified,[454] limited access secure multiparty displaced database computation,[455] or creating auditable machine learning algorithms.[456]

This Note recognizes that coregulation has been a central premise of *proposed* legislation in the United States, including the Obama Administration's privacy initiative and bills sponsored by members of Congress from both parties—none of which became law.[457] However, this Note argues that growing emphasis on state level regulation, such as the CCPA and BIPA, coupled with the general increased public awareness (and anxiety) of privacy harms may be the beginning of a corrective. Under such, the "no penalty" default will become an increasingly less-desirable posture for industry than participation in regulatory rulemaking.[458] Additionally, as the FTC would retain the auxiliary alternative under negotiated rulemaking for developing its own rules pending a negotiation breakdown, the potential for failure is substantially mitigated. While negotiated rulemaking is not a panacea, the combination of incentivized opaqueness, potential for consumer harm, and lacking effectiveness of FIPPs in retail facial recognition suggests the need for new approaches to regulation.

---

[453] William Tyree & Heather Sliwinski, *FaceFirst Announces Mask-ID for Enhanced Facial Recognition Privacy, Increased Security of Biometric Data*, CISION: PRWEB (Nov. 13, 2018), https://www.prweb.com/releases/facefirst_announces_mask_id_for_enhanced_facial_recognition_privacy_increased_security_of_biometric_data/prweb15907135.htm [https://perma.cc/FM3D-TBPL].

[454] *See generally* Yongjun Wang & Dimitrios Hatzinakos, *Face Recognition with Enhanced Privacy Protections*, *in* IEEE INT'L CONFERENCE ON ACOUSTICS, SPEECH AND SIGNAL PROCESSING 835 (2009).

[455] Erkin Zekeriya et al., *Privacy-Preserving Face Recognition*, *in* PRIVACY ENHANCING TECH.: LECTURE NOTES IN COMP. SCI. 5672 (Ian Goldberg & M. Atallah eds., 2009).

[456] Raymond, *supra* note 413, at 397–401.

[457] *See* McGeveran, *supra* note 447, at 981–82.

[458] *See* Kaminski, *supra* note 399, at 947.

3. Safe Harbor

While at present the FTC likely still lacks the ability to be a true "regulatory hammer,"[459] this Note suggests that the Child Online Privacy Protection Act (COPPA) is sign that the FTC has already been operating with a receptiveness for a broader collaborative approach.[460] Current FTC enforcement of COPPA suggests that the FTC is capable of a regulatory approach that balances the benefits of collaborative governance mechanisms with more restrictive privacy enforcement mechanisms including monetary fines.[461] In expanding the FTC's authority under COPPA, Congress required establishment of a co-regulatory regime through a safe harbor—tiered liability incentivizing compliance in the absence of regulatory action.[462] This accomplishes the dual interests of providing justification for greater authority to issue monetary penalties against "bad actors," while limiting the political blowback from requiring a large-scale expansion of the FTC.[463]

Under the safe harbor, a regulated entity may satisfy the requirements of rules by following a set of practice-based guidelines and being deemed in compliance by an authority authorized by the FTC.[464] The COPPA safe harbor, as an example, may have proven too lenient of a standard for compliance with minimal regulator

---

459 *Id.*

460 *See* Rubinstein, *supra* note 448, at 395–99.

461 *See id.*

462 15 U.S.C.A. § 6503 (Westlaw through Pub. L. No. 116-5); *see also* Rubinstein, *supra* note 448, at 416–17.

463 The FTC has brought twenty-eight cases and collected more than $10 million in civil penalties under COPPA. Peder Magee, *Happy 20th Birthday COPPA*, FTC (Oct. 22, 2018, 10:30 AM), https://www.ftc.gov/news-events/blogs/business-blog/2018/10/happy-20th-birthday-coppa [https://perma.cc/PJC5-M7QT].

464 Safe harbor programs must be approved by the FTC. The FTC will approve a safe harbor program only after a public notice and comment period and upon a finding that the safe harbor program's self-regulatory guidelines "meet the requirements" of the COPPA Rule. 15 U.S.C. § 6503(b)(2). Specifically, a safe harbor program must: (1) "provide substantially the same or greater protections for children" as the COPPA Rule; (2) implement "[a]n effective, mandatory mechanism for the independent assessment" of operators' compliance that includes "a comprehensive review" of each operators' "information policies, practices, and representations"; and (3) impose "[d]isciplinary actions for subject operators' non-compliance with self-regulatory program guidelines." 16 C.F.R. § 312.11(b) (Westlaw, Westlaw through 2019).

follow up beyond self-certification.[465] However, as Ira Rubinstein suggests, the safe harbor requirement can be used as a "carrot" available to parties that go beyond baseline requirements, pushing industry norms towards a more consumer privacy-respecting stance.[466] Using a safe harbor to incentivize greater sharing of privacy-performance enhancing practices and corporate governance methodologies can improve information available to market participants while rewarding performance with reduced liability and possible consumer good will.[467] In subsequent steps, a rule issued could empower a not-for-profit entity to provide benchmarking and certification of compliance.[468]

4. Supplemental Enforcement

A statute authorizing FTC regulation of facial recognition could supplement its effectiveness by allowing enforcement by state attorneys general. As Danielle Citron has noted, state attorneys general can address privacy-related harms effectively because they are closer to the problems, accountable to their voters, and face fewer bureaucratic requirements.[469] Similar to recent attorney general enforcement actions under COPPA,[470] FTC authority could

---

[465] *See, e.g.*, *New York AG Determines TRUSTe's COPPA Safe Harbor Program Falls Short*, WINSTON & STRAWN (Apr. 24, 2017), https://www.winston.com/en/privacy-law-corner/new-york-ag-determines-truste-s-coppa-safe-harbor-program-falls.html [https://perma.cc/7BX9-PMQ6] (discussing a lawsuit settled with the New York AG against a private COPPA safe harbor compliance where it failed to adequately review program members' websites to ensure compliance with COPPA). Additionally, this Note argues that setting compliance, as COPPA does, exclusively on notice-based principles does little to change overall practices.

[466] *See* Rubinstein, *supra* note 448, at 418–19.

[467] *See* KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 246 (2015) ("Our research suggests instead that the countries that pushed more of the responsibility for meaningfully defining, interpreting, and enforcing privacy back toward corporations were rewarded with richer firm practices.").

[468] *See* Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S J.L. & POL'Y FOR INFO. SOC'Y 723, 748 (2004) ("Without benchmarks, self-regulation and regulation, for that matter, have no clear metrics for measuring success.").

[469] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 750 (2016).

[470] *See, e.g.*, Sapna Maheshwari, *Oath Agrees to $5 Million Settlement Over Children's Privacy Online,* N.Y. TIMES (Dec. 3, 2018), https://www.nytimes.com/2018/12/03

be supplemented by classifying a violation of facial recognition rules as a *per se* "unfair or deceptive act or practice" allowing for state level enforcement under UDAP statutes.[471] State attorneys general, by supplementing the investigative and enforcement resources of the FTC, can emphasize the importance of compliance without creating additional uncertainty of balkanized or contradictory privacy regulations.

CONCLUSION

Governing facial recognition technology is difficult. The technology is inherently opaque and in tension between anxieties of digital instrumentalization and technological idealism. However, corporate surveillance in retail risks creating extensive consumer profiles that can undermine important civil liberties, and which consumers cannot easily avoid or adequately manage. Facial recognition needs stringent regulation to protect the public interest. Taking only an individual-rights approach risks failing to correct systemic problems while increasing the self-management requirements of consumers who are already susceptible to a widening information deficit. The "light touch" self-regulatory model risks being outpaced by technological change and overly permissive standards. This Note finds that movement towards a collaborative governance with an emphasis on negotiated rulemaking is required to provide the flexibility and expertise needed to regulate an emerging technology, while correcting incentives towards producing enforceable standards.

/business/media/oath-children-online-privacy.html [https://perma.cc/G9XF-CS6C] (discussing the settlement with the New York attorney general that is the largest a company has paid for a case associated with COPPA).

[471] UDAP stands for Unfair, Deceptive or Abusive Acts or Practices. *See* 15 U.S.C.A § 6504 (Westlaw, Westlaw through 2019).