For sale: Window to the Soul
Eye Tracking as the Impetus for Federal Biometric Data Protection

Ian Taylor Logan*

ABSTRACT

Eye tracking has existed as an important tool in numerous fields since the 1950s. Today, eye tracking hardware is smaller, cheaper, and more accurate than ever. As a result, eye tracking is anticipated to be ubiquitous within Virtual Reality (VR) headsets as a way to increase calibration accuracy, as well as the user's sense of immersion. Despite the importance of eye tracking data to the fields of marketing, behavioral science, and neuroscience, sparse literature has been published regarding the privacy implications of collecting such data from unwary consumers in an age where the collection of data through Internet-connected devices is largely unregulated. The purpose of this Comment is twofold: (1) to highlight a few of the numerous types of sensitive information that can be derived from eye-tracking data, and (2) to demonstrate an urgent requirement for legislation that comprehensively protects biometric identifiers from sale and exploitation.

The current pace of legislative enactment (itself a dramatic foil to the explosive rate of technological innovation) indicates that the best way to promote user privacy as well as innovation is to promulgate laws that create a right of personal privacy in biometric identifiers, instead of laws that regulate technology. Several statutes designed to regulate technology, rather than protecting the data it can collect, have proven that such schemes are minimally effective at best, and require constant amendment and re-negotiation to the point of impotence. This Comment argues that if privacy rights are established regarding biometric identifiers, technological innovation will be welcomed with less friction, allowing for

*J.D. Candidate, The Pennsylvania State University, Penn State Law, 2019. The writer wishes to thank Professor Anne McKenna for her invaluable expertise, Melissa Blanco for her patience and devotion in editing, the staff of *Penn State Law Review*, as well as the friends, family, and loved ones who offered support as this Comment took shape.

more rapid growth in a market supported by eager and informed consumers.

Table of Contents

I. INTRODUCTION 781
II. BACKGROUND 782
A. Biometric Data and its Applications 783
B. Eye Tracking Within the Internet of Things 786
C. A Lack of Federal Biometric Privacy Protection 788
1. Federal Trade Commission 789
2. Children's Online Privacy Protection Act 791
3. Developing Innovation and Growing the Internet of Things Act 791
D. State Biometric Privacy Protection 792
1. Illinois & the Biometric Information Privacy Act 792
2. Vindication of Biometric Rights under BIPA 793
a. Facebook 793
b. Shutterfly 795
3. California 796
a. California Online Privacy Protection Act 796
b. The California Consumer Privacy Act of 2018 797
4. Other State Legislation 799
E. International Protection of Biometric Data 800
1. General Data Protection Regulation 800
III. ANALYSIS 802
A. Biometric Data is Uniquely Sensitive 803
B. Protection of Biometric Data is a Right, Not an Option 804
C. The Federal Government is Currently Inadequate in its Biometric Protection 806
D. The Federal Government is Poised to Support a National Statute Protecting Biometric Data 806
IV. RECOMMENDATION 807
A. The Statute Must Provide Users a Right to Their Data 808
B. The Statute Must Protect Biometric Data Specifically 809
C. The Statute Must Provide for a Private Right of Action 810
V. CONCLUSION 810

I. INTRODUCTION

In 2013, Alicia Puente Cackley, then Director of Financial Markets and Community Investment for the U.S. Government Accountability Office, addressed the Senate Committee on Commerce, Science, and Transportation. In her words:

> The Federal laws that address the types of consumer information that can be collected and shared are not comprehensive. Under most circumstances, information that many people may consider very personal or sensitive can be collected, shared, and used for marketing. This can include information about physical and mental health, income and assets, political affiliations, and sexual habits and orientation.[1]

In the years since Cackley's address, her causes for concern have not abated; the perils associated with data privacy have only become more dire as technology becomes more engaging, pervasive, and invasive.[2]

Virtual and Augmented Reality (VR, AR) have existed at the periphery of the commercial technology market for decades.[3] As hardware becomes less expensive and software more sophisticated, society stands at the threshold of a massive cultural shift. No longer a question of *if*, but *when*, commercial VR presents a new vehicle by which creators, architects, retailers, and advertisers can reach consumers. While fervor for VR and AR bubbles beneath the surface of the mainstream, the federal government seems blind to the inevitable shift in implications of this new technology.

Cackley's remarks reflect the understanding that the Internet has developed into an unregulated playground for companies, engendering concerns about what sorts of consumer information can be collected, analyzed, sold or otherwise exploited.[4] Without regulation, targeted advertising has become more prevalent and more relevant to consumers,

1. *What Information Do Data Brokers Have On Consumers and How Do They Use It?: Hearing Before the S. Comm. on Commerce, Sci., & Transp*., 113th Cong. 60 (2013) [hereinafter *Data Brokers Hearing*].

2. *See infra* Section II.A.

3. *See* Craig E. Engler, *Affordable VR by 1994*, COMPUTER GAMING WORLD, Nov. 1992, at 80, 80, http://bit.ly/2LcWxvm. In 1992, several companies including Nintendo, Spectrum HoloByte, Visions of Reality, and Sense8 were working on hardware and software for VR. *Id.* Virtuality, the VR benchmark at the time, was designed by W Industries. *Id.* Companies rumored to be creating content for VR included Walt Disney and MCA (now Universal Pictures Home Entertainment). *Id.* at 81. It was speculated that commercially viable, in-home VR systems would be available by 1994. *Id.*

4. *Data Brokers Hearing, supra* note 1, at 6–7 (Staff Rep. for Sen. Rockefeller, Chairman, S. Comm. on Commerce, Sci., & Transp.) (offering a sample of information collected by data brokers including personal characteristics and preferences, health and financial information, vehicle, ailments, pets and shampoo purchases).

but increased revenue in the data mining industry has sparked debate over the balance between consumer and company benefit of data use.[5]

Debates about benefits conferred to consumers seldom account for the deeply personal nature of some of the most valuable consumer data.[6] Likewise, the benefits of more relevant advertisements do nothing to mitigate the fact that consumers, by and large, have no say as to what information is collected, to whom it is sold, and how it is used after its collection.

Consumer data has been collected, analyzed, and sold for decades,[7] and its use is often seen as an imperative for competitive businesses to thrive.[8] Deeply entrenched in today's online business paradigm, a substantial decline in data collection is beyond the realm of reasonable possibility. However, the potential of VR to drastically shift the ways in which society consumes digital content calls for federal legislation to protect a specific and acutely sensitive form of consumer data: biometrics.[9]

This Comment will begin with a discussion of the various applications of eye-tracking data and its place in consumer technology, leading into a discussion of state, national, and international biometric data protection.[10] The following section will offer an analysis of the inadequacies of the current federal data protection framework.[11] The final section will advocate for the enactment of a federal biometric data protection statute, listing several components that are imperative for a comprehensive and effective law.[12]

II. BACKGROUND

While eye-tracking data is one of the most sensitive forms of data, the eyes are far from the most frequently-exploited form of biometric

5. *See id.* at 65 (statement of Alicia Puente Cackley, Dir. of Fin. Mkts. & Cmty. Inv., U.S. Gov't Accountability Office) ("Advertising representatives noted that targeted marketing and advertising helps underwrite applications and services available free to consumers. Some resellers said that targeted behavioral advertising gives consumers information relevant to their specific interests, needs, or preferences. However, some privacy advocates believe that consumer benefits have been overstated."); *cf.* John Shaeffer, *The Economics of Online Privacy*, FORBES (Mar. 26, 2012, 01:19 PM), https://bit.ly/2AlbIia (arguing many privacy advocates are out of touch with what consumers want, and that opt-in data tracking defaults would decimate the current online advertising paradigm).

6. *See infra* Section II.A.

7. *Data Brokers Hearing, supra* note 1, at 7 (Staff Rep. for Sen. Rockefeller, Chairman, S. Comm. on Commerce, Sci., & Transp.).

8. *See* Thomas H. Davenport, *Competing on Analytics*, HARV. BUS. REV. (Jan. 2006), https://hbr.org/2006/01/competing-on-analytics.

9. *See infra* Section IV.

10. *See infra* Section II.

11. *See infra* Section III.

12. *See infra* Section IV.

identifiers.[13] Currently finger-prints and face-prints are among the more popular, known for their use in unlocking phones or tagging friends in photos.[14] As VR and AR products develop, however, eyes may become a key identifier of tech users.[15]

A. Biometric Data and its Applications

Biometrics measure "physiological characteristics like—but not limited to—fingerprint, iris patterns, or facial features that can be used to identify an individual."[16] While eye-tracking data takes many forms,[17] iris and retina scans[18] are used to identify an individual like a fingerprint.[19] Unlike a fingerprint, behavioral and cognitive information can be derived from eye tracking,[20] pupillometry,[21] and spontaneous blink rate.[22]

Eye tracking data is collected when the saccades[23] and fixations of the eye are captured by a beam of near-infrared light bouncing off the

13. *See* Bob Violino, *Biometric Security is on the Rise*, CSO (Mar. 3, 2015, 3:48 AM), https://bit.ly/2ljRGPw.

14. *Id.*; *see also Fingerprints: The Most Popular Biometric*, INAUTH (Jan. 9, 2017), https://bit.ly/2S1UHiP.

15. Danny Thakkar, *Top Five Biometrics: Face, Fingerprint, Iris, Palm and Voice*, BAYOMETRICS (Jan. 23, 2017), https://bit.ly/2OKNnq1 (ranking iris scanning as "the most accurate biometric system," despite substantial investment costs); *see also* TOBII GAMING, https://tobiigaming.com/ (last visited Nov. 18, 2018) (offering multiple forms of eye-tracking integration, and over one hundred eye-tracking-equipped PC games).

16. *Biometrics*, NAT'L INST. OF STANDARDS & TECH. (Feb. 2, 2010), https://www.nist.gov/programs-projects/biometrics.

17. *See* Maria K. Eckstein et al., *Beyond Eye Gaze: What Else Can Eyetracking Reveal About Cognition and Cognitive Development?*, 25 DEV. COGNITIVE NEUROSCI. 69, 70–73 (2017) (delineating eye gaze, pupillometry and spontaneous blink rate as common ocular measurements and fixation, saccades, and scan path as gaze metrics).

18. *See* CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE § 31:10 (3d ed. 2007). An iris scan "measures the outer and inner edge of the iris as well as hundreds of other sections," allowing researchers to record minute changes in dilation. *Id.* Retina scans require "the individual [to] look directly into a beam of light, which reflects off the retina . . . and the scanner takes measurements of the pattern created by the reflected light," allowing researchers to record the viewer's eye movement and attention. *Id.* at § 31:9.

19. *See id* at § 31:9 (explaining how iris and retinal patterns "are unique, even between identical twins, and static enough to be used throughout life.").

20. *See generally* Dario D. Salvucci & Joseph H. Goldberg, *Identifying Fixations and Saccades in Eye-Tracking Protocols*, *in* PROCEEDINGS OF THE EYE TRACKING RESEARCH AND APPLICATIONS SYMPOSIUM 71, 71 (2000) (offering several contexts in which researchers have utilized eye tracking).

21. *See generally* Simona Graur & Greg Siegle, *Pupillary Motility: Bringing Neuroscience to the Psychiatry Clinic of the Future*, CURRENT NEUROLOGY & NEUROSCI. REPS., (June 19, 2013), https://doi.org/10.1007/s11910-013-0365-0 (discussing the myriad applications of pupil measurement in psychiatry and other fields).

22. *See* Eckstein et al., *supra* note 17, at 80.

23. "Saccades are rapid, ballistic movements of the eyes that abruptly change the point of fixation." *Types of Eye Movements and Their Functions*, *in* NEUROSCIENCE (Dale Purves

retina as the eye moves across a screen or environment.[24] This data can then be stored for further analysis.[25] Eye movement, like breathing, can be controlled by the individual, but is more commonly a subconscious,[26] or reflexive[27] movement, resulting in more "truthful" data than that gathered in a survey or a study of conscious decision-making.[28] Stated another way, where a person looks may provide more accurate information than a survey or interview. One study suggests that "gaze reveals developing preferences for moral choices," and that through eye tracking a moral decision can be anticipated, manipulated, and even changed based on patterns of eye movement and timed interruption of the thought process.[29] Changes in pupil dilation, or pupillometry, has also been used to study the process of decision-making.[30]

The same technology that can track eye movement can also measure pupil dilation,[31] and is used to study neurocognitive arousal as it applies to task-engagement.[32] Studies indicate that certain pupil dilation anomalies are indicative of psychiatric conditions such as depression, and can be used to identify non-depressed individuals who are prone to depression.[33] Both pupillometric and gaze-tracking data can be used to identify "key features" of Autism Spectrum Disorder,[34] "such as empathy in adults and children as young as two years old."[35]

In addition, certain systemic diseases like Parkinson's and Alzheimer's can have specific impacts on eye movement that can be

et al. eds., 2d ed. 2001) (ebook) [hereinafter *Eye Movements*], https://www.ncbi.nlm.nih.gov/books/NBK10991/.

24. *What is Eye Tracking and How Does It Work?*, IMOTIONS (Jan. 12, 2016) [hereinafter *What is Eye Tracking?*], https://imotions.com/blog/eye-tracking-work/ ("Near-infrared light is directed towards the center of the eyes . . . causing visible reflections [which] are tracked by a camera.").

25. *Id.*

26. *See* Mo Costandi, *How Your Eyes Betray Your Thoughts*, THE GUARDIAN (June 2, 2015), http://bit.ly/2RQ846n.

27. *See Eye Movements*, *supra* note 23.

28. *See* Adi Robertson, *Tobii Lets You Play Assassins Creed With Your Eyes*, VERGE (Jan. 8, 2016, 6:19 PM), https://www.theverge.com/2016/1/8/10736510/tobii-eye-tracking-assassins-creed-vr-ces-2016.

29. *See* Philip Pärnamets et al., *Biasing Moral Decisions by Exploiting the Dynamics of Eye Gaze*, 112 PROC. NAT'L ACAD. SCIS. 4170, 4173 (2015).

30. *See id*.; *see also* Graur & Siegle, *supra* note 21.

31. *Are Pupil Size Calculations Possible With Tobii Eye Trackers?,* TOBII PRO [hereinafter *Tobii Eye Trackers*], https://bit.ly/2CYhGbh (last visited Dec. 9, 2018).

32. *See* Peter R. Murphy et al., *Pupil-Linked Arousal Determines Variability in Perceptual Decision Making*, PLOS COMPUTATIONAL BIOLOGY, Sept. 2014, at 1, 6 https://doi.org/10.1371/journal.pcbi.1003854.

33. *See* Graur & Siegle, *supra* note 21.

34. *See id*.

35. *Id*.

observed in eye-tracking data.[36] A 2015 release from Johns Hopkins Medicine notes that eye-tracking goggles are superior to MRI and CT scans for identifying evidence of stroke.[37] Another study asserts that, "[d]espite being an indirect measure of brain function," eye tracking offers more advantages than electroencephalograms (EEG) and functional magnetic resonance imaging (fMRI) in cognitive studies.[38]

Key differences between eye-tracking studies are now found in how the data is collected, but rather how the raw data is analyzed in conjunction with the stimuli used to elicit the data.[39] Theoretically, the same tools can be used to diagnose autism as can be used to determine which of two soup can labels is more attention-grabbing.[40] This type of information has obvious and significant value to employers, insurance providers, pharmaceutical companies, and others within the health care field, all of which are currently able to purchase this data from private data collection firms without federal restriction.[41]

Outside the realm of diseases and disorders, behavioral scientists have used eye tracking to study the subtle differences in how individuals of different sexes respond to sexual stimuli.[42] Study results suggest that

36. *See* Daniele Cruz & Erin L. Boyle, *Neurologic Disorders Have Varied Ocular Symptoms*, OCULAR SURGERY NEWS (July 1, 2006), https://bit.ly/2JfgAs9.

37. *Eye-Tracking Devices Helps Detect Stroke*, JOHNS HOPKINS MED. (Sept. 1, 2015), https://bit.ly/2PegKoX. For $40, the eye-tracking procedure boasts 99 percent accuracy compared to the reported 80 percent accuracy of a $1500 MRI or the 16 percent accuracy of a $300 CT scan. *Id.*

38. *See* Eckstein et al., *supra* note 17, at 70. The mobility and portability of the headsets or screen trackers make for study environments more natural and comfortable than the "noisy and space-restricted environment of the MRI scanner." *Id.* Equipment can also be brought to schools, hospitals, and care centers, giving studies a broader, more diverse study pool. *Id.* Importantly, accuracy does not suffer, as the eye tracking sampling rates are fast enough (up to 2,000 measurements per second as of 2016) to rival the temporal resolution of an EEG. *Id.*

39. *See Tobii Eye Trackers*, *supra* note 31 (Tobii eye tracking hardware collects both occulomotor and pupillometric data); *see also Tobii Pro Studio*, TOBII PRO [hereinafter *Tobii Pro Studio*], https://bit.ly/2J9siEC (Tobii Pro Studio software boasts its efficacy in studying marketing and research as well as psychology.).

40. *Cf. Tobii Pro Studio*, *supra* note 39.

41. Ieuan Jolly, *Data Protection in the United States: Overview,* THOMPSON REUTERS PRACTICAL LAW (Oct. 1, 2018), https://tmsnrt.rs/2J8Ik1r ("In the US, there is no single, comprehensive federal (national) law regulating the collection and use of personal data . . . Instead, the US has a patchwork system of federal and state laws and regulations that can sometimes overlap, dovetail and contradict one another.").

42. *See* Amy D. Lykins et al., *Sex Differences in Visual Attention to Erotic and Non-Erotic Stimuli*, 37 ARCHIVES SEXUAL BEHAV. 219, 226 (2008) (finding that heterosexual men look at the opposite sex significantly longer than heterosexual women, and heterosexual women seem to "disperse their attention evenly between opposite and same sex figures" when presented in an erotic context). *See generally* Heather A. Rupp & Kim Wallen, *Sex Differences in Viewing Sexual Stimuli: An Eye-Tracking Study in Men and Women*, 51 HORMONES & BEHAV. 524 (2007) [hereinafter Rupp & Wallen, *Sex Differences*] (noting a measurable difference in the pupillary responses of men, women,

purchasers of biometric data could determine the sexual preference, propensities, and perhaps contraception use of an individual based on eye-tracking data.[43] Studies of women and men, as well as female-centric eye tracking studies, show that hormone fluctuation impacts eye-gaze and pupil dilation.[44] These minute fluctuations can point to when, during a menstrual cycle, the pupillometric data was collected.[45] Use of oral contraception (birth control) has been detectable in such studies as well.[46] Without question, sexual orientation, hormone fluctuation, and use of contraception are as personal to an individual as they are valuable to a company. Ignoring the intrinsically private nature of such information, to leave companies free to exploit it is indefensible.

B. Eye Tracking Within the Internet of Things

Although eye tracking is not yet ubiquitous in consumer tech, its impact may be massive. Rapid developments in technology have created a pervasive, and somewhat nebulous network of devices referred to as the Internet of Things (IoT).[47] The moniker refers to the interconnectivity of any devices—smart-watches, refrigerators, vehicles, headphones, and smart assistants—that are able to connect and assimilate into the broad network of the Internet.[48] As VR and AR software, headgear, and

and women on contraceptives to sexual stimuli). Patterns involving temporal length of gaze or the division of attention between figures of different sexes may betray the sex of the viewer, if not the viewer's sexual preferences. *See* Gerulf Rieger & Ritch C. Savin-Williams, *The Eyes Have It: Sex and Sexual Orientation Differences in Pupil Dilation Patterns*, PLOS ONE, Aug. 2012, at 1, 6–8, https://bit.ly/2Yoruq0.

43. Rupp & Wallen, *Sex Differences*, *supra* note 42, at 525; *see also* Rieger & Savin-Williams, *supra* note 42, at 6–8.

44. *See* Bruno Laeng & Liv Falkenberg, *Women's Pupillary Responses to Sexually Significant Others During the Hormonal Cycle*, 52 HORMONES & BEHAV. 520, 527 (2007) (explaining that "by monitoring the physiological parameter of pupillary size we can measure women's changes in attention towards targets of sexual desire and successfully tap into a high-level psychological appraisal of affective–sexual interest"); Rupp & Wallen, *Sex Differences*, *supra* note 42, at 524. *See generally* Rieger & Savin-Williams, *supra* note 42.

45. Laeng & Falkenberg, *supra* note 44, at 527 ("The findings confirmed the presence of cyclic differences in pupillary diameters while watching facial portraits of sexually interesting individuals."). "Cyclic" here refers to the ovulatory, luteal, and menstrual phases of the menstrual cycle. *Id.*

46. *See id.* ("Remarkably, the participants using contraceptive pills did not show cyclic fluctuations of pupil sizes.").

47. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 6 (2015) [hereinafter FTC, INTERNET OF THINGS], http://bit.ly/2Eexg2f (defining the IoT as "'things' such as devices or sensors—other than computers, smartphones, or tablets—that connect, communicate or transmit information with or between each other through the Internet.").

48. Jacob Morgan, *A Simple Explanation of the Internet of Things*, FORBES (May 13, 2014), https://bit.ly/2Akj8SD.

spectacles make their way into the commercial market, the use of these devices for gaming, home entertainment, and creative expression will demand Internet connectivity. Tobii, one of the foremost purveyors of eye-tracking equipment, has been integral to the introduction of eye tracking to virtual reality hardware, and already markets laptops equipped with eye-tracking software to enhance research and gaming experiences.[49] The inextricable link between games and the web ensures that VR and AR will be part of the estimated 50 billion devices that will fall under the expansive umbrella of the IoT by 2020.[50]

Increases in accuracy and sophistication, coupled with reasonable prices[51] make eye tracking features appealing to both marketers and entertainers.[52] For example, foveated rendering (a process that uses eye tracking to understand where and how the human eye focuses to make content more immersive and visuals more life-like) has been applied in VR software to enhance video game environments and training simulations.[53] Foveated rendering relies on pupillary motility and necessarily requires the collection of biometric data any time a user engages with a virtual or augmented environment.[54] The remarkable increase in calibration and immersion made possible by eye tracking all but ensures that it will become standard in commercial VR and AR hardware.[55]

Advertising and marketing companies have used eye-tracking technology for years to analyze the efficacy of supermarket layouts, product labels, advertisements, and displays.[56] Compounded with studies of eye movement that reveal individual details about attention, arousal,

49. Devindra Hardawar, *Tobii Proves that Eye Tracking is VR's Next Killer Feature*, ENGADGET (Jan 13, 2018), https://engt.co/2S7KMtd.

50. FTC, INTERNET OF THINGS, *supra* note 47, at 1; *see also* S. 88, 115th Cong. §2(a)(2) (2017).

51. *What is Eye Tracking?*, *supra* note 24; *see also Eye Tracker Prices – An Overview of 15+ Eye Trackers*, IMOTIONS (Jan. 12, 2016), https://bit.ly/2OBICnA.

52. *See* Salvucci & Goldberg, *supra* note 20.

53. Paul Miller, *Nvidia's Foveated Rendering Tricks for VR Could Improve Graphics and Immersion*, VERGE (Jul 22, 2016, 5:23 PM), https://bit.ly/2AlVPI5. Foveated rendering processes the path of the viewer's pupils and maintains high quality imagery in their direct line of sight, while the image at the viewer's periphery and beyond their sight renders at a lower quality. *Id.* This process creates a viewing experience more akin to how the eye process images, and the use of lower quality images allows the headset to operate more efficiently on slower processors. *Id.*; *see also* Hardawar, *supra* note 49.

54. Hardawar, *supra* note 49.

55. *Id*. (noting that "[a]ccurate eye tracking delivers a better sense of presence . . . the ultimate goal for virtual reality."). Tobii CEO Henrik Eskilsson noted that VR will eventually require eye tracking. *Id*.

56. *See Marketing and Consumer Research*, TOBII PRO (2017), https://bit.ly/2OBIFQi (discussing different marketing studies in which eye tracking has been utilized).

decision-making, and memory,[57] eye-tracking data is an immensely valuable resource to marketers in pursuit of the most engaging and efficient advertising campaigns.[58]

Although marketing and neurology may seem like disparate fields, eye-tracking studies within both rely on the same fundamental technology and the same form of biometric data to learn about an individual.[59] When eye-tracking data is collected from a device, such as a VR headset or AR spectacles, this data can be analyzed by companies[60] against extant eye-tracking studies to extrapolate information about users that was not volunteered nor related to the device from which the data was collected.[61] Stated another way, a marketing agency could theoretically purchase data from a VR video game producer, compare the eye-tracking data to behavioral studies about teen impulse control, and use that information to sell clothing to that video game's target demographic. The broad application and intrinsic value of such personal data combines to increase incentives for companies to retain, use, and sell eye-tracking data in the absence of prohibitive laws.

C. A Lack of Federal Biometric Privacy Protection

Despite its value and sensitivity, the federal government currently has no comprehensive laws in place to protect the biometric data of U.S. citizens. In 2013, the Senate Commerce Committee issued a report on the status of individual privacy and the data collected by "data brokers."[62] The report acknowledged:

> Current law generally allows resellers [of data] to collect personal information from sources including warranty registration cards, surveys, and online sources such as discussion boards, social media

57. Eckstein, *supra* note 17, at 87.

58. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 37 (2010) [hereinafter FTC, PROTECTING CONSUMER PRIVACY], http://bit.ly/2zRagDC ("[T]he more information that is known about a consumer, the more a company will pay to deliver a precisely-targeted advertisement to him.").

59. *See generally What's Your Field?*, TOBII PRO (2017), https://bit.ly/2LZbggx (suggesting that any Tobii product, utilizing the same fundamental technology, will assist in any realm of research or study).

60. *See* FTC, INTERNET OF THINGS, *supra* note 47, at 15.

61. *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 93 (2014) ("[E]ach type of consumer sensor (e.g., personal health monitor, automobile black box, or smart grid meter) can be used for many purposes beyond that particular sensor's original use or context, particularly in combination with data from other [IoT] devices.").

62. FTC, PROTECTING CONSUMER PRIVACY, *supra* note 58, at 68 (defining data brokers as "companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes . . . .").

> sites, blogs, and web browsing histories and searches. Current law does not require disclosure to consumers when their information is collected from these sources.[63]

The committee further announced that "no federal statute provides consumers the right to learn what information is held about them and who holds it for marketing or look-up purposes."[64] Nor does any law require companies selling consumer data "to allow individuals to review [their] personal information . . . control its use, or correct it."[65] As a result, the collection, dissemination, and regulation of consumer data is largely left in the hands of the companies and data brokers who profit from collection, analysis, use, and resale of consumer data, including biometrics.

1. Federal Trade Commission

The agency predominantly responsible for consumer privacy protection is the Federal Trade Commission (FTC). Section 5 of the FTC Act of 1914[66] ("FTC Act") declares "unfair or deceptive acts or practices in or affecting commerce"[67] to be unlawful-a broad authority, most often applied (in the realm of privacy) to cases involving the collection of data that is inconsistent with a particular company's terms of agreement.[68]

The FTC's jurisdiction reaches nearly all facets of trade affecting commerce, not simply matters of data privacy.[69] The array of issues handled by the FTC means data privacy claims are not the sole concern of the FTC. As such, investigations are typically launched on behalf of large classes of plaintiffs.[70]

63. *Data Brokers Hearing*, *supra* note 1, at 60 (statement of Alicia Puente Cackley, Dir. of Fin. Mkts. & Cmty. Inv., U.S. Gov't Accountability Office).

64. *Id.* at 59.

65. *Id*.

66. Federal Trade Commission Act of 1914 § 5, 15 U.S.C. § 41 (2012 & Supp. 2017).

67. 15 U.S.C. § 45(a)(1) (2012 & Supp. 2017).

68. *See, e.g.*, *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, FED. TRADE COMM'N (Aug. 9, 2012), https://bit.ly/1qz3quA (describing how Google directly violated self-imposed protocol it had conveyed to customers, knowing that customers would rely on that information); *Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users' Profile Information*, FED. TRADE COMM'N (Dec. 14, 2016) [hereinafter *Ashley Madison FTC Settlement*], https://bit.ly/2gCXcFf ("[T]he defendants assured users their personal information . . . was private and securely protected . . . [b]ut the FTC alleges the security of AshleyMadison.com was lax.").

69. *See* 15 U.S.C. § 45(a).

70. *What We Do,* FED. TRADE COMM'N, https://bit.ly/2oLywjq (last visited Dec. 29, 2018).

Further, the FTC Act reserves the right to bring legal action to the FTC,[71] the U.S. Attorney General,[72] or in some cases a State Attorney General.[73] Without a private cause of action, citizens have no power to enforce the Act and protect their information on an individual basis.

Seemingly aware its lack of authority over many primary collectors of private data, the FTC published "best practices" for the collection and protection of consumer information.[74] While the best practices encourage data collectors to adopt more transparent[75] and consumer-friendly[76] practices, the best practices are in no way enforceable. Without legal enforceability, any heightened regulation of user data is left to the discretion of the companies collecting the data. After the Data Broker Accountability and Transparency Act of 2015[77] died in Congress, the FTC's best practices-initially seen as an outline for future federal legislation-became toothless suggestions to the $159 billion data broker industry[78]

One week after the announcement of the Equifax data breach,[79] however, the Data Broker Accountability and Transparency Act of 2017[80] was reintroduced in the Senate.[81] The proposed bill does not prohibit the collection or sale of any form of data; rather, the bill calls for greater ease for consumers to access and correct the sensitive data about them that companies are still free to collect and sell.[82]

71. 15 U.S.C. § 45(m)(1)(A).
72. *See id.* § 45(l).
73. *See id.* § 45b(e)(1).
74. *See* FTC, PROTECTING CONSUMER PRIVACY, *supra* note 58, 15–16.
75. *See id.* at 48–60.
76. *See id.* at 60–64.
77. Data Broker Accountability and Transparency Act of 2015, S. 668, 114th Cong. (2015).
78. *Data Brokers Hearing*, *supra* note 1, at 2 (statement of Sen. Rockefeller, Chairman, S. Comm. on Commerce, Sci., & Transp.).
79. *See Equifax Announces Cybersecurity Incident Involving Consumer Information*, EQUIFAX (Sept. 7, 2017), http://bit.ly/2RWBUpu.
80. Data Broker Accountability and Transparency Act of 2017, S. 1815, 115th Cong. (2017).
81. *In Wake of Equifax Data Breach, Blumenthal, Colleagues Introduce Legislation to Hold Data Broker Industry Accountable*, SEN. RICHARD BLUMENTHAL (Sept. 14, 2017), http://bit.ly/2UxJqJp.
82. Data Broker Accountability and Transparency Act of 2017, S. 1815, 115th Cong. § 4 (2017). As of the time of this publication, the Act has been introduced to the Senate without final decision. *See S.1815 - Data Broker Accountability and Transparency Act of 2017*, CONGRESS.GOV, https://bit.ly/2qUqtmy (last visited March 12, 2019).

2. Children's Online Privacy Protection Act

In contrast to the current protection of adult consumer data, the Children's Online Privacy Protection Act (COPPA)[83] regulates companies' ability to collect and use data created by or belonging to individuals below the age of 13.[84] COPPA, enforceable by the FTC, requires websites that knowingly collect data from children to, among other things, (1) provide notice of data collection and receive informed consent from parents and guardians,[85] (2) permit and abide by requests of parents to discontinue the use and collection of data,[86] and (3) "prohibit conditioning of a child's participation" on the child's giving of personal data beyond what is reasonably necessary to play the game, or use the service provided by the website.[87]

Promulgated in 1998, COPPA does not explicitly provide for the protection of most biometric data, nor the vehicles[88] by which such data is likely to be collected. The statute was amended in 2013 to include mobile apps,[89] however, the statute's broad language to regulate "operator[s] of website[s] and online service[s],"[90] still leaves open for debate the applicability of COPPA to new devices unforeseen by past lawmakers.

3. Developing Innovation and Growing the Internet of Things Act

While the significance of biometric protection seems to elude lawmakers, the unique characteristics and opportunities presented by the IoT seem to have their attention. In 2015, the U.S. Senate unanimously passed a resolution "calling for a national strategy for the development of the Internet of Things."[91] In response, the Developing Innovation and Growing the Internet of Things Act (DIGIT) was passed by the Senate and currently sits with the House of Representatives for review.[92] DIGIT empowers the Secretary of Commerce to create a working group to assess the current state of the IoT, as well as budgetary and logistical hurdles that

83. Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681-728 (1998) (codified at 15 U.S.C. § 6501–06 (2012 & Supp. 2017)).
84. 15 U.S.C. § 6502.
85. 15 U.S.C. § 6502(b)(1)(A).
86. 15 U.S.C. § 6502(b)(1)(B)(ii).
87. 15 U.S.C. § 6502(b)(1)(C).
88. For example, smartphones, wearable devices, and VR headsets.
89. *Revised Children's Online Privacy Protection Rule Goes Into Effect Today*, FED. TRADE COMM'N (July 1, 2013), https://bit.ly/2PKBy4h.
90. 15 U.S.C. § 6502(a)(1).
91. Developing Innovation and Growing the Internet of Things Act, H.R. 686, 115th Cong. § 2(a)(7) (2017).
92. *H.R. 686: DIGIT Act,* GOVTRACK, https://bit.ly/2yTuFqj (last visited Dec. 10, 2018).

could discourage the development of the IoT.[93] The duties of the working group also prioritize the development of methods by which federal agencies can benefit and reduce threat risks from use of the IoT.[94]

DIGIT also would establish a "steering committee" to advise the working group on "policies or programs" that, among other things, (1) "promote or are related to" privacy of IoT users, or those affected by it;[95] and (2) "may enhance" IoT security.[96] While such language instills hope, privacy policies may conflict with the overarching goal of *developing* the IoT, making protection of private citizens possible, but dubious.

D. State Biometric Privacy Protection

In the absence of adequate federal protection, state statutes have cropped up, addressing the need for more stringent and relevant privacy laws.[97] To date, only Illinois,[98] California,[99] Texas,[100] and Washington[101] have enacted statutes specifically tailored to the protection of biometric data, although a few other states have shown interest in enacting similar laws.[102]

1. Illinois & the Biometric Information Privacy Act

The first key statute enacted to comprehensively protect biometric data was Illinois's 2008 Biometric Information Privacy Act (BIPA).[103] The statute differs from today's federal notions of data regulation by addressing biometric data as something that can and should be protected,[104] rather than something that always has been, and thus will continue to be, collected, sold, and exploited.[105]

93. *See* H.R. 686 § 4(b)(1).
94. *See* id. § 4(b)(4).
95. *See id.* § 4(e)(2)(C)(i).
96. *See id.* § 4(e)(2)(C)(ii).
97. *See* Ted Claypool & Cameron Stoll, *Developing Laws Address Flourishing Commercial Use of Biometric Information*, BUS. L. TODAY (Am. Bar Ass'n), May 2016, at 1, 1–3, http://bit.ly/2QsiFaL.
98. 740 ILL. COMP. STAT. ANN. 14/1 (2008).
99. California Consumer Privacy Act of 2018, 2018 Cal. Legis. Serv. ch. 55 (West) (codified at CAL. CIV. CODE div. 3, pt. 4, tit. 1.81.5).
100. TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017).
101. WASH. REV. CODE § 19.375 (2017).
102. Claypool & Stoll, *supra* note 97, at 3; *Florida Proposes State Biometric Data Privacy Legislation*, HEALTH IT SECURITY (March 11, 2019), https://bit.ly/2u3yhE1; Katherine E. Deal et al., *Four More States Propose Biometric Litigation*, DRINKER BIDDLE (Feb. 14, 2017), https://bit.ly/2LCRHHK.
103. Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14 (2008).
104. *Id.* 14/10.
105. *See* S. 1815, 115th Cong. (2017); FTC, PROTECTING CONSUMER PRIVACY, *supra* note 58.

Notably, the statute (1) requires informed consent prior to data collection; (2) prohibits companies from profiting from consumer biometrics; (3) outlines data protection, retention, and destruction obligations; and (4) provides individuals with a right of action against BIPA violators.[106] To date, BIPA has not been used to assert a violation of biometric privacy violation regarding eye tracking, iris or retina scans, or pupillometry. However, several major companies have been successfully prosecuted for BIPA violations regarding facial scans[107]—a similarly sensitive form of biometric data.[108]

2. Vindication of Biometric Rights under BIPA

BIPA stands apart from other biometric statutes primarily because of its private right of action. This key distinction has allowed consumers to hold companies responsible for BIPA violations, while other statutes remain effectively useless to private citizens.[109]

a. Facebook

In *In re Facebook Biometric Info. Privacy Litig*., several Illinois citizens alleged that Facebook's face-scanning algorithm[110] violated BIPA by scanning and storing the biometric facial scans of thousands of users without their consent.[111] Initially filed in the Northern District of Illinois, Facebook removed to the Northern District of California and argued that BIPA did not apply to the case because the plaintiffs had all "accepted and agreed" to Facebook's terms of use, which stipulated a contractual choice-of-law provision, and were therefore subject to California law in any disputes with Facebook.[112] The court agreed unequivocally that plaintiffs were given adequate notice and had accepted and agreed to be parties to

106. 740 ILL. COMP. STAT. 14/15.

107. *See* Rivera v. Google, 238 F. Supp. 3d 1088, 1093–96 (N.D. Ill. 2017); *see also infra* Section II.D.2.a–.b.

108. *Nowhere to Hide*, THE ECONOMIST (Sept. 9, 2017), https://www.economist.com/leaders/2017/09/09/what-machines-can-tell-from-your-face.

109. *See infra* Section II.D.4.

110. Designed to recognize faces of friends to streamline the process of "tagging" those friends in photos.

111. In re Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1159 (N.D. Cal. 2016) (alleging the Tag Suggestion program violated BIPA because Facebook failed to (1) properly inform plaintiffs that their biometric identifiers were being collected and stored; (2) properly inform plaintiffs of the length of time and uses for which such data was collected; (3) provide a publicly accessible schedule outlining plans to permanently delete collected data; and (4) obtain written consent from plaintiffs to collect their biometric identifiers).

112. *Id.* at 1159.

the California choice-of-law provision.[113] However, the court ultimately found that the California choice-of-law provision was "contrary to a fundamental policy of Illinois,"[114] which gave Illinois a significantly greater interest in the outcome of the BIPA dispute.[115]

The court then addressed an ambiguity within the statute.[116] Facebook moved to dismiss the case, arguing that BIPA "excludes from the definitions of 'biometric identifier' and 'biometric information' (1) photographs and (2) any information derived from those photographs."[117] Facebook argued that the scans constituting biometric data were, "derived exclusively from uploaded photographs."[118]

The court denied the motion, noting that statutory interpretation demanded "the Court . . . view the statute as a whole, construing words and phrases in light of other relevant statutory provisions . . . ."[119] The court noted that, when viewed alongside the other sources marked for exclusion,[120] photographs referred to paper prints rather than digital images.[121] The court held that this interpretation of the statute aligned with the "statute's focus . . . on newer technology like scans of face geometry, whose 'full ramifications' are not known."[122] The court further supported its decision by observing that the same decision was reached when the same question was raised in the Northern District of Illinois.[123]

113. *Id.* at 1167.

114. *Id.* at 1169. The court cited specific language of BIPA to highlight the enumerated policy concerns of the Illinois legislature:

> (1) "Biometrics are unlike other unique identifiers . . . therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions"; (2) "[t]he full ramifications of biometric technology are not fully known"; and (3) "[t]he public welfare, security and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information".

Id. (citations omitted) (quoting 740 ILL. COMP. STAT. ANN. 14/1 (2008)).

115. *Id.* ("[I]f California law is applied, the Illinois policy of protecting its citizens' privacy interests in their biometric data . . . would be written out of existence."). The court balanced the "strong policy considerations favoring the enforcement of freely negotiated choice-of-law clauses" with the likelihood "that the chosen law is contrary to a fundamental policy" of BIPA, and that Illinois "has a materially greater interest in the determination of the matter," in accord with the test set out in *Wash. Mut. Bank v. Super. Ct.*, 15 P.3d 1071 (Cal. 2001). *In re Facebook*, 185 F. Supp. 3d at 1168–69.

116. *Id.* at 1170.

117. *Id*.

118. *Id*.

119. *Id.* at 1171 (citing People v. Gutman, 959 N.E.2d 621, 624 (Ill. 2011)).

120. *See* 740 ILL. COMP. STAT. 14/10 (2008) (explaining that exclusions included writing samples, demographic information, identifiable tattoos, and physical descriptors).

121. *In re Facebook*, 185 F. Supp. 3d at 1171.

122. *Id*. (quoting 740 ILL. COMP. STAT. 14/5(f) (2008)).

123. *Id.* at 1171 (citing Norberg v. Shutterfly, 152 F. Supp. 3d 1103 (N.D. Ill. 2015)).

b. Shutterfly

Shutterfly, an online photo sharing, organizing, and printing service,[124] has been the defendant party twice in cases concerning BIPA violations.

In *Norberg v. Shutterfly*,[125] the Illinois judiciary's first pass at interpreting BIPA,[126] the plaintiff alleged that Shutterfly collected biometric data via facial recognition technology from individuals who were not active users of Shutterfly's services.[127] Shutterfly filed a motion to dismiss on the grounds Facebook would assert the following year-that "BIPA excludes biometric identifiers . . . derived from photographs," and as a result, the plaintiff had not stated a claim for which relief could be granted.[128] In a brief opinion denying the motion, the court concluded that the plaintiff filed a plausible claim because he was not a customer of the website and was therefore not presented with a written biometrics policy, nor given the opportunity to consent.[129]

Similarly, in *Monroy v. Shutterfly*,[130] the plaintiff, a non-member and non-user of Shutterfly's services, alleged that a citizen of Illinois uploaded a photograph of the plaintiff and entered his name when prompted to tag the face identified in the image.[131] According to the complaint, Shutterfly's facial recognition software created a "highly detailed 'map' or 'template'" of the plaintiff's facial geometry based on "unique contours of his face and the distances between his eyes, nose and ears."[132] This facial geometric template allowed Shutterfly to extract and store information about the plaintiff's age, gender, race, and geographic location without notice or consent.[133]

Similar to its defense in *Norberg*,[134] Shutterfly asserted that, although a "scan of face geometry" was collected, BIPA excludes from its protective scope any biometric information derived from photographs.[135] To support this assertion, Shutterfly argued that all other terms included in BIPA's definition of "biometric identifier" involve "in-person

124. *Norberg*, 152 F. Supp. 3d at 1105–06.
125. Norberg v. Shutterfly, 152 F. Supp. 3d 1103 (N.D. Ill. 2015).
126. *Id.* at 1106.
127. *Id.*
128. *Id.* at 1105.
129. *Id*.
130. Monroy v. Shutterfly, No. 1:16-cv-10984, 2017 WL 4099846 (N.D. Ill. Sept. 15, 2017).
131. *Id.* at *1.
132. *Id.*
133. *Id.*
134. *Norberg*, 152 F. Supp. 3d at 1106.
135. *Monroy*, 2017 WL 4099846, at *2.

processes."[136] Dispensing with this argument,[137] the court observed that Shutterfly's narrow interpretation of the statute would "leave little room for the law to adapt and respond to technological development." The Illinois court reiterated the sentiments of Judge Edmond Chang in a similar BIPA violation case against Google,[138] stating, "[A]dvances in technology are what drove the Illinois legislature to enact the Privacy Act in the first place, [so] it is unlikely that the statute sought to limit the definition of biometric identifier by limiting how the measurements are taken."[139]

In practice, BIPA's private right of action and provision for protection of individual biometric information (as opposed to regulation of technology) shows a cogent and effective approach to lawmaking in the face of rapid and unpredictable advancements in the tech industry. BIPA seems to benefit from a clear policy and straightforward language, despite some difficulty with the interpretation of the term "photograph."[140] Thus, BIPA presents a promising template for a future federal biometric protection bill.

3. California

The commercial technology industry in California has prompted several legislative actions. Although these efforts are not always successful in protecting consumers or even clarifying consumer rights, two legislative enactments exemplify technology's impact on California's approach to law making.

a. California Online Privacy Protection Act

In 2004, the California Online Privacy Protection Act[141] (CalOPPA) became the first state law requiring websites and online services "that collect[] personally identifiable information . . . about individual consumers" to implement and "conspicuously post [a] privacy policy" on their websites.[142] While privacy protection remains the goal of the statute, its definition of "personally identifiable information" does not include language that expressly or otherwise protects biometric information.[143]

136. *Id.* at *4 (noting that "biometric identifiers" include "retina or iris scans, fingerprints, voiceprints, and hand scans," in addition to facial geometric scans.).
137. *Id.* at *4 ("It appears that fingerprints and retinal scans can be obtained from images and photographs.").
138. Rivera v. Google, 238 F. Supp. 3d 1088 (N.D. Ill. 2017).
139. *Monroy*, 2017 WL 4099846, at *2 (citing *Rivera*, 238 F. Supp. 3d at 1096).
140. *See supra* Section II.D.2.
141. California Online Privacy Protection Act, CAL. BUS. & PROF. CODE § 22575–79 (West 2018).
142. *Id.*
143. *Id.* § 22577.

The state's failure to anticipate the rapid evolution of technology prompted a 2012 announcement from the State Attorney General that CalOPPA does, in fact, apply to mobile applications of smartphones and tablets.[144] The language of the statute does not specifically cover biometric information, nor does it regulate many of the devices categorized within the IoT,[145] showing how quickly a technology or industry-focused law can slip into obsolescence if not carefully drafted.

b. The California Consumer Privacy Act of 2018

At the end of June of 2018, California Governor Jerry Brown signed into law the California Consumer Privacy Act (CCPA).[146] The law provides consumers considerable individual oversight of the data collected by companies operating online as an extension of California's fundamental right of privacy.[147]

The CCPA requires companies that collect personal information to inform consumers of the categories of data they collect and the purposes for collection before or at the time of collection.[148] The law also provides consumers a right to know what personal information has been collected about them.[149] Consumers, however, can only obtain this information by requesting it from the collecting company.[150] The statute covers a broad range of data and notes specifically that the term "personal information" is inclusive of biometrics.[151]

In addition to knowledge and access, the statute provides consumers with a right to have such data deleted.[152] This right is hedged by certain exceptions, allowing companies to refuse to delete consumers' personal information in certain circumstances.[153] For example, companies are not

144. *California Online Privacy Protection Act (CalOPPA)*, CONSUMER FED'N OF CAL., https://bit.ly/2pjyhhq (last updated July 29, 2015).

145. *See generally* CAL. BUS. & PROF. CODE § 22575 (West 2018). The statute does not prohibit the collection or use of consumer data. *Id*. Instead, the statute requires commercial websites and online services to "conspicuously post" privacy policies that include what types of data the website collects from users. *Id.* § 22575(a).

146. Ben Adler, *California Passes Strict Internet Privacy Law With Implications For The Country*, NPR (June 29, 2018, 5:05 AM), https://n.pr/2MxIVtT.

147. *See* California Consumer Privacy Act of 2018, ch. 55, 2018 Cal. Legis. Serv. (West) (codified at CAL. CIV. CODE div. 3, pt. 4, tit. 1.81.5).

148. CAL. CIV. CODE § 1798.100(b) (West 2018).

149. *Id.* § 1798.100(c).

150. *Id*.

151. *Id.* § 1798.140(o)(1)(E). "Biometric information" is defined as "an individual's physiological, biological or behavioral characteristics . . . that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. *Id.* § 1798.140(b).

152. *Id.* § 1798.105(a).

153. *Id.* § 1798.105(d)(1)–(5).

required to delete collected data if it is necessary to continue providing the consumer with a requested service, detect security incidents or illegal activity, identify and repair software bugs, or exercise free speech.[154] Because the CCPA does not go into effect until 2020, uncertainty exists as to how broadly courts will construe these exceptions, leaving some critics concerned that the right to delete personal information is a hollow promise.[155]

While much of the law's language shows an intent to empower citizens in their right to privacy, certain provisions have left privacy advocates concerned about the law's adequacy.[156] For example, the law provides citizens the right to forbid companies from selling their collected data to third parties.[157] Furthermore, companies are proscribed from discriminating against consumers for exercising that right.[158] However, this right, known as an opt-out provision, is not a default; therefore citizens must first have knowledge of their right to prevent companies from selling their personal information.[159] Another concern is that companies may offer quality and monetary incentives for the use and sale of consumer information.[160] While consumers cannot be punished for exercising their rights, others may be compensated for waiving their rights.[161] This could give companies the option to offer a lower-quality service as the default, reserving premium services for those willing to waive their fundamental rights to privacy.

Finally, critics have raised concerns over the ability of consumers to have these rights fully enforced.[162] The CCPA provides consumers with a private right of action, but only in limited circumstances.[163] While consumers can launch a civil suit against companies for disclosure of data in the event of a security breach, no private right of action is provided in the event a company refuses to comply with a consumer's request for data

154. *Id.*

155. *See* Adam Schwartz et al., *How to Improve the California Consumer Privacy Act of 2018*, ELEC. FRONTIER FOUND. (Aug. 8, 2018), https://bit.ly/2CRoxDe.

156. *ACLU Statement: New Law Falls Woefully Short of Protecting Californians' Privacy*, AM. CIVIL LIBERTIES UNION OF N. CAL. (June 28, 2018) https://bit.ly/2NWfEJM [hereinafter *ACLU Statement*].

157. CAL. CIV. CODE § 1798.120(a).

158. *Id.* § 1798.125(a)(1). Examples of this include denying or altering the quality of goods and services provided to customers, or charging a different price for goods or services because a consumer opted out of third-party data sales. *See id.* § 1798.125(a)(1)(A)–(D).

159. *Id.* § 1798.120(a).

160. *Id.* § 1798.125(b)(1).

161. *See generally id.* § 1798.125.

162. *See ACLU Statement*, *supra* note 156.

163. CAL. CIV. CODE § 1798.150(a)(1).

access, deletion, or prohibition of data sale.[164] The Attorney General, on the other hand, is vested with the authority to prosecute any violation of the CCPA;[165] however, this limited designation of authority may prove inimical to consumer data protection as seen in jurisdictions where data statutes lack a private right of action.[166]

Efforts to appease both consumers and data collectors have resulted in a promising, but imperfect Act.[167] In the time before the law goes into effect, both consumer privacy advocates and tech companies will be launching efforts to strengthen-or chip away at-the protections it affords.[168]

4. Other State Legislation

Despite the successes of BIPA, efforts by other states to adopt similar legislation have proven less effective due to small, but significant, differences in statutory language.[169]

In 2009, for example, Texas enacted the Capture or Use of Biometric Identifier Act (CUBI).[170] In 2017, Washington enacted legislation substantively similar to that of Texas,[171] though under the Washington law, data collected from physical or digital photos is not protected.[172] Neither law provides a private right of action for citizens, who must instead appeal to their respective attorneys general.[173]

Without a private right of action, some speculate that the laws will not carry the weight necessary to protect citizens,[174] while others contend that individual causes of action will prove "burdensome" on growth and innovation of businesses.[175] Since its 2009 ratification, CUBI has not been

164. *See id.* § 1798.150–.155.
165. *See id.* § 1798.155.
166. See *infra* Section II.D.3.
167. Harper Neidig, *Tech Mobilizes Against California Privacy Law*, THE HILL (July 1, 2018, 9:00 AM), https://bit.ly/2yrwhZ4.
168. *Id*.
169. *See* Claypool & Stoll, *supra* note 97; *see also* Douglas Kelly, *Five States Introduce New Data Security Laws*, LAWROOM (Mar. 7, 2017), https://bit.ly/2Jasaog.
170. Capture or Use of Biometric Identifier Act, TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017).
171. *See* WASH. REV. CODE ANN. § 19.375.010 (West 2018).
172. Kartikay Mehrotra, *Tech Companies are Pushing Back Against Biometric Privacy Laws*, BLOOMBERG BUSINESSWEEK (July 19, 2017, 8:26 PM), https://bloom.bg/2tO6PYp.
173. *See* TEX. BUS. & COM. CODE ANN. § 503.001(d); WASH. REV. CODE ANN. § 19.375.030(2).
174. *See* Paul Shukovsky, *Washington Biometric Privacy Law Lacks Teeth of Illinois Cousin*, BLOOMBERG LAW (July 18, 2017), https://www.bna.com/washington-biometric-privacy-n73014461920/ (quoting Drinker Biddle & Reath attorney, Justin O. Kay, as saying that statutes without individual causes of action "will likely be a footnote.").
175. *See id.* (quoting Hutton & Williams privacy attorney, Lisa Sutton).

used by the State's attorney general to bring a single suit protecting citizens' biometric identifiers.[176]

Following BIPA's enactment, large tech companies have begun lobbying legislators to spike similar enactment efforts.[177] Before the CCPA was enacted, California and Connecticut proposed biometric privacy bills, both of which passed state assemblies but died in the senate.[178] Montana, Arizona, Missouri, Alaska, New Hampshire, and New York all made proposals to protect biometric identifiers, many modeled closely after BIPA, but none made it out of committee.[179]

As it stands, the arid landscape of federal biometric privacy protection has prompted states to attempt legislative maneuvers to rectify this oversight with varying degrees of success. The vast majority of citizens, however, remain vulnerable to exploitation by private data collectors at a time when data is becoming more sensitive, and collection is becoming more invasive.

E. International Protection of Biometric Data

The ever-expanding reach of companies like Google and Facebook implicates the privacy concerns of consumers outside the United States.[180] Acknowledging the continued failure of legislation on home soil, and showing thoughtful concern for the sensitivity of personal information, as well as the ongoing risk of breach, the European Union has set a new standard in data protection that has forced many American-based companies to alter their practices.

1. General Data Protection Regulation

The European Union's recent General Data Protection Regulation (GDPR),[181] presents a thoughtful and comprehensive step toward protecting the rights of individual consumers in contrast to the patchwork, industry-focused regulatory fabric of the United States.

The GDPR assigns to EU citizens a right to their data.[182] In so doing, the GDPR imposes upon companies several obligations intended to

176. Mehrotra, *supra* note 172.
177. *Id.*
178. *Id.*; *see also* A.B. 83, 2015–2016 Leg., Reg. Sess. (Cal. 2015).
179. Mehrotra, *supra* note 172; *see* Shukovsky, *supra* note 174; H.B. 144, 28th Leg., 1st Sess. (Alaska 2013); A.B. 5232, 2017–2018 Leg., Reg. Sess. (N.Y. 2017).
180. Kris Lahiri, *What Is General Data Protection Regulation?*, FORBES (Feb. 14, 2018, 01:21 PM), https://bit.ly/2Ds9uj3.
181. Regulation 2016/679, 2016 O.J. (L 119) 1 (EU).
182. *Id*. art. 1. The Regulation provides for the "protection of natural persons in relation to the processing of personal data" as a "fundamental right." *Id*.

increase data-holder transparency and user autonomy on the Internet.[183] The language of the regulation is broad, suggesting a cooperative understanding between the legislative and judicial bodies that will allow courts to interpret the language dynamically as technology changes.[184] For example, Article 24 of the GDPR refers to the responsibility of data controllers to "implement appropriate . . . measures to ensure . . . that processing is performed in accordance with" the rights of citizens laid out in the regulation.[185] The use of the term "appropriate" shows an understanding that effective security precautions will change with technology.

Along with the broad language, similar deference is given to supervisory authorities for purposes of determining fines for GDPR violations.[186] The GDPR has no hardline rules on punishment, but notes that the supervisory authority "shall ensure" that administrative fines are "effective, proportionate, and dissuasive."[187] Fines can be up to "4% of annual global turnover."[188] Already, Google has run afoul of the regulation, incurring a €50 million fine in France for failing to obtain "valid consent" when collecting data for targeted advertisements.[189]

In addition to the sweeping responsibility to implement appropriate safeguards, the GDPR enumerates several specific rights which shape the more general "right to data" now held by EU citizens.[190] Primarily, the GDPR (1) provides EU citizens with the right to know if a website, business, or other control is collecting personal data and if so, what data is being collected and the extent to which that data is being used;[191] (2) provides users with a right to correct personal information if found to be inaccurate;[192] and (3) codifies the oft-debated "right to erasure," granting a "data subject" the right to have personal data concerning him or her erased by the collecting company "without undue delay,"[193] as well as requiring data collectors to inform affiliated data users of the erasure request to ensure complete deletion.[194]

To increase awareness and transparency, the GDPR delineates data collector obligations in a way that demystifies questions of liability, and

183. *See id.* arts. 24–43.
184. *See id*. art. 24.
185. *Id*.
186. *See id*. art. 83.
187. *Id*. art. 83(1).
188. *GDPR FAQs*, EU GDPR, https://bit.ly/2PcmAqH (last visited Dec. 10, 2018).
189. Vincent Manancourt & Tom Webb, *Google Ordered to Pay First Multi-million GDPR Fine*, LEXOLOGY (Jan. 29, 2019), https://bit.ly/2TOOED1.
190. *See, e.g.*, Regulation 2016/679, *supra* note 181, arts. 15–17.
191. *Id.* art. 15.
192. *Id.* art. 16.
193. *Id.* art. 17(1).
194. *Id.* art. 17(2).

explains the general protocol companies must take in the event of breach.[195] Foremost, the GDPR requires data-holders to notify citizens of data compromise within seventy-two hours of becoming aware of the breach.[196] The GDPR enumerates a list of information the controller is required to provide to the consumer in order to adequately satisfy the regulation's notice requirement,[197] including the contact information of a data protection officer from whom more information can be obtained.[198]

Second, the GDPR imparts cooperative liability on companies and their associated data processors.[199] Article 28 places a burden on data controllers not to contract with a processor unless it "provid[es] sufficient guarantees to implement appropriate . . . measures" to "ensure the protection of the rights" of EU citizens.[200] In addition, processors are prohibited from engaging with other processors "without prior specific or general written authorisation of the controller," increasing transparency by requiring a sort of chain of title for data use and transfer.[201]

Finally, and most importantly, the GDPR provides for a private right of action, which is imperative if a data protection statute is to prove effective.[202] Article 82 permits any individual who "has suffered material or non-material damage" as a result of a GDPR violation to seek an award "from the controller or processor for the damage suffered."[203]

The EU's GDPR provides an insightful and adaptable example of data protection, from which the United States can learn. On a federal level, no remotely comparable protection exists, but concerns over biometric data privacy have prompted several states to enact data protection statutes, though few have been effective. Consumers are thus left with no right to their own uniquely sensitive and irreplaceable biometric data. Given the amount and nature of the information that can be gathered through biometrics, nothing short of federal legislation will be adequate to protect U.S. citizens.

III. ANALYSIS

Even a cursory glance at the technological landscape in the United States today reveals an overwhelming view of user data as a commodity rather than a virtual manifestation of an individual's most private

195. *See id*. arts. 24, 28, 33(1).
196. *Id.* art. 33(1).
197. *Id.* art. 33(3).
198. *Id.* art. 33(3)(b).
199. *See id.* art. 28.
200. Regulation 2016/679, *supra* note 181, art. 28(1).
201. *Id.* art. 28(2).
202. *See supra* Section II.D.3.
203. Regulation 2016/679, *supra* note 181, art. 82(1).

information.[204] The vast universe of the IoT will not cease to expand; it is simply too valuable.[205] The breakneck speed at which the IoT is growing indicates that previously unimaginable technological advances are right around the corner. While the climate of technological innovation portends economic boon, the price paid is the privacy of millions of citizens.

A. Biometric Data is Uniquely Sensitive

Without question, biometric identifiers such as fingerprints, gait, heart rate, or face scans are uniquely personal and revealing of their owners.[206] Eye tracking, however, sits atop the list as perhaps the most sensitive, and most valuable identifier, and is thus the perfect example of why biometric data needs legislative protection on a national scale.[207]

Because pupillary motility cannot be consciously controlled, and eye movement can only be controlled to a certain extent, our eyes are our most-external, least-inhibited projectors of brain activity.[208] That companies, researchers, and algorithms are able to extract meaning from the recorded "messages"—sent from brain to body and expressed through the eyes—suggests that in a rudimentary sense, eye tracking allows for the reading of minds.[209] This is true in a medical sense (translating occulomotor responses to make a diagnosis) and in a behavioral context (reading messages from the brain to study interest, arousal, or decision-making).[210]

For example, suppose a teen receives a VR headset for his birthday. He uses it to play a popular game about superheroes, displayed as characteristically muscled and scantily clad. The player, knowingly or not, will spend more time looking at favored characters. This visual stimulus

204. Abhas Ricky, *What Should Be Your Data Monetization Strategy to Compete in the Borderless Economy?* FORBES (May 8, 2018, 9:45 AM), https://bit.ly/2CXhtFo; *see also* Alessio Botta et al., *Monetizing Data: A New Source of Value in Payments*, MCKINSEY & CO. (Sept. 2017), https://mck.co/2AlFKlP.

205. Theo Priestly, *The Internet Of Things Is A Fragmented $19 Trillion Roulette Gamble*, FORBES (Oct. 5, 2015), https://bit.ly/2yvo1Hc. Forbes anticipates a $19 trillion valuation of the IoT in 2020. *Id.*

206. ERIKA MCCALLISTER ET AL., NAT'L. INST. OF STANDARDS & TECH., NIST SPEC. PUBLICATION NO. 800-122, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) 2-1 to -2 (2010), http://bit.ly/2G73bUL. The National Institute of Standards and Technology (NIST) lists biometric data as one form of Personally Identifiable Information, which it defines as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity . . . and (2) any other information that is linked or linkable to an individual . . . ." *Id*.

207. *See supra* Section II.A.

208. *See supra* Section II.A.

209. *See* Eckstein et al., *supra* note 17, at 70 (explaining that scientists have lauded eye tracking for its ability to "provide an ideal neuroscience model to investigate association between brain mechanisms and behavior").

210. *See supra* Section II.A.

elicits a pupillary dilation from the user without the user's knowledge.[211] That biometric data, including where the user looked, for how long, and how the pupil reacted, might be considered "supplemental data."[212] Synthesized with "enterprise-level data"[213] to create a user model, this profile of a young consumer can be sold to a purveyor of targeted advertising.[214]

Having analyzed the data and derived meaning from the reaction to superhero stimuli, the company determines that advertising highlighting the male figure will be most effective on this individual, and in doing so either correctly (or incorrectly) infers a conclusion about the user's sexuality.[215] "Sex sells," as the adage goes. Advertisers have a higher chance of selling a product if they know the sexual interests of a targeted consumer – but imagine if a company, quietly collecting data, targets suggestive advertisements at a consumer before his friends, parents, or even he himself fully understands those interests. If such information can be derived from eye movement, and there is no legislation to prevent its collection, it *will* be analyzed, stored, and sold. Without controls on data sale, information gleaned from user behavior may even lead to discrimination by employers or insurance providers.[216]

B. Protection of Biometric Data is a Right, Not an Option

VR applications span swaths of fields and interests from military training and mechanical troubleshooting[217] to entertainment, and travel, suggesting VR and AR will be used by consumers of every kind.[218] The

211. *See supra* Section II.A.

212. Botta et al., *supra* note 204. Supplemental data is a broad classification spanning from "raw data derived from external sources such as social media, weather data, and digital IDs to synthesized, value-added analytics that [can be] captured through predictive modelling, [or] sentiment analysis . . . ." *Id*.

213. *Id.* Enterprise-level data refers to information provided directly to a company for the use of its product or service (e.g., user preferences and settings). *Id.*

214. *Id.* (explaining that companies can "extract value through the monetization of the data itself . . . through third parties."); *see also* Michael Fertik, *Your Future Employer is Watching You Online. You Should Be, Too.*, HARV. BUS. REV. (Apr. 3, 2012), https://bit.ly/2P9tNYR.

215. *See* Rieger & Savin-Williams, *supra* note 42, at 6 ("Results suggested that pupil dilation is a significant indicator of sexual orientation."); *see also supra* Section II.A.

216. Marshall Allen, *Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates*, PROPUBLICA (July 17, 2018, 5:00 AM), https://bit.ly/2NnbLgX; *see also* Fertik, *supra* note 214.

217. Lauren Goode, *Microsoft's HoloLens 2 Puts a Full-Fledged Computer on Your Face*, WIRED (Feb. 24, 2019, 12:20 PM), https://bit.ly/2XjOEK1.

218. *See* Howie Leibach, *Meet the Consumers That Will Make or Break Virtual Reality Next Year*, SINGULARITYHUB (Dec. 17, 2015), https://bit.ly/2q2upRB (finding that, although male millennials are the "most aware" of VR, the majority of those polled, including Baby Boomers express interest in experiencing VR); *see also* Aaron Burch, *VR*

"truthful" nature of the information derived from eye movement will provide companies with personal information about users without their knowledge.[219] To exploit such information for profit is to violate an individual's right to privacy in a significant way.[220]

Outlining a proposed Consumer Privacy Bill of Rights, a 2012 White House report noted, "Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data."[221] An expectation of privacy is sure to be violated when information derived from reflexive or impulsive movements–sometimes knowingly, but more often unknowingly made–are used to collect information about an individual wholly unrelated to the task or activity for which the device was used in the first place.

The sheer volume of valuable information that can be derived from eye-tracking data[222] makes it unlikely that companies will retain data solely to improve their products when, perhaps, more demand exists for the data than the product.[223] Companies and users are quick to extol the realism brought to VR by technology like foveated rendering,[224] but do so without consideration for the sensitivity of the data relinquished in the process.[225] Although an immersive VR experience is an achievement worthy of pursuit and excitement, a tool as powerful as eye tracking should be incorporated into toys or home entertainment systems with equal consideration for the concomitant privacy implications.

and Consumer Sentiment, TOUCHSTONE RESEARCH (Jan. 28, 2016), https://bit.ly/2R3q2Bm ("While interest and appeal of VR does decline with age, there remains a substantial level of interest even among Baby Boomers (64% are positive towards VR and about half are interested).").

219. *See* Costandi, *supra* note 26; Robertson, *supra* note 28.

220. While this statement is an assertion by the author, the sentiment is reflected and supported by the policy and purpose behind data privacy statutes such as BIPA and the CCPA. *See supra* Sections II.D.1., II.D.3.b.

221. U.S. WHITE HOUSE OFFICE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 1 (2012), https://www.hsdl.org/?view&did=700959.

222. Allen, *supra* note 216. A former Aetna employee described the insurer's purchase of data sets describing "hundreds of personal details" about millions of Americans. *Id*.

223. Ricky, *supra* note 204 ("While many companies are entrenched in programs to use big data to help make better-informed decisions, the next step . . . is to turn that information into profit.").

224. *See supra* note 53 and accompanying text.

225. *See* Hardawar, *supra* note 49.

C. The Federal Government is Currently Inadequate in its Biometric Protection

Currently, the FTC Act permits only the Commission or the Attorney General to bring actions for personal privacy violations,[226] which are brought almost exclusively on behalf of large classes in the event of a substantial breach.[227] Due to the lack of federal statutes protecting biometrics and other data privacy, the "unfair and deceptive" language of Section 5 of the FTC Act has been applied only to companies that have misrepresented or violated their own terms of use and self-imposed privacy policies.[228] Leaving regulation in the hands of those collecting undeniably valuable data is like letting the CEO of Exxon determine best practices in a world without the EPA. It appears that the FTC has never pursued a case regarding the improper collection, sale, or use of biometric data, though it maintains the authority to act in the event of unfair or deceptive practices involving the misuse of biometric information.[229] Still in its incipiency, Illinois's BIPA has been used several times to protect the bioinformatic rights of individuals and classes to great effect.[230]

D. The Federal Government is Poised to Support a National Statute Protecting Biometric Data

"Congress is good at two things: doing nothing, and overreacting. So far, we've done nothing on Facebook . . . We're getting ready to overreact."[231] After Cambridge Analytica and potentially other third parties accessed the data of nearly 87 million Facebook users, CEO Mark Zuckerberg spent two days before Congress fielding questions,

226. *See* 15 U.S.C. § 56 (2012 & Supp. 2017).

227. *See, e.g.*, *Ashley Madison FTC Settlement*, *supra* note 68 (noting that the Ashley Madison breach affected 36 million account holders); *Operator of Online Tax Preparation Service Agrees to Settle FTC Charges That it Violated Financial Privacy and Security Rules*, FED. TRADE COMM'N (Aug. 29, 2017), https://bit.ly/2iZXTeY (explaining that TaxSlayer's failure to "implement safeguards to protect the security, confidentiality and integrity of customer information" resulted in the hackers gaining full access to over 9,000 user accounts); *Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims*, FED. TRADE COMM'N (Aug. 15, 2017), https://bit.ly/2uY81Jj (detailing Uber's failure to provide "reasonable security to prevent unauthorized access" to consumers' data, resulting in the breach of over 100,000 drivers' names and license numbers).

228. *See* Peppet, *supra* note 61, at 137.

229. Michael P. Daly et al., *Biometrics Litigation: An Evolving Landscape*, DRINKER BIDDLE (Apr. 1, 2016), http://bit.ly/2AkVKEE.

230. *See supra* Part II.C.2. (describing numerous cases involving BIPA violations that have returned with verdicts for the plaintiffs).

231. *Facebook: Transparency and Use of Consumer Data: Hearing Before the H. Comm. on Energy & Commerce,* 115th Cong. 161–62 (2018) (prelim. transcript) [hereinafter *Facebook Hearing*], http://bit.ly/2UsrQXf (statement of Rep. Billy Long).

apologizing for abusing users' trust, and vowing to improve Facebook's practices.[232] Well before Zuckerberg's public admonishment, Facebook purchased Oculus VR for $2 billion.[233] The broad commercial viability of VR and AR, and the insufficiency of state governments to provide adequate data protection, suggests that now is an appropriate time to implement a federal biometric privacy statute.

The looming threat of massive fines under the GDPR or from the FTC[234] have prompted Facebook and other tech giants to proactively discuss potential federal data protection legislation.[235] Large companies are concerned that without a uniform law to guide standards and practices, states will continue to draft and enact their own.[236] In drafts of federal legislative proposals, tech companies emphatically seek two provisions: a pre-emption clause to supersede state laws like BIPA, and an exclusive grant of enforcement authority to the FTC.[237]

Even before the Cambridge Analytica breach, the apparent success of BIPA prompted proposals of similar statutes by many other states.[238] However, the legislation's efficacy has prompted lobbyists from massive tech companies to spike the passage of similar statutes in a staggering number of states.[239] The push for state preemption and FTC oversight portends ineffective regulation if tech companies achieve their goals in shaping legislation.

IV. RECOMMENDATION

The sensitivity of biometric data, increased use in eye-tracking research, and projected explosion of eye-tracking technology in the consumer market all suggest a need for statutory data protection. While a broad statute protecting all personal data is advisable, any new legislation must specifically provide for, or cover by broad definition, biometric information protection.

232. Georgia Wells & John D. McKinnon, *Facebook Data on 87 Million Users May Have Been Improperly Shared*, WALL STREET J. (Apr. 4, 2018, 9:19 PM), https://on.wsj.com/2GZO0wc.

233. Chris Welch, *Facebook Buying Oculus VR for $2 Billion*, THE VERGE (March 25, 2014, 5:34 PM), https://bit.ly/2ybNPWn.

234. Tony Romm & Craig Timberg, *FTC opens investigation into Facebook after Cambridge Analytica scrapes millions of users' personal information*, WASH. POST (Mar. 20, 2018), https://wapo.st/2q5uqVc.

235. Dina Temple-Raston, *Why The Tech Industry Wants Federal Control Over Data Privacy Law*, NPR (Oct. 8, 2018, 5:00 AM), https://n.pr/2OJcVrt.

236. *See supra* Section II.C.3. The myriad states that have implemented or attempted to pass biometric privacy laws run the gamut of red, blue, and purple states, indicating widespread concern for data protection. *Id*.

237. Temple-Raston, *supra* note 235.

238. *See supra* Section II.C.3.

239. *See* Mehrotra, *supra* note 172.

A. The Statute Must Provide Users a Right to Their Data

The CCPA expands the inalienable right to privacy of all California citizens to include online data.[240] The GDPR likewise shows respect for the right of an individual to own and control his or her data, by using broad language to prescribe and protect citizen rights rather than prohibit the behavior of a company or industry.[241] Broad, inclusive language conferring upon users the right to their data shows regard for fundamental rights of individuals and ensures longevity of the statute.[242] Broad and inclusive language akin to that in the GDPR and CCPA forces companies to be mindful of consumer rights as they innovate, and prevents the need for new laws as innovation renders existing laws obsolete or inadequate. Thus, the federal statute must provide users a right to their personal data.

To countenance the provision of a fundamental right to one's data, the proposed statute should provide users with a right to access, deletion, and refusal of sale, similar to the provisions enumerated in the GDPR and CCPA.[243] Such provisions comport with some of the most fundamental and long-standing pillars of property and ownership in legal jurisprudence,[244] and should not be discarded simply because the property in question is digital.

Further, the statute should mandate opt-in data use policies instead of the opt-out provisions.[245] If a right is truly fundamental, one should not have to know the right exists in order to exercise or protect it. An opt-in data retention default supports the policy of unfettered user ownership and

240. *See* California Consumer Privacy Act of 2018, ch. 55, § 2(a), 2018 Cal. Legis. Serv. (West) ("Fundamental to this right of privacy is the ability of individuals to control the use, including the sale, of their personal information.").

241. *See* Regulation 2016/679, *supra* note 181, art. 24. The GDPR imparts responsibility on data controllers to "implement appropriate . . . measures to ensure . . . that processing is performed in accordance with" the rights of citizens laid out in the regulation. *Id.*

242. *See* CONSUMER FED'N OF CAL., *supra* note 144. Less than a decade after its adoption, CalOPPA had to be clarified, and subsequently amended to account for the rapid changes in technology. *Id*. The upshot here is that tech- or industry-focused statutes stay relevant for less time than laws assigning an inalienable right.

243. *See supra* Section II.D.3.B.

244. *See* J.E. Penner, *The "Bundle of Rights" Picture of Property*, 43 UCLA L. Rev. 711, 732 (1996) (citing A.M. Honore, *Ownership*, *in* OXFORD ESSAYS IN JURISPRUDENCE 107, 112–24 (A.G. Guest ed., 1961)). Ownership of property confers upon the owner a right to use, transfer, alienate, lease, or destroy the item or parcel in concert with a duty to prevent harm. *Id*. These rights should apply in equal measure to data once ownership is established as a matter of law.

245. *See* Luke Irwin, *GDPR: When Do You Need to Seek Consent?*, IT GOVERNANCE (Aug. 30, 2017), http://bit.ly/2B6WHji. "Opt-in" refers to a policy that requires a user to give informed consent to a certain action such as collection or sale of data. *Id.* "Opt-out" policies are much more popular and assume consent to use data until the user actively rescinds that consent. *Id.*

autonomy while an opt-out default indicates a preference toward data-collecting companies through a pre-supposed waiver of rights.[246]

To balance the needs of consumers with those of companies, the proposed statutes should accord users the choice to waive some rights. Thus, if users choose to waive certain protections, companies may reward or otherwise compensate users for their data and information. However, the methods by which companies incentivize customers to waive their rights must be carefully monitored to avoid coercive or unfair practices.

Certain fundamental rights should remain inalienable and non-waivable regardless of incentive. The choice to have data collected and sold by companies should be left to users; however, the right to (1) see what is collected, (2) correct inaccurate information, (3) know the purpose of its collection, and (4) know the places to which it is being sold or transferred must be immune from waiver. This will allow users and companies to benefit from the value of user data while remaining transparent about the process.

B. The Statute Must Protect Biometric Data Specifically

A sweeping data protection statute will encompass myriad forms of data; however, no data is more sensitive than biometrics,[247] and thus the statute must provide explicitly for biometric data protection. Although the CCPA is not a biometric-specific statute, the law casts a wide definition of "personal information," which includes biometric data.[248] The statute offers further clarity by offering an illustrative, but non-exhaustive definition of "biometric information."[249] A federal statute must follow this example. Illustrative definitions make legal interpretation easier for courts,[250] and non-exhaustive definitions ensure longevity of the statute by leaving open the possibility of protection for biometric identifiers that have not yet been explored or exploited by technological innovation.

Ambiguous language can frustrate the efficacy of the statute,[251] and thus the language of BIPA and its analysis in court should be considered in the process of drafting a federal statute. Language excluding "information derived from . . . photographs" from the statute's protection was addressed to determine if the term referred to physical photographs or

246. *See supra* Section II.D.3.b.
247. *See supra* Section II.A.–.B.
248. CAL. CIV. CODE § 1798.140 (West 2018).
249. *See supra* note 152 and accompanying text.
250. *See* In re Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1171 (N.D. Cal. 2016) (relying on the enumerated exclusions to interpret ambiguous language in favor of plaintiff class); *see also* Section II.D.2.a.
251. *See supra* Section II.D.2.a.

digitized images.[252] The court construed in favor of the statute's overall policy of biometric protection,[253] but ambiguity in the language presented the risk of a gaping hole in the statute's coverage.[254] Drafters of a federal statute should avoid such ambiguities to ensure comprehensive protection for consumers.

C. The Statute Must Provide for a Private Right of Action

While the gravamen of this comment is the importance of statutory protection of biometric identifiers, a private right of action is of tantamount importance if the statute is to have any commendable impact. The right of an individual to sue privately under the statute further supports the idea that biometric data and information is emphatically the property of its owner by placing the ability to protect that property in the owner's hands.

Exclusive FTC oversight will prove insufficient to protect the rights granted to users.[255] The FTC's reach is broad, but adding responsibility as massive as biometric data regulation will only bloat the Commission, resulting in an emaciated process of investigation and litigation. As it stands, the FTC is only open to investigating the most egregious and expansive data breaches.[256] The proposal by large companies for exclusive FTC oversight is unsurprising, but dangerous if implemented.

The risk of over-burden and under-performance is the same reason this Comment advocates for a statute rather than a regulation. While an agency devoted to the protection of user data is compelling, the agency's efficacy would ebb and flow with administrative changes and fluctuations in budget. This is not to say that agencies are useless in the effort to protect user data. The FTC's ability to investigate substantial violations and prosecute vast class-action suits makes it a welcome partner in the effort to protect user privacy. Biometric identifiers, however, are too uniquely sensitive to be protected differently year-to-year, or solely in the event of massive breach. Consumers deserve as much the right to own their biometric data as they do the right to defend it.

V. CONCLUSION

The wave of VR and AR is cresting, bringing with it new forms of entertainment for all ages.[257] As technology evolves and Americans invite

252. *In re Facebook*, 185 F. Supp. 3d at 1170.
253. *See id.* at 1171.
254. *See supra* Section II.D.2.A.
255. Temple-Raston, *supra* note 233.
256. *See supra* Section II.C.1.
257. *See supra* Section III.B.

more immersive and invasive forms of entertainment into their homes, federal laws need to reflect an understanding of the risks of innovation by protecting individual rights of privacy rather than regulating technology. While some state laws have been enacted to protect the biometric data of individuals,[258] others have fallen short in ways that essentially nullify the efforts of lawmakers to enact lasting policy.[259]

In the excitement that has surrounded VR for decades, little research has been compiled to show how much personal information can be derived from the involuntary movements of eyes and pupils.[260] In the remaining moments before VR becomes a part of every-day life, a federal statute must be enacted to ensure that safety and privacy are concomitant with the use and enjoyment of new technology capable of collecting biometric information.

258. *See supra* Section II.D.1–.2.
259. *See supra* Section II.D.3.
260. *See supra* Section II.A.