Seattle Journal of Technology, Environmental & Innovation Law

Volume 12
Issue 2 *Issue 2*

Article 2

5-26-2022

Biometric Data Collection and Big Tech: Imposing Ethical Constraints on Entities that Harvest Biometric Data

Ian Ducey
Seattle University School of Law

Biometric Data Collection and Big Tech: Imposing Ethical Constraints on Entities that Harvest Biometric Data

Cover Page Footnote

Ian Ducey graduated from Seattle University College of Law in May of 2022. He would like to thank the editors of SJTEIL for their edits, feedback, and dedication to the success of this article. Ian would also like to thank his friends for putting up with his ranting about data privacy and biometrics He would like to give special thanks to his girlfriend Blake Lamberty for her unwavering support and dedication throughout all of law school.

Biometric Data Collection and Big Tech: Imposing Ethical Constraints on Entities that Harvest Biometric Data

Ian Ducey[*]

I. INTRODUCTION

Amazon can tell when you are sleeping, when you are awake, and when you are stressed, and they can do it before you may recognize it yourself. At least it will be able to if you decide to buy their newest wearable health monitoring technology. In 2020, Amazon joined Google's Fitbit and Apple's Apple Watch in the wearable technology market with the Amazon Halo.[1] A wristband outfitted with a variety of sensors designed to help manage and record health identifiers, including body fat percentage, step tracking, sleep tracking, and now emotional responses.[2] Many companies have begun developing and exploring the power that comes from harvesting our biometric data.[3] Companies like Apple, Google, and Amazon have established massive reach through their existing platforms, which millions of people regularly use.[4] These

[*]Ian Ducey graduated from Seattle University College of Law in May of 2022. He would like to thank the editors of SJTEIL for their edits, feedback, and dedication to the success of this article. Ian would also like to thank his friends for putting up with his ranting about data privacy and biometrics He would like to give special thanks to his girlfriend Blake Lamberty for her unwavering support and dedication throughout all of law school.

[1] David Phelan, *Amazon Halo: Jaw-Dropping New Health-Monitoring Wearable & Service Revealed*, FORBES (Aug. 27, 2020), https://www.forbes.com/sites/davidphelan/2020/08/27/amazon-halo-jaw-dropping-new-health-monitoring-wearable-and-service-revealed-measures-body-fat-in-a-way-never-seen-before/#297e56c6a4af [https://perma.cc/DF6N-5B83].

[2] *Id.*

[3] Carra Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, 26 J. L. & POL'Y 769 (2018), https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1570&context=jlp [https://perma.cc/NH9U-FRLT].

[4] More than 100 million people pay for Amazon Prime. Alina Selyukh, *What Americans Told us About Online Shopping Says A Lot about Amazon*, NPR (June 6, 2018), https://www.npr.org/2018/06/06/615137239/what-americans-told-us-about-online-shopping-says-a-lot-about-amazon [https://perma.cc/8ZYF-CXMY]; Google receives over 3.8 million searches per minute. Kenshoo, *Marketing Metrics: Daily Searches on Google and Useful Search Metrics for Marketers*, KENSHOO (Feb. 25, 2019), https://kenshoo.com/monday-morning-metrics-daily-searches-on-google-and-other-google-facts/#:~:text=Although%20Google%20does%20not%20share%20exact%20numbers,%20as.per%20day,%20or%202%20trillion%20searches%20per%20year! [https://perma.cc/4PPN-M2UT]; In 2017 Apple had over 1.4 billion active devices worldwide. Juli Clover, *Apple Now Has 1.4 Billion Active Devices Worldwide*, MACRUMORS (Jan. 29, 2019),

companies have discovered the usefulness of accessing biometric data to complement their already expansive traditional data collection practices and are beginning to expand their capacity to develop technologies that allow them to take advantage of their existing reach.[5] As these corporations invest in wearable biometric reading devices, "wearables," they can also take advantage of their massive capacity to utilize the information they extract from the biometric readings of users through their wearable technology.[6]

To address these problems, Washington State should take two more steps. To respond to this changing technological environment, Washington State should adopt new definitions for biometric identifiers, to expand legal coverage for potentially abusable data that companies are beginning to harvest. Washington State should also address the risk of in-house abuse by large corporations that use consumer data in various projects by imposing a higher standard of consent to harvest biometric data from consumers. Further, the Federal Government should adopt similar ethical standards to those imposed on biomedical research organizations which gather, store, and use massive quantities of patient data. The Federal Government should also set an informed consent requirement based on dynamic consent and should require corporations to provide notice and obtain affirmative consent every time they want to use consumer biometric data for a new project. Dynamic consent incorporates an initial consent agreement and creates an ongoing dialogue where consumers can choose to allow or choose to bar the use of their data for new projects as the corporate interest arises.[7] Implementing ethical standards will require corporations and consumers engage in ongoing dialogue about creating a system with less potential for abuse and ensure that corporations do not cause harm when people agree to something they may not understand.

This article will explain why consumer data matters to corporations and what makes wearables attractive as tools for information gathering. To do so, the article will briefly explain what Amazon, Google, and Apple are using wearables for and explain why data is a driver for success in the modern corporate world. Next, the article will describe what biobanks are and how the consent theories biobanks rely on can be applied to large-scale data collection processes used by big tech companies. Then, the article will turn to the status of biometric data protection laws in Illinois and Washington because of Illinois' existing private right of action and longer history for a better analysis of the impacts and Washington to address what they have done well and how they can improve. The article will next address the state of federal law on biometric data protection in

---

https://www.macrumors.com/2019/01/29/apple-1-4-billion-active-devices/ [https://perma.cc/CL8J-ENKS].

[5] *See* Andrea Dodet, *Wearable Technologies: Challenges of a High Growth Market*, COPENHAGEN BUSINESS SCHOOL (Oct. 1, 2015), https://research-api.cbs.dk/ws/portalfiles/portal/58429895/andrea_dodet.pdf [https://perma.cc/SQ3N-YU4Z]. (the author discusses a study reviewing the viability of using wearables to supplement traditional avenues of data collection.)

[6] Selyukh, *supra* note 4; Kenshoo, *supra* note 4; Juli Clover, *supra* note 4.

[7] *See* Isabelle Budin-Ljosne et al, *Dynamic Consent: A Potential Solution to Some of the Challenges of Modern Biomedical Research*, BMC BIOMEDICAL ETHICS (Jan. 25, 2017), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5264333/ [https://perma.cc/VZG4-XQMN].

the United States. The article concludes with proposed next steps for both Washington State and the United States: the best solution will be to strengthen definitions and notice requirements, impose ethical constraints on companies that harvest biometric data, and require them to seek dynamic consent to use the data they gather from consumers.

II. WHY THE FOCUS ON CONSUMER DATA?

Consumer data is big business.[8] Companies use data to understand consumer spending habits, create enticing offers, and deliver goods and services worldwide. Data drives much of what large corporations do, as they use data to build highly accurate, detailed pictures of the world through the lens of their extensive consumer bases.[9] Biometric data may represent the most powerful use of data harvesting the world has ever seen.[10] The abuse of biometric data presents a new arena for those who worry about data privacy around the globe, from the Chinese government's use for "improving" its citizenry to corporate actors spying on consumers through their aggressive data harvesting practices, to the increasing risk of having a data breach reveal the most personal information about a person.[11]

III. BIG TECH'S BIOMETRIC WEARABLES

Multiple tech companies have begun to invest extensively in biometric wearable to cater to a growing desire for at home health data for consumers. This data is a boon to consumers, who are interested in what they can learn about their personal health and can easily become a boon to the companies that will happily begin to collect it. Amazon recently announced its newest project with biometric data harvesting firmly in mind, the Amazon Halo, which can continuously monitor the wearer's biometrics in the name of promoting health and wellness.[12] The amount of

---

[8] Thomas Davenport & Jill Dyché, *Big Data in Big Business*, INTERNATIONAL INSTITUTE FOR ANALYTICS (May 2013), https://www.iqpc.com/media/7863/11710.pdf [https://perma.cc/7QJE-MCMQ].

[9] Kashmir Hill, *How Target Figured out a Teen Girl was Pregnant Before her Father Did*, FORBES (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=5512e81c6668 [https://perma.cc/X4WL-6TLS].

[10] *See generally* J. Chaki, N. Dey, F. Shi and R. S. Sherratt, *Pattern Mining Approaches Used in Sensor-Based Biometric Recognition: A Review*, 19 IEEE SENSORS J., 3569-3580 (May 15, 2019). (a review of data mining practices in biometric wearables and the explosive growth and development they have experienced in the last decade).

[11] Katya Pivcevic, *Chinese Government biometric surveillance intensifying amid pandemic response*, BIOMETRIC UPDATE (Nov. 6, 2020), https://www.biometricupdate.com/202011/chinese-government-biometric-surveillance-intensifying-amid-pandemic-response [https://perma.cc/FGZ2-J4EL] ("Chinafile's report highlights the government's aims to have cameras installed in every aspect of societal life, blanketing particular areas of interest to authorities. However, details of how the nationwide surveillance network operates remain ambiguous"); Simon Denyer, *China wants to give all of its citizens a score – and their rating could affect every area of their lives*, INDEPENDENT (Oct. 24, 2016), https://www.independent.co.uk/news/world/asia/china-surveillance-big-data-score-censorship-a7375221.html [https://perma.cc/K34L-CHJD]; *See* Charlie Osborne, *Big Data or 'Corporate Spying'?*, ZDNET (November 6, 2012), https://www.zdnet.com/article/big-data-or-corporate-spying/ [https://perma.cc/8HTA-5RUC]; *See* Adrian Cheek, Helene Deschamps Marquis, Beth Dewitt, *The growing threat of data breaches*, DELOITTE, https://www2.deloitte.com/ca/en/pages/risk/articles/growing-threat-of-data-breaches.html [https://perma.cc/B29Q-436A].

[12] Phelan, *supra* note 1.

information that Amazon stands to gather through wearable technology as it becomes widespread potentially represents a fundamental shift in how a consumers and their biometric data interact with the corporate world.[13] According to Amazon, the Halo is so finely tuned that it can read a person's emotions based on skin temperature and vocal patterns.[14] While this technology is exciting for its many legitimate consumer uses, the risk of abuse by corporations is significant enough to warrant preemptive government response despite the potential chilling effect preemptive regulation can have.

Amazon debuted the Halo in August 2020 to compete with the Fitbit and the Apple Watch as their first iteration of a wearable healthcare assistant with the ability to monitor a wide variety of health identifiers.[15] Amazon launched the Halo to much fanfare, touting a first-of-its-kind technology that allows the Halo to monitor users' tone of voice to learn about their stress and help users track how their emotions affect their bodies.[16] The Halo includes two microphones, which can be turned on and off at the user's discretion and periodically or continuously monitor the wearer's tone of voice.[17] In concert with the phone application, the Halo can then alert the wearer that they are stressed out or are suffering from another adverse physical reaction to an emotional state.[18] While Amazon has been the most aggressive about utilizing wearables with an expansive scope of biometric data collection possibilities, it is not alone in its efforts to turn biometrics into research-friendly data points.[19]

Google completed the purchase of Fitbit in January 2021.[20] Fitbit was one of the first popular biometric wearables on the US market and which consumers primarily used, as the name suggests, for fitness data tracking.[21] However, Fitbit has not been without controversy even before Google bought the company. In Fitbits early days the company published consumer use data as a default that Fitbit indexed and made searchable by anyone on the internet leading to serious privacy concerns and a violation

---

[13] *Cf.* Alana Semuels, *Many Companies Won't Survive the Pandemic. Amazon Will Emerge Stronger Than Ever*, TIME (July 28, 2020), https://time.com/5870826/amazon-coronavirus-jeff-bezos-congress/ [https://perma.cc/PP8W-YA8N]. (Amazon is debuting this technology as it stands to see a significant increase in its market share as it weathers the pandemic and appears stronger from the decreased competition. This ability to scoop up greater market share will allow it to accumulate even more data from consumers, including from the data it can harvest from its wearables.)

[14] Phelan, *supra* note 1.

[15] Phelan, *supra* note 1.

[16] Phelan, *supra* note 1.

[17] Dieter Bohn, *Amazon Announces Halo, a Fitness Band and App that Scans Your Body and Voice*, THE VERGE (Aug. 27, 2020), https://www.theverge.com/2020/8/27/21402493/amazon-halo-band-health-fitness-body-scan-tone-emotion-activity-sleep [https://perma.cc/A6YK-84MG].

[18] *Id.*

[19] *Id.*

[20] Fowler, *supra* note 12; Michael Liedtke, *Google Muscles up with Fitbit Deal Amid Antitrust Concerns*, Associated Press (Jan. 14, 2021), https://www.detroitnews.com/story/tech/2021/01/14/google-buys-fitbit-amid-antitrust-concerns/115295040/ [https://perma.cc/WF98-PH6B] (Google purchased Fitbit for 2.1 billion dollars).

[21] *Fitbit*, WIKIPEDIA (March 27, 2022), https://en.wikipedia.org/wiki/Fitbit [https://perma.cc/378Y-KJ7M] (Fitbit launched in 2007 and debut their first model in 2009).

of norms if not rules.[22] The social outcry forced them to change that policy and redact the previously posted information.[23] Since the acquisition by Alphabet, Google's parent company, consumers raised alarm bells about whether Fitbit data was going to be combined with Google's other services and sold to advertisers.[24] Currently, Fitbit and Alphabet maintain they are not doing this and have no plans to change.[25] However, relying on corporate promises may not be enough to assuage public concerns about the chance that these corporations change their stance in the future if the money is right.

Apple began its foray into the technology of biometric readings with the Apple Watch. The most recent iteration of the Apple Watch includes a pulse oximeter as part of Apple's latest foray into the healthcare field.[26] All three of these wearables offer healthcare adjacent services that allow the consumer to constantly monitor various health indicators and outputs.[27] For example, Apple has marketed the Apple Watch for its health monitoring capabilities, including its pulse oximeter, heart rate monitor, and step counter, among a variety of other options.[28] However, some problems with the accuracy of Apple Watch's mounted pulse oximeters have many questioning the technology's usefulness.[29] Furthermore, the Apple Watch does not yet monitor the tone of voice for stress or other health indicators. Still, it already has a built-in microphone, which theoretically could be repurposed for such a task.[30]

IV. WHY DATA CONTROL AND CONSUMER CONSENT MATTER?

The oncoming wearables revolution should raise consumer's privacy concerns for a variety of reasons. First, companies can already learn an exceptional amount about a person based on just their browsing

---

[22] *See* Jack Loftus, *Dear Fitbit Users, Kudos on the 30 Minutes of "Vigorous Sexual Activity" Last Night*, GIZMODO (July 3, 2011), https://gizmodo.com/dear-fitbit-users-kudos-on-the-30-minutes-of-vigorous-5817784 [https://perma.cc/W943-3BA6] (Fitbit was tracking and publishing data which included showing when and for how long people were doing things like having sex. While this may not be a violation of rules, many would agree that it is a violation of social norms).

[23] Jennifer Elias, *Some Fitbit users say they are getting rid of the devices because they don't trust Google*, CNBC (Nov. 11, 2019), https://www.cnbc.com/2019/11/17/people-getting-rid-of-fitbits-after-google.html [https://perma.cc/GT99-ZUKZ].

[24] Kari Paul, *'Tossed my Fitbit in the trash': users fear for privacy after Google buys company*, THE GUARDIAN (Nov. 6, 2019), https://www.theguardian.com/technology/2019/nov/05/fitbit-google-acquisition-health-data.

[25] *Id.*

[26] *Pulse Oximeter*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/pulse%20oximeter [https://perma.cc/HZ22-U27T] (a pulse oximeter is "a device that measures the oxygen saturation of arterial blood in a subject by utilizing a sensor attached typically to a finger, toe, or ear to determine the percentage of oxyhemoglobin in blood pulsating through a network of capillaries"); Reed Albergotti, *Apple's New Watch draws attention to its health care play*, THE WASHINGTON POST (Sept. 15, 2020), https://www.washingtonpost.com/technology/2020/09/15/apple-event-2020-apple-watch/ [https://perma.cc/H9CT-9W76].

[27] Phelan, *supra* note 1; Albergotti, *supra* note 20.

[28] Albergotti, *supra* note 20.

[29] Fowler, *supra* note 12.

[30] *Status Icons and Symbols on Apple Watch*, APPLE SUPPORT (Sept. 15, 2020), https://support.apple.com/en-us/HT205550#:~:text=With%20watchOS%207%2C%20the%20microphone%20icon%20means%20your,activates%20the%20microphone%2C%20such%20as%20Handwashing%20or%20Walkie-Talkie [https://perma.cc/X2CS-AJB5].

or buying habits.[31] When Amazon, Google, or Apple partner the information they already gather with a person's emotional response data or other biometric information, the amount they can learn about their consumers quickly becomes unfathomably broad. For example, using location tracking combined with emotional tracking could inform a corporate entity about a driver's road rage, even isolated incidents which do not affect their driving, and allow a corporation to sell that information to an insurance company. Consumers should always have the right to decide if they are comfortable giving Amazon, Google, or Apple information about themselves and whether these corporations can use that information as they see fit.[32] To ensure that consumers feel comfortable, and responsibly informed enough to make that decision, the law will need to keep pace with technology.

The current focus on protecting consumer data and preventing the unfettered sale and trade of consumer biometric data by state and international governments is admirable and important. Current law mandates corporations to protect data, inform consumers of data breaches or hacks that could expose their information, and ensure that entities must either get consent to transfer data or prevent corporations from transferring the data to another entity.[33] However, these laws leave a glaring hole in the regulatory scheme. Massive corporations like Amazon, Google, and Apple can use the biometric information they gather however they see fit, so long as that data stays in-house, without informing their potentially unwitting consumers.[34] These corporations are so large and diverse that they can use the data they gather for a myriad number of purposes, from marketing research to new product development, without the need to contract with a third party and alert users to novel uses.

So long as the law stays silent on this issue, it will not protect consumers from abuse when Amazon, Google, or Apple take the information they gather from health monitoring wearables and put it toward whatever purpose they wish. Whether that is consumer tracking, targeted marketing, or research into how products and website interaction affect users. Without requiring entities to provide notice to consumers and get consent for the projects they plan to use consumer data for—despite all the good that existing privacy protection laws afford biometric identifiers—the lack of notice still places consumers in an unenviable position of turning over data without knowledge of its use or purpose to use the latest technology.

---

[31] Hill, *supra* note 9.

[32] Manoush Zomorodi, *Do You Know How Much Private Information You Give Away Every Day*, TIME MAGAZINE (Mar. 29, 2017), https://time.com/4673602/terms-service-privacy-security/ [https://perma.cc/Y9ZM-HBJH].

[33] 740 ILL. COMP. STAT. 14 (2008): Biometric Information Privacy Act; WASH. REV. CODE § 19.375: Biometric Identifiers; TEX. CODE ANN. BUS. & COM. Title 11, Subtitle A, Chapter 503: Biometric Identifiers; CA. CIV. CODE § 1798.130: California Consumer Privacy Act of 2018 (West 2018); N.Y. GEN. BUS. § 899-aa – 899-bb (McKinney 2019); ARK. CODE ANN. § 4-110: Personal Information Protection Act (West 2019).

[34] WASH. REV. CODE § 19.375: Biometric Identifiers; 740 ILL. COMP. STAT. 14 (2008): Biometric Information Privacy Act (while both laws prevent a private corporation from profiting off the sale or transfer of biometric information, a company can use the information they have gathered for whatever in-house purpose they consider necessary).

Potential consumer data abuse by corporations that gather biometric data is of great concern and preventing this abuse should motivate government at all levels. In house abuses unfortunately do not represent the only threat and the ever-present fear of a data breach should give consumers pause before allowing corporations to collect their personal biometric data.[35] In the event of a large-scale breach, an entity housing the biometric data of millions of users cannot rectify a data breach by giving consumers new eyes or new heart rhythms, it cannot change the way their body responds to stress for them.[36] This data could then very easily become public, for anyone to access, effectively forever.

V. DATA DRIVES THE INFORMATION AGE

Companies in the tech industry rely on data for all manner of things and consumer data is a critical piece of their business model. How efficiently corporations collect consumer data drives how effectively they can use it. Data has become a form of currency for the corporate world in the information age, and the more data companies can gather on their users and consumers, the richer they will become as they translate that information into dollars.[37] Traditional data harvesting helps corporations develop everything from new products to targeted marketing, and when combined with the new accessibility of biometric information, corporations will be able to develop a more fine-tuned target for advertising and product development.[38] As biometric data collection improves and the userbase grows, marketing experts are especially excited about the improvements for real time tracking and the level of insight it provides for anyone monitoring the wearable.[39]

Non-biometric data collection is already a big business as companies are able to build highly accurate pictures of their users based on demographic information, search history, and purchase history that they collect passively as users visit websites, shop in store, and engage with their services.[40] Large companies like Amazon, Google, and Apple already enjoy a dominant position in society and in the market and look to

---

[35] Dan Jackson, *AG Report: Washingtonians Affected by Data Breaches Nearly Doubled in 2020*, WASHINGTON ATTORNEY GENERAL'S OFFICE (Oct. 28, 2020), https://www.atg.wa.gov/news/news-releases/ag-report-washingtonians-affected-data-breaches-nearly-doubled-2020 [https://perma.cc/M5AE-MZ42].

[36] Ron Dichter, *Biometrics: Are We Going Too Far?*, FORBES FINANCE COUNCIL (June 5, 2017), https://www.forbes.com/sites/forbesfinancecouncil/2017/06/05/biometrics-are-we-going-too-far/#1b37671b8d52 [https://perma.cc/82BE-9TE7]. ("biometrics are tricky… [I]f a biometric is compromised, you're done. You can't get a new ear." Quoting an interview with Stanford University Associate Professor of Law Woodrow Hartzog)

[37] *See* Frank Ohlhorst, *Big Data Analytics: Turning Big Data into Big Money*, JOHN WILEY & SONS, (2012) (using data to drive business potential has become so vital that authors are drafting how-to books to help aspiring business owners reap the benefits).

[38] Rex Yuxing Du, Oded Netzer, David Schweidel & Debanjan Mitra, *Express: Capturing Marketing Information to Fuel Growth*, AMERICAN MARKETING ASSOCIATION, J. OF MARKETING, 1-21, 3 (2020), https://journals-sagepub-com.proxy.seattleu.edu/doi/pdf/10.1177/0022242920969198 [https://perma.cc/9KMX-F3C3] (for business purposes, biometric data is being used to evaluate marketing creatives… enabling marketing research firms to collect data on how individuals respond to advertising and identify creatives that are most likely to resonate with the target audience").

[39] *Id.* at 4 ("a compelling aspect of biometric data is its real-time nature. Smartwatches and activity trackers monitor heart rate and blood pressure at a given moment. Such wearable devices also offer a means by which individuals can be motivated").

[40] Hill, *supra* note 9.

take advantage of biometric products to grow their data harvesting ability.[41] The additional capability to track consumer biometric information, like monitoring stress while watching tv or heart rate while driving, will provide these companies with an unheard-of level of access to consumers. Companies with access on this level could effectively know everything about any wearable using consumer in real-time, even down to people's most private and personal emotions.[42] While improved advertising might be a boon to many consumers, the drawbacks of allowing nearly unfettered data collection by corporations warrants a careful case-by-case consideration by consumers about whether they are okay with that level of data collection. The solutions offered in this paper ensure that if consumers are uncomfortable with biometric data collection, they can remove themselves while still enjoying new and improved technology.

Companies are not blind to consumers' privacy concerns, and for now, companies across the board promise they are not storing or mining data they collect and interpret.[43] One day, however, these companies may decide that exploiting harvested consumer biometric data is too profitable or important to ignore. Policy makers must confront how to protect consumer rights before corporate abuse leads to irreparable harm. In most states, any company could sell the data it collects to any third party. Theoretically, a consumer's insurance rates could increase because Amazon sold data showing that consumer's heart rate increases whenever they begin to drive. Companies can collect and store the data indefinitely and use it for any purpose they consider necessary without ever informing consumers they were doing it.

VI. COMPARING BIG TECH DATA HARVESTING TO BIOBANKING RESEARCH TECHNIQUES

Getting samples for medical research can be an expensive and time-consuming process for researchers. To help alleviate this problem, many biomedical researchers have turned to the use of biobanks.[44] A biobank is an organization that collects and stores large quantities of biological samples, ensuring a steady and effective supply of samples for research purposes.[45] Traditional biobanks collect samples from biopsies and other surgeries.[46] They must collect samples from large sections of the

[41] Douglas Schmidt, *Google Data Collection* 2, DIGITAL CONTENT NEXT (Aug. 15, 2018), https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0074-d-0018-155525.pdf [https://perma.cc/79RR-KVX8] ("Google utilizes the tremendous reach of its products to collect detailed information about people's online and real-world behaviors").
[42] Phelan, *supra* note 1 (Amazon Halo can tell when you are stressed and warn you about it.)
[43] Phelan, *supra* note 1.
[44] *See generally* M G Hansson, *Ethics and Biobanks*, 100 BRIT. J. OF CANCER 8 (2008), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2634684/ [https://perma.cc/ZV5Z-G5HN] (the use of human tissue material in combination with information about disease history and lifestyle in biomedical research has attracted a lot of interest by biomedical scientists).
[45] *Cf. Biobank*, NATIONAL INSTITUTE OF HEALTH (July 5, 2016), https://www.nih.gov/AllofUs-research-program/biobank [https://perma.cc/E5ZA-7YM8]. ("a biobank is a repository that stores and manages biological samples known as biospecimens for use in research.")
[46] Elena Lapaz, *The Spanish Biobank Network, 10 years coordinating the collection of samples for research*, EL-LIPSE (Jan. 3, 2020) https://ellipse.prbb.org/the-spanish-biobank-network-10-years-coordinating-the-collection-of-samples-for-research/ [https://perma.cc/Z5FP-ZHAK].

population to ensure they have a wide variety of samples when researchers request access.[47]

Modern tech companies currently engage in large-scale data harvesting and then compile a repository of consumer data points. Amazon, Google, and Apple gather potentially billions of biometric data points from their consumers and store them indefinitely for various uses. Modern tech companies are acting like biobanks with electronic data points replacing physical tissues. Balancing the power dynamic between corporations and consumers is essential and using a dynamic consent model will help shift the balance of power toward consumers.

The most common theory of consent for biobanks is broad consent.[48] Broad consent is the system used when most people think of consent. Usually, a corporation or other entity asks once at the beginning of the interaction for permission to use data or samples in the future.[49] Companies write consent agreements to provide the corporation with extensive leeway to use that data for their ends then. Consumers can still withdraw their consent to have their data collected by request or demand as the situation may require.[50] Companies almost always employ broad consent. By placing board consent language within the terms and conditions, which people usually do not read, they cast as wide a net as possible to catch a large consumer base.[51] Broad consent helps in the biobank world because the samples collected are usually stored for extended periods. It is easy to lose contact with donors who typically do not have an ongoing relationship with the biobank in charge of their samples.[52] Tech companies whose products live on a consumer's wrist or in their pocket have near-continuous access to their donors, a benefit which biobanks do not enjoy. To manage these ethical concerns, broad consent is an easy solution. It allows the biobank to describe the upcoming research framework without specifics and allows the donor to "fire and forget." They can give a sample, sign a form, and never think about it again if they do not want to. They also never know if or for what any samples they may give are used for, which may be a blessing to some and a curse to others.

---

[47] *Id.*

[48] Kristin Steinsbekk, Bjorn Myskja & Berge Solberg, *Board Consent versus Dynamic Consent in Biobank Research: Is Passive Participation an Ethical Problem*, EUR. J. HUM. GENETICS, 897-902 (Jan. 9, 2013), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3746258/ [https://perma.cc/JZC2-UF9G].

[49] *Id.*

[50] *Cf.* Steinsbekk, Myskja & Solberg, *supra* note 48 at 897.

[51] *See* Caroline Cakebread, *You're not alone, no one reads the terms of service agreements*, BUSINESS INSIDER (Nov 15, 2017), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11#:~:text=A%20Deloitte%20survey%20of%202%2C000%20consumers%20in%20the,higher%20with%2097%25%20agreeing%20to%20conditions%20before%20reading [https://perma.cc/8L4W-ZSBR] (roughly 91% of Americans do not read the terms of service for online agreements before they sign them).

[52] *Cf.* Steinsbekk, Myskja & Solberg, *supra* note 48 at 898-899. (because there is a passive relationship between donor and biobank, it is much easier for there to be a loss of communication channels between donor and biobank. Broad Consent needs fewer points of contact between donor and biobank to continue to allow the sample to be useful is beneficial to biobanks because it makes it easier for them to operate. They are not reliant on being able to get in touch with donors continually.)

A burgeoning theory in biobank ethics is the use of "dynamic consent."[53] Dynamic consent is a more active process of obtaining and maintaining donor consent for research projects than broad consent.[54] Dynamic consent requires the biobank to get consent at the time of donation, and every time the biobank uses the donor sample in a new project.[55] The biobank needs to reaffirm consent from the donor for that specific use of their sample.[56] This system has several significant advantages: (1) it centers donors in the decision-making process, (2) it increases respect for the autonomy of donors, and (3) it transfers control of the decision making process of the use of a donor's samples back to the donors.[57] The most significant drawback is the loss of useful samples when the biobank loses contact with donors or when donors refuse to consent for their samples to be used.[58] Unlike the current broad consent model, dynamic consent's stringent framework requiring corporations/ biobanks to provide consumers information about their data use helps keep consumers better informed.[59]

Dynamic consent is still not common in the world of biobanking.[60] Researchers raise concerns about what dynamic consent will mean in practice when it gives individual donors the right to make ethical determinations about where their samples go, potentially constraining research projects because of personal fluctuating ethics, or lack of response to new questionnaires from donors.[61] Maintaining the infrastructure necessary to track donors over an extended period of time to ensure that samples will still be available for use when projects require them will necessitate a change in planning and execution for traditional biobanks.[62] In recognition of these problems, many biobanks have turned to technology to improve the infrastructure they need to communicate with donors efficiently.[63] This embrace of technology by traditional biobanks all but ensures that tech companies will be well positioned to communicate with consumers when they wish to engage with consumers' data. If biobanks can adopt new, more effective means of communicating with donors, then it makes sense that tech companies that regularly exist on their consumer's wrists or in their pockets or both would have a massive advantage in communicating changes in biometric data usage for consumers' dynamic consent.

---

[53] *See generally* Steinsbekk, Myskja & Solberg, *supra* note 48.
[54] *See generally* Steinsbekk, Myskja & Solberg, *supra* note 48.
[55] *Id.* at 898.
[56] *Id.*
[57] *See generally* Steinsbekk, Myskja & Solberg, *supra* note 48.
[58] *Cf.* Steinsbekk, Myskja & Solberg, *supra* note 48. (In a system where samples can't be used unless a donor affirmatively consents to each use of a sample the biggest risk to the biobank is that people will either be unable to respond, forget or for some other reason refuse. A switch to dynamic consent would be forced to address these issues.)
[59] *Id.* at 898.
[60] *Id.*
[61] *Id.* at 901.
[62] *Cf.* Steinsbekk, Myskja & Solberg, *supra* note 48. (The new model proposed by the authors would not be successful without some dramatic shifts in technology and infrastructure use to support it).
[63] *Cf.* Steinsbekk, Myskja & Solberg, *supra* note 48 at 899. (A fair amount of this technology change was driven by a changing ability to use email instead of traditional mail. The rise of smart phones will only improve this ability to reach donors with relative ease.)

Modern researchers have recognized the difficulty common theories of consent in research participation have concerning ethical concerns that arise from massive levels of passive monitoring that comes with the reach of Amazon, Apple or Google.[64] These corporations are doing the sort of data harvesting the largest biobanks can only dream of, thanks to their vast consumer bases.[65] The only significant difference between a traditional biobank and tech companies is the form of the sample.[66]

As private corporations gather more biometric information through wearables, they effectively act more like biomedical research firms engaged in biobanking for undetermined research projects. The imposition of dynamic consent would have a significant benefit in American's daily life when one considers the level of daily involvement Amazon, Google and Apply have on daily life. A significant problem for dynamic consent from a traditional biobank's perspective is losing sample materials because the biobank cannot reach the donor with requests for consent to use their samples. Unlike a traditional biobank, Amazon, Google, and Apple have near continuous access to their users through the ubiquitous nature of smartphones and will be able to ensure higher response rates by using the technology already in place to affirm or deny consent. Every time a new project is about to begin, these tech companies can send an alert to users allowing them the option to consent effectively on the spot to that data usage.[67]

VII. WHERE IS CONGRESS? THE FEDERAL RESPONSE TO BIOMETRIC PRIVACY

Few states have passed laws on biometric privacy, which makes the legal landscape unstable with the potential to shift dramatically if states adopt laws with up to fifty different standards. Despite a minority of states taking up biometric privacy laws, the Federal Government continues to drag its feet in finding a workable solution. The Senate is beginning to

---

[64] *See* Barbara Koenig, *Have We Asked Too Much of Consent*, HASTINGS CENT. REP. 1, 44 (Jul. – Aug. 2014), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4249719/ [https://perma.cc/L3R4-RC5K]. (the idea that consent has its limitations and consent in the context of what Apple, Google, and Amazon are doing is failing the consumers who theoretically should have some idea what it is they are consenting to give meaningful consent).

[65] *See 10 Largest Biobanks in the World*, BIOBANKING.COM (May 28, 2018), https://www.biobanking.com/10-largest-biobanks-in-the-world/ [https://perma.cc/2CQP-RZZX] (the largest biobank in the world has roughly 20 million human derived samples dating back 30 years. These numbers are insignificant when compared to the reach of tech companies whose consumers number in the hundreds of millions or even billions).

[66] *Cf.* Hansson, *supra* note 44. (While the cited paper does not explicitly discuss a comparison between traditional biobanks and tech companies' data collection practices, its discussion of what a biobank is and looks like appears substantially like the data pools collected by tech companies for significant later use).

[67] *Cf.* Andrew Gazdecki, *What is a Push Notification? And Why Should You Care?*, BIZNESS APPS, (Feb. 2014), https://www.biznessapps.com/blog/what-is-a-push-notification/ [https://perma.cc/KC7B-2GLE] (just as Twitter and Facebook can send a push notification to a user's phone when they are tagged or a new post is made, companies that utilize wearables paired to mobile applications can use push notifications to allow users to open a link to review what they would be consenting to allowing their data to be used for and allows the company to comply with dynamic consent requirements).

consider a bill on the subject, though it is still in the first stages of Congressional consideration.[68]

In early August 2020, Senator Bernie Sanders (I-Vt) and Senator Jeff Merkley (D-Or) introduced the National Biometric Information Privacy Act, which is modeled heavily on Illinois's BIPA law.[69] The law is built on three key provisions: (1) a requirement to obtain consent from individuals prior to collecting their biometric identifiers; (2) a private cause of action against covered entities that violate its protections; and, (3) an obligation to protect biometric identifiers similarly to how organizations are required to protect other sensitive information like Social Security Numbers.[70] The bill provides for statutory damages, either $1,000 for each violation or actual damages, whichever would be larger of the two.[71] The bill, as currently proposed, excludes academic institutions and government agencies at every level.[72] The bill requires that all covered entities be required to maintain and publish a written policy detailing their data retention schedule and guidelines for destroying retained biometric information.[73] The bill also limits retention to one year after the consumer's last interaction with the entity.[74] Additionally, the bill incorporates a component of California's general data privacy law, which would create a "right to know," requiring covered entities to inform consumers about the purpose and length of the collection, storage, and use, as well as obtain a written release from consumers about the collection, storage, and use.[75] Finally, the bill would require covered entities to obtain a written release prior to the disclosure of any biometric identifier, which would have to include the data being disclosed, the reason for the disclosure and the recipients of the data.[76]

As of January 2021, the bill has been read twice on the Senate floor and was referred to the Senate Judiciary Committee.[77] The Committee has not acted further since referral.[78] It will be important for those concerned with privacy to monitor and pressure members of the Judiciary Committee to take up the issue in the near future, especially when the alternative is the piecemeal set of solutions states are adopting.

VIII. A BRIEF STATE LAW OVERVIEW

[68] Joseph Lazzarotti, *National Biometric Information Privacy Act, Proposed by Sens. Jeff Merkley And Bernie Sanders*, JDSUPRA (Aug. 6, 2020), https://www.jdsupra.com/legalnews/national-biometric-information-privacy-19153/ [https://perma.cc/KJ33-F7J7].
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] Congressional staffer, *All Actions S.4400*, US Congress, (Aug. 3, 2020), https://www.congress.gov/bill/116th-congress/senate-bill/4400/all-actions.
[78] A search of the Committee on the Judiciaries official website revealed no minutes of proceedings, hearings, or debate on S. 4400 – National Biometric Information Privacy Act. https://www.congress.gov/bill/116th-congress/senate-bill/4400/all-actions.

A small number of states have enacted laws that protect their citizens and punish corporations with civil penalties for selling or distributing biometric information without consumer consent.[79] These states also impose civil penalties if a corporation negligently fails to protect biometric information from data hacks.[80] So far, seven states (Illinois, Washington, Texas, California, New York, Arkansas, and Virginia) have enacted laws that protect the privacy interests of consumers.[81] While a few are biometric specific, the rest are focused more generally on consumer privacy.[82] While all seven states have different requirements to maintain compliance, they all impose different penalties and define protected information in different ways.[83] This patchwork regulatory scheme creates confusion for corporations and consumers that work with biometric information. Maintaining this patchwork regulatory scheme will lead to issues with enforcement and compliance for corporations that will have to contend with a wide variety of complicated laws across state lines. This will increase costs for companies that must follow, and potentially litigate, untested laws each time a state passes a new biometric protection law.[84]

This patchwork of state laws does not work efficiently in a world where most corporations are national or global in scope and use data in a global setting.[85] Violations may vary between states as some states require corporations notify consumers about what their biometric information may be used for, and different states demand notice at different times or for different things. Others may impose stricter requirements like requiring

---

[79] Ted Claypoole & Cameron Stoll, *Developing Laws Address Flourishing Commercial Use of Biometric Information*, BUS. LAW TODAY, AM. BAR ASS'N. (May, 2016), https://www.americanbar.org/groups/business_law/publications/blt/2016/05/08_claypoole/ [https://perma.cc/6C6L-BK87].

[80] *Id.*

[81] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14 (2008); Biometric Identifiers, WASH. REV. CODE § 19.375 (2017); Biometric Identifiers, TEX. CODE ANN. BUS. & COM. Title 11, Subtitle A, Chapter 503; California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.130 (West 2018); N.Y. GEN. BUS. § 899-aa – 899-bb (McKinney 2019); Personal Information Protection Act, ARK. CODE ANN. § 4-110: (West 2019); Rebecca Klar, *Virginia Governor Signs Comprehensive Data Privacy Law*, THE HILL (Mar. 2, 2021), https://thehill.com/policy/technology/541290-virginia-governor-signs-comprehensive-data-privacy-law [https://perma.cc/UA7Z-5L4V].

[82] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14 (2008); Biometric Identifiers, WASH. REV. CODE § 19.375 (2017); Biometric Identifiers, TEX. CODE ANN. BUS. & COM. Title 11, Subtitle A, Chapter 503 (Illinois, Texas, and Washington are all specific to biometrics) California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.130 (West 2018); N.Y. GEN. BUS. § 899-aa – 899-bb (McKinney 2019); Personal Information Protection Act, ARK. CODE ANN. § 4-110: (West 2019); Klar, *supra* note 81 (The rest have only general data privacy protection laws that apply to consumer biometrics by extension)

[83] California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.130 (West 2018); Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14 (2008); Biometric Identifiers, WASH. REV. CODE § 19.375 (2017) (for example, California law encapsules their biometric protection in a general data privacy bill while states like Washington and Illinois specifically target and define protected biometric data and identifiers).

[84] Shaun Jamison, Note, Creating *a National Data Privacy Law for the United State*, 10 CYBARIS 1, Article 2. (2019), https://open.mitchellhamline.edu/cybaris/vol10/iss1/2 [https://perma.cc/WBC9-V2AN].

[85] *See* Dan Alaimo, *Amazon Dominates International Marketplace Reach*, RETAIL DIVE (Sept. 10, 2018), https://www.retaildive.com/news/amazon-dominates-international-marketplace-reach/531926/ [https://perma.cc/T526-XUCT]. (in 2018 Amazon reached across 58 countries and had the world's largest online population reach of 1.2 billion people).

consent before companies can use their data.[86] These statutory inconsistencies create a situation where companies risk making costly mistakes in the patchwork system, or where they may simply stop doing business in the jurisdictions that impose the strictest requirements. The world's reliance on the internet can make legal changes arising at state boundaries a hinderance if corporations must adjust their virtual world up to fifty different ways. The federal government can help alleviate the stress of a state-by-state patchwork by adopting a national standard.

Enforcement varies across state lines. Some states rely on a private cause of action wherein any citizen can bring a claim for monetary damages against any company they believe has violated their biometric privacy rights.[87] On the other hand, some states limit who may bring the action to the state Attorney General's office, typically under the framework of the state's consumer protection act.[88] Limiting the cause of action to the Attorney General's office creates a significant risk of under-enforcement in situations where the state Attorney General's office does not have the political will or the resources to pursue these infractions.[89] This bottleneck does more harm than good to consumers who are looking to ensure that companies in violation of the law are held accountable for their transgressions or mistakes.

IX. STATE SOLUTIONS: THE IMPORTANT TANGIBLE DIFFERENCES BETWEEN TWO COMPREHENSIVE BIOMETRIC DATA PROTECTION LAWS IN ILLINOIS AND WASHINGTON

Illinois passed the nation's first biometric specific data protection law. Every state since then has copied the basic parameters of the Illinois biometric data protection scheme. While each state invariably has tweaked the law to a certain degree, the concepts remain largely the same across the country. Illinois has one of the only state laws that allows a private cause of action and because it has been in effect the longest, the state has built up the largest amount of case law on the topic. This allows for a more thorough analysis of the impacts a private cause of action for violations of biometric law has on the state and the consumers within.

---

[86] California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.130 (West 2018) (California's Information privacy law requires only that business which collect personal information provide notice to consumers); Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14 (2008) (Illinois requires corporations provide both notice and consent before private entities can gather and store consumer biometric data).

[87] *See* NBC, *Illinois Facebook Users Can Now File Claims for Payouts in $650 Million Lawsuit settlement*¸ NBC CHICAGO (Sept. 22, 2020), https://www.nbcchicago.com/news/local/illinois-facebook-users-can-now-file-claims-for-payouts-in-650-million-lawsuit-settlement/2342967/ [https://perma.cc/3777-ZTU4] ("the lawsuit — one of more than 400 filed against tech companies big and small in the past five years, by one law firm's count…").

[88] TEX. CODE ANN. BUS. & COM. Title 11, Subtitle A, Chapter 503; Biometric Identifiers, WASH. REV. CODE § 19.375: Biometric Identifiers (2017) (Texas and Washington limit the cause of action to the state Attorney General's Office).

[89] WASH. REV. CODE § 19.375: Biometric Identifiers (2017) (Washington State's biometric protection law only creates a public cause of action through the Attorney General's office through the framework of the state's Consumer Protection Act. Private citizens have no personal ability to sue offending companies).

A. Illinois

In 2008, Illinois passed the Biometric Information Privacy Act (BIPA).[90] This was the first privacy law in the U.S. that specifically protected biometric information.[91] Illinois employed a narrow definition of biometric identifiers, limiting protections to the following identifiers: iris scans, fingerprints, voiceprints, and facial or hand geometric scans.[92] Besides being the first of its kind, BIPA is the only state law that explicitly grants a private cause of action to its citizens, allowing them to pursue private civil suits when they believe their biometric privacy rights have been infringed upon by a corporation.[93] The law also limits how long a company is allowed to maintain records of consumers' biometric identifiers.[94] Additionally, the law created standard damages for each infraction, delineating between negligent violations ($1000 per infraction) and willful or reckless violations ($5000 per infraction).[95] Furthermore, the law imposes strict requirements on corporations; the corporation must obtain written informed release from each consumer to transfer information to any other entity.[96] Even with this release, BIPA prevents a corporation from profiting off the transfer of biometric information.[97]

Illinois's private cause of action provision has significantly affected litigation in the state. Illinois has become a hotbed of class action litigation against companies that deal in biometric information.[98] The largest class action suit was settled in 2020 against Facebook and created a $650 million award to be distributed to Illinois' Facebook users whose data was used improperly.[99] This class action suite arose out of Facebook's use of artificial intelligence in facial recognition technology through Facebook's photo tagging feature.[100] Facebook created a massive database of every user's face for the tagging feature without asking users for their consent.[101] The rise in litigation has been a double-edged sword for the state as it has led to large class-based payouts for BIPA violations, while also substantially increasing litigation costs as hundreds of plaintiffs brought suit for violations by businesses around the country.[102] The benefits to consumers from class-based payouts and the changes it invariably drives in market decisions likely outweighs the negatives of increased costs due to large amounts of litigation.

---

[90] 740 ILL. COMP. STAT. 14: Biometric Information Privacy Act (2008).
[91] *See Id.* (Illinois BIPA law, passed in 2008, was the first of its kind in the nation).
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] NBC Chicago, *supra* note 87.
[99] *Id.*
[100] NBC Chicago, *supra* note 87.
[101] *Facebook Claims*, DATA DIVIDEND PROJECT (Nov. 23, 2020), https://www.datadividendproject.com/cladetails/facebookclaims [https://perma.cc/37TC-LPAL] ("Facebook users in Illinois filed a class action, alleging that Facebook had not obtained written releases from them and retained the data without retention deletion schedules as required by the Illinois Biometric Information Privacy Act").
[102] Lazzarotti, *supra* note 68; DATA DIVIDEND PROJECT, *supra* note 101; NBC Chicago, *supra* note 87.

Deciding how much of this litigation is called for will continue to plague any legislature crafting a bill centered around protecting biometric privacy. State legislatures will have to decide if they want to subject companies and courts to more potentially frivolous lawsuits and accept the attendant costs in exchange for getting more money to injured private citizens, or if it would be better to provide a bottleneck with the state Attorney General's office.[103] Either option creates benefits and drawbacks. State Attorney's General can ensure that lawsuits are worth bringing, thereby limiting their number, which keeps litigation costs down. This option is beneficial to both companies and the court system. Allowing for private causes of action ensures that companies are directly answerable to the people who suffer from their wrongful acts or negligence. This option is more beneficial to private citizens who have been harmed.

B. Washington

Washington State adopted a biometric privacy protection law, last amended in 2017, which focused on preventing corporations from negligently or willfully releasing protected consumer biometric information.[104] Similar to the law in Illinois, Washington requires the company gathering biometric identifiers to either provide notice and obtain consent or provide a mechanism to stop the data from being distributed outside the collecting entity.[105] Washington's law defines biometric identifiers using traditional metrics like fingerprint, voiceprint, iris or retina scans.[106] The law also includes a catchall provision for "unique biological patterns or characteristics that is used to identify a specific individual."[107] The Washington law lacks a private cause of action and standards for how long the company will store data after the last usage.[108] The law carves out audio or video records and the data or information generated or derived from those recordings when used in security and law enforcement spheres.[109] The law also creates complex technical disparities between audio recording exemptions and voiceprints being considered protected information.[110] The distinction that an audio recording is acceptable but the spectrographic production of the same audio recording is not may create more confusion than it does protection.

---

[103] Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, Regulating Biometrics, 96-103, 97, https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf#:~:text=While%20other%20states%20such%20as%20Texas%20and%20Washington,United%20States%20with%20a%20private%20cause%20of%20action [https://perma.cc/5C3B-NTAJ].

[104] WASH. REV. CODE § 19.375: Biometric Identifiers (2017).

[105] *Id.*

[106] WASH. REV. CODE § 19.375.010: Biometric Identifiers: Definitions (2017).

[107] *Id.*

[108] WASH. REV. CODE § 19.375: Biometric Identifiers (2017).

[109] WASH. REV. CODE § 19.374.040.

[110] A voiceprint is "an individually distinctive pattern of certain voice characteristics that is spectrographically produced" *Definitions of voiceprint*, MERRIAM-WEBSTER https://www.merriam-webster.com/dictionary/voiceprint [https://perma.cc/C4UM-7H3B]; *Cf.* WASH. REV. CODE § 19.375.010: Biometric Identifiers: Definitions (2017) (because the law treats an audio recording and voiceprint differently it may create problems with enforcement as the two types of audio analysis overlap with each other in how they are captured).

As technology around biometric data harvesting improves, the information that Amazon, Google and Apple can derive from that data should change how Washington defines protected biometric identifiers. To keep up with the changing technological landscape, the law must expand to include protected biometric information to keep pace with the increasingly granular level of information that companies can glean off the biometric information they harvest.

The difference between Washington and Illinois' enforcement of their respective laws is stark. Since the Illinois law's inception, private actors brought over 400 lawsuits against companies that allegedly violated BIPA.[111] In contrast, the Washington State Attorney General's office has not initiated any lawsuits for violations of Washington's biometric privacy protection law despite 60 reported data breaches in 2019 and 51 cases in 2020.[112] The problems with Washington's enforcement system are self-evident because the State Attorney General's office either lacks the resources or lacks the political will to pursue these violations. While the court may dismiss a larger number of lawsuits in Illinois before discovery under Illinois's BIPA law, the difference between 400 and zero provides a stark example of the weakness of placing the only enforcement mechanism in the hands of an Attorney General's office.

X. WHAT SHOULD LEGISLATURES DO TO ADDRESS THESE PROBLEMS?

There are a variety of proactive steps that both state and the federal legislators should consider adopting to cut off the problems before they get out of hand. Legislators should take steps to ensure that consumers have all the information they need to give consent for the use of their biometric data such as defining and limiting what companies like Amazon, Google, and Apple are able to do with biometric information they gather without the informed consent of their consumers. Washington State should expand the definition of protected biometric information beyond the list of "identifiers," currently based around face, retinas, and fingerprints, to include biometric information more generally.[113] To strengthen the law further, Washington should amend the law to require consumers to opt in instead of the current standard where companies provide notice and allow consumers to opt out.[114] This will prevent default bias and ensure that more biometric data is protected.[115] It will also ensure that companies who want

[111] NBC Chicago, *supra* note 87.
[112] Jackson, *supra* note 35 (A review of the Washington State Attorney General's office website returned no results for lawsuits resulting from reported data breaches).
[113] WASH. REV. CODE § 19.375.010: Biometric Identifiers: Definitions (2017).
[114] 740 ILL. COMP. STAT. 14, Biometric Information Privacy Act (2008); WASH. REV. CODE § 19.375: Biometric Identifiers (2017). (most data privacy laws default to allowing data collection while allowing consumers the option to opt out).
[115] Crawford Hollingworth & Liz Barker, *Bias in the Spotlight: default bias*, RESEARCH WORLD (July 31, 2020), https://archive.researchworld.com/bias-in-the-spotlight-default-bias/#:~:text=%EE%80%80Bias%20in%20the%20Spotlight%3A%20default%20bias%EE%80%81.%20When%20presented,or%20our%20voice%20mail%2C%20which%20we%20rarely%20change [https://perma.cc/7Z9V-KW2Z]. (default bias is the idea that people, when an option from a preset list is preselected for them, will tend to "go with the flow." A simple example is our voicemail message which people rarely change when a basic one is provided).

to collect such data will have to explicitly ask and will ideally encourage transparency to bring consumers on board with the idea of data harvesting. The current standard is weaker because "for consumers with weak or conflicted preferences, any default will be 'sticky,' meaning that more consumers will stay in the default position."[116] Lastly, the most important thing Washington should do is create a private cause of action to ensure that corporate mistakes and malfeasance will be held to account by the people who they harm. The Senate should amend Senate Bill 4400 in line with the amendments proposed for Washington's biometric privacy law.[117]

Governments at every level should broaden the definition of what data biometric privacy laws protect. Additionally, the government should treat corporations that engage in electronic biometric data harvesting as biobanks and impose similar ethical donor consent requirements on what corporations may do with data.[118] The United States would better serve consumers by requiring that corporations use a dynamic consent model.

A. Proposed Solution: United States

The United States should adopt a national standard by passing Senate Bill 4400. This bill, referenced above, relies on similar language and provisions as Illinois' BIPA. Senate Bill 4400, currently in committee, is a sensible, effective law that would create a national standard centering biometric data protection in the hands of corporations and would give enforcement options to the public.[119] Nationalizing the standards in biometric data protection will provide clarity for both businesses and consumers as well as ensure protection from security breaches for residents of states that have failed to pass data privacy laws which extend to biometrics.[120]

The Senate should also expand the scope of the bill to include biometric information beyond traditional identifiers. The law should also bar the transfer of non-identifying biometric information when packaged with any form of personally identifying information.[121] Currently, entities can transfer these information packages without violating existing iterations of state biometric identifier privacy laws.[122] Closing this loophole will help protect consumers nationwide from abuses that could arise from the transfer of anonymous biometric information with other information that data analytics will be able to use to reidentify a wearables user. Finally, Congress should amend the proposed bill requiring entities

---

[116] Lauren Willis, *Why Not Privacy by Default*, 29 BERKELEY TECH L. J. 61, abstract (2014), https://dSchoash.harvard.edu/bitstream/handle/1/11266829/Why%20Not%20Privacy%20by%20Default%20Nov3.pdf?sequence=1&isAllowed=y [https://perma.cc/W25E-4NH4].

[117] Lazzarotti, *supra* note 68.

[118] Hansson, *supra* note 44.

[119] Steinbekk, Myskja, Solberg, *supra* note 48.

[120] *See* Pope, *supra* note 3.

[121] *See* Tanusree Sharma, Masooda Bashir, *Toward a Comprehensive set of PII for Ensuring Privacy Protections*, IDEALS (Dec. 5, 2020), https://www.ideals.illinois.edu/bitstream/handle/2142/109067/PII%20Paper-TS.pdf?sequence=2&isAllowed=y [https://perma.cc/ScZK9U-QPBK].

[122] *Id.* (experts already worry about the ability of data analytics to link what were previously anonymous data sets to re-identify participants. Closing as many loopholes as possible to prevent transfers of even anonymized data should be a top priority for lawmakers).

to obtain informed consent from consumers to use collected biometric data each time they wish to use biometric data for a new project. Companies adopting a dynamic consent standard provides consumers with sufficient notice and will allow consumers to determine the extent to which corporation may use the data they collect in each new project, will ensure that consumers have an informed understanding of corporate data usage, and will help to limit abuses of information which can arise when corporations use consumer biometric data without their knowledge or consent.[123]

Consumer protections of biological information does not seem to be a partisan issue in Congress. President Biden has not expressed a stance one way or another on specific consumer privacy changes regarding biometrics or otherwise.[124] There has been some early pushback on the Senate bill by security and law enforcement who argue the bill is out of touch and does not speak to realities on the ground.[125] Legal experts expect the Biden administration to make consumer privacy protections a priority issue; however, the extent to biometrics remains to be seen.[126] Further, as the United States deals with cultural changes, protecting biometric data does not seem to be the kind of bill that would motivate either party or partisan group based on some sort of US "culture wars."[127] This should hopefully improve its chance at passage because it will not be made into a partisan punching bag and can instead be negotiated in good faith.

The companies at the center of this argument around the right level of legal protections for biometric information employ strong lobbying arms and commit millions of dollars a year to ensure that they have a say in the political workings of the country.[128] Amazon, Google, and Apple will likely aggressively lobby against any additional requirements that curtail their freedoms to freely use the information they harvest.[129] Congress should not be deterred from debating legislation already put forth in the Senate despite the inevitable lobbying against national legislation. Amending the legislation to include a private cause of action and greater protections for packages of information that avoid current legal bars to transfer.

---

[123] Isabelle Budin-Ljosne et al, *supra* note 7.
[124] White House, https://www.whitehouse.gov/?s=boimetric+privacy (visited Feb. 2, 2021) [https://perma.cc/9KEG-P8HB] (a search of the White House website reveals no information or formal policy stance by the Biden Administration on biometric data or privacy policy in the field).
[125] *See* Joel Griffen, *Senate bill would place limits on use of facial recognition, other biometrics by private companies*, Security Info Watch (Aug. 5, 2020), https://www.securityinfowatch.com/access-identity/biometrics/facial-recognition-solutions/news/21149050/senate-bill-would-place-limits-on-use-of-facial-recognition-other-biometrics-by-private-companies [https://perma.cc/B8BJ-HN5V].
[126] Kristin Bryan, Lydia de la Torre, Glenn Brown & Aaron Garavaglia, *Election 2020: Looking Forward to What a Biden Presidency May Mean for Data Privacy and Data Privacy Litigation*, SQUIRE PATTON BOGGS (Nov. 12, 2020), https://www.consumerprivacyworld.com/2020/11/election-2020-looking-forward-to-what-a-biden-presidency-may-mean-for-data-privacy-and-data-privacy-litigation/ [https://perma.cc/2436-BMW2].
[127] *Culture War*, DICTIONARY.COM, https://www.dictionary.com/browse/culture-war (visited April 4, 2021) [https://perma.cc/836A-K6NB] ("a conflict or struggle for dominance between groups within a society or between societies, arising from their differing beliefs, practices, etc").
[128] Cecila Kang and Kennith Vogel, *Tech Giants Amass a Lobbying Arm for an Epic Washington Battle*, THE WASHINGTON POST (June 05, 2019) https://www.nytimes.com/2019/06/05/us/politics/amazon-apple-facebook-google-lobbying.html [https://perma.cc/ZGL6-APE9].
[129] *Id.*

B. Proposed Solution: Washington State

Washington's legislature should take the initiative to create better biometric privacy laws while fighting for a uniform federal law. Washington should amend their biometric privacy law to supply a private right of action using a heightened pleading standard, broaden how the state defines biometric identifiers to include certain other biometric data, and impose a dynamic consent standard on companies that want to collect or use consumer biometric data. Washington's law could be significantly improved if the legislature were to take a few critical steps to improve the law. The first step is to amend the law to incorporate a private cause of action because the Washington State Attorney General has not brought suit to protect state citizens and may not be able to bring the necessary resources to bear.[130] Washington's version of biometric data security law is enforced under the Consumer Protection Act, and therefore only enforceable by the Washington State Attorney General.[131] The framework of the Consumer Protection Act does not have enough of an impact on protecting consumer data stolen via data breaches. However, it has decreased the overall number of attacks yearly.[132] Further, as referenced above, the Washington State Attorney General's office has not sued an entity for a violation of Washington's biometric protection laws.[133] The disparity between the flood of litigation in Illinois over violations of their biometric protection law and Washington's are substantially similar means that the large number of lawsuits in Illinois are arising primarily because Illinois' citizens can bring suit for violations.[134] In Washington, aggrieved consumers, must rely on the Attorney General.[135] The Illinois Facebook settlement shows violations of both Washington's and Illinois' laws that require more robust enforcement measures to protect Washingtonians.[136] Consumers will be negatively impacted with little recourse to address data breaches or the willful use of their biometric data in inappropriate ways on their own without changes to Washington law.

Data breaches and corporate abuses of consumer biometric information present a unique danger to consumers due to the individual uniqueness of such information, the inherently extremely personal nature,

---

[130] Jackson, *supra* note 35.
[131] WASH. REV. CODE § 19.375.030.
[132] Jackson, *supra* note 35. (The 2020 report by the state Attorney General's office "showed that the number of Washingtonians affected by breaches nearly doubled in the last year…33 cyber-attacks were reported to our office in 2020… 2019 when 43 cyberattacks were reported").
[133] Jackson, *supra* note 35. (a contemporaneous search of the Washington State Attorney General's website revealed no suits under Washington's Biometric Data Protection Act).
[134] NBC Chicago, *supra*, note 87 (there have been more than 400 class action lawsuits related to BIPA since its passage in Illinois); Jackson, *supra*, note 35 (there have been no lawsuits in Washington under its biometric privacy law).
[135] WASH. REV. CODE § 19.375.030.
[136] *See* NBC Chicago, *supra* note 87 (The violations in data harvesting in Illinois were not limited by the state's geography and because both Washington and Illinois law work in substantial similar way in terms of the privacy protections, Facebook's violation of BIPA almost certainly resulted in a similar violation here in Washington).

and the fact that a person whose biometric data is compromised by a hack is left with little recourse. Unlike other data breaches where banks can change credit card numbers, an individual cannot change his or her iris shape or blood O2 measurements.[137] The loss of immutable information is a special danger because it cannot be changed if it becomes compromised. A nefarious actor who gains access to the biometric data a consumer uses to lock their bank account now has access to that biometric data forever. A consumer will either be at risk of having their bank account hacked or be unable to use that biometric data for security purposes ever again. This danger outweighs any chilling effect such new legislation may have on improvements to the technology or the societal uptake of biometric wearables. The immutable nature of biometric data presents a particular problem in the face of data breaches. Consumers should have extra ability to limit the spread of their biometric data to less secure corporations. The state legislature should amend the law to strengthen biometric protections based on this special danger. A private cause of action will ensure that companies are vigilant to prevent state law violations.

i. Dynamic Consent

The most effective method to protect consumers would be Washington State amending the current law to require corporations to use dynamic consent standards when interacting with consumers to ask permission to harvest consumer biometric data and the proposed amended version of the current law.

ii. Private Cause of Action with Statutory Damages

The private cause of action could grant Washingtonians the right to sue companies that do not get dynamic consent to use data on new projects or for data breaches. The law should also codify statutory damages. Calculating damages for a breach of this nature would be difficult. Courts would likely be hard pressed to develop reasonable damage awards for victorious plaintiffs without a statutory standard.[138] Using Illinois as a model, Washington should create similar statutory damage requirements for negligent violations ($1000 per infraction) and willful or reckless violations ($5000 per infraction).[139]

iii. Impose a Heightened Pleading Standard to Prevent a Flood of Vexatious Litigation

A proposed solution that will allow Washington to find the right balance of enforcement litigation is to use a heightened pleading standard

---

[137] *See* Pope, *supra* note 3.
[138] *See* Sande Buhai, *Statutory Damages: Drafting and Interpreting*, 66 U. KAN. L. REV. 523-563, (2017), https://heinonline-org.proxy.seattleu.edu/HOL/Page?collection=journals&handle=hein.journals/ukalr66&id=615&men_tab=srchresults [https://perma.cc/X79X-UTVC].
[139] 740 ILL. COMP. STAT. 14: Biometric Information Privacy Act, (2008).

in the private cause of action. Heightened pleading standards are used to great effect in other areas of the law, most notably fraud.[140] The heightened pleading standard would require plaintiffs bringing a private cause of action to plead, with particularity, all allegations of how their data was misused or the company's failure to take reasonable steps to protect it.[141] That would allow private parties who believe their privacy rights have been infringed upon to bring suit while also helping ensure corporations who harvest data are not crushed under a constant barrage of potentially frivolous litigation making it to discovery, which can be extremely expensive.[142]

The current law's lack of a private right of action is another significant drawback in how it protects specific biometric identifiers.[143] The law is also hampered by the lack of a modern set of definitions for protected biometrics. These include "fingerprints, voiceprints, eye retinas, irises, and other unique biological characteristics."[144] However, as private entities harvest more data and engage with that data in more complicated ways, biometric information goes beyond traditional considerations of a biometric identifier.[145] The information that wearables gather goes beyond what the law has traditionally defined as an "identifier."[146] A prime example is as follows: a person's O2 measurements may not be personally identifiable, but it would still be concerning if a corporation could take those readings from a person at will. The Halo can even measure a person's emotional state and allowing a corporation to know how a person is feeling at any given time is likely a concern for many people.[147] Emotional readouts do not meet the current definition of a biometric identifier under Washington law.[148] Society generally may not think of emotions as a biometric identifier, but consumers may view it as an aggressive invasion of privacy. The legislature should amend the law to include protections for biometric information more generally.

Washington's current law requires a corporation to notify consumers about the company's plan to harvest biometric data.[149] Consumers tend not to read documents and clauses hidden deep in the

---

[140] *See* Federal Rules of Civil Procedure 9(b): Pleading Special Matters; Fraud or Mistake
[141] *Id.*
[142] Elizabeth J. Cabraser & Katherine Lehe, *Uncovering Discovery*, 12 SECONA CONF. J. 1 (2011), https://thesedonaconference.org/sites/default/files/publications/Cabaser%201-46_0.pdf [https://perma.cc/U6JZ-R9R6].
[143] WASH. REV. CODE 19.375.010: Biometric Identifiers: Definitions "biometric identifiers" under Washington law is considered "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual").
[144] WASH. REV. CODE 19.375.010: Biometric Identifiers: Definitions
[145] *See* Maria Korolov, *What is biometrics? 10 physical and behavioral identifiers that can be used for authentication*, CSO ONLINE (Feb. 12, 2019), https://www.csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-biometric-data-is-risky.html [https://perma.cc/7NTZ-2X8A] (Washington law does not specify things like stress responses or heart rhythm in its list of biometric identifiers, but they are nonetheless commonly individualized. Biometrics even extend as far as behavioral responses).
[146] *See* Phelan, *supra* note 1 (The Halo can track many physical aspects of a person beyond biometric identifiers).
[147] *Id.*
[148] WASH. REV. CODE 19.375: Biometric Identifiers.
[149] WASH. REV. CODE 19.375: Biometric Identifiers.

terms and conditions of the myriad products people consume daily.[150] Similarly,, consumers fail to read the terms and conditions on their important documents like mortgages or car leases; therefore, consumers are unlikely to read the terms of conditions on everyday products.[151] States should respect consumer autonomy; therefore, these limits should be aimed at stopping in-house abuses of harvested data by covered entities as opposed to halting all data harvesting. Washington can strengthen consumer protection by requiring corporations to inform their consumers what they are doing with their data, including what they do in-house. Limiting the risk of in-house abuse will ensure consumers have greater peace of mind to make their choices without worrying about abuse by corporations they allow to harvest their data. States across the country have shown that the best way to protect consumer biometric information from theft by a data breach is to put the onus on the company that wants consumer biometric data.[152] The next step in that protection scheme should require covered entities to obtain informed consent. Washington should require more than simple notice; informed consent should be a minimum addition to the law as written.[153] The current notice requirements are low, and the entities covered by the law could provide notice by burying the terms hundreds of pages deep in the terms and conditions. Requiring corporations to use dynamic consent would regularly update consumers on plans for data use. It will ensure that consumers have a more active role in whether and how covered entities use their data.[154]

Dynamic consent would require greater effort from covered entities to inform consumers about the inherent risks of giving away or allowing the harvest of their biometric information.[155] Requiring a short and plain statement of the risks of sharing biometric data would ensure that consumers can make informed decisions.[156] Requiring that the consent form be provided separately from the rest of the terms and conditions will make it more likely that consumers will read it.[157] Dynamic consent would also allow consumers to retain greater control over what happens to and

---

[150] Ian Ayres; Alan Schwartz, *The No-Reading Problem in Consumer Contract Law*, STANFORD L. REV., 545-607, 546 (Mar. 3, 2014), http://www.stanfordlawreview.org/wp-content/uploads/sites/3/2014/03/66_Stan_L_Rev_545_AyresSchwartz.pdf [https://perma.cc/U5NR-TQPR].

[151] *Id.* at 546-547 (Citing Kleimann Communication Group, Inc., *Know Before You Owe: Evolution of the Integrated Tila-Respa Disclosures*, 25 (2012), http://files.consumerfinance.gov/f/201207_cfpb_report_tila-respa-testing.pdf [https://perma.cc/NB3M-E38S]).

[152] 740 ILL. COMP. STAT. 14 (2008): Biometric Information Privacy Act; WASH. REV. CODE § 19.375: Biometric Identifiers; TEX. CODE ANN. BUS. & COM. Title 11, Subtitle A, Chapter 503: Biometric Identifiers; CA. CIV. CODE § 1798.130: California Consumer Privacy Act of 2018 (West 2018); N.Y. GEN. BUS. § 899-aa – 899-bb (McKinney 2019); ARK. CODE ANN. § 4-110: Personal Information Protection Act (West 2019).
(every state law that protects biometric privacy require the company to actively work to protect the data).

[153] *Informed Consent: More than Getting a Signature*, QUICK SAFETY (Feb. 2016), https://www.jointcommission.org/-/media/deprecated-unorganized/imported-assets/tjc/system-folders/joint-commission-online/quick_safety_issue_twenty-one_february_2016pdf.pdf?db=web&hash=5944307ED39088503A008A70D2C768AA [https://perma.cc/3322-XGLT].

[154] Budin-Ljosne et al, *supra* note 7.

[155] Budin-Ljosne et al, *supra* note 7.

[156] *Cf.* Quick Safety, *supra* note 153.

[157] *Id.*

with their data.[158] Washington should impose ethical constraints on what private entities may do with consumer biometric data and require consent to collect the data and use it on specific projects.[159] Washington and the Federal Government should treat entities like Amazon, Google, and Apple as biobanks and impose similar ethical constraints, including requiring dynamic consent from consumers because they function like donors for a biobank. Washington and the Federal Government can strengthen privacy protections while still ensuring that if consumers are comfortable with Amazon, Google, and Apple using their biometric information, those corporations are still allowed to do so.

Requiring dynamic consent also ensures that if a corporation were not previously retaining biometric information decides to begin retaining consumer biometrics, that corporation would have to alert consumers to the change and provide those consumers the opportunity to decide for themselves if that is acceptable to them. This will allow consumer to make choices to protect their privacy without forcing them to decide if they want to keep using their devices or turn their wearable into nothing more than a wristband.

XI. CONCLUSION

Biometric wearables are quickly becoming commonplace as people enjoy using them for various health and fitness goals or simple personal curiosity. As their use grows, so does the risk of harm arising from the theft or corporate misuse of consumer data harvested by these wearables. The heart rate monitors, wristbands, watches, and vocal emotion detection software people are wearing are getting smarter and recording more aspects of our lives.[160] It is only a matter of time before companies begin to harvest consumer biometric data on a grand scale as companies begin to embrace the power of biometric data in marketing and other market research. These large tech companies will start to act like biobanks gathering samples for use in later undetermined projects when they do. The US should proactively impose the same ethical constraints on corporations that operate like biobanks as they do on traditional biobanks. The use of dynamic consent will also help protect consumers from corporate abuses. Giving consumers the choice to use dynamic consent helps protect them from abuses when corporations use their data without their knowledge. The paper also supplied an overview of state laws in Illinois and Washington that represent the quality of protections for biometric identifiers and demonstrate two potential options for enforcement of biometric protections. Private causes of action will allow consumers to have greater enforcement powers to ensure that when corporations violate laws that protect biometric data.

Washington State and the Federal Government must recognize reality and protect biometric data beyond identifiers. The best way to do

[158] Budin-Ljosne et al, *supra* note 7.
[159] Hansson, *supra* note 44.
[160] Bohn, *supra* note 17.

so is to amend existing Washington law to provide a private cause of action with a heightened pleading standard that will allow for greater enforcement than the Washington State Attorney General has provided under the Consumer Protection Act framework.[161] This will allow Washington State to strike an appropriate balance between chronic under-enforcement and prevent the tidal wave of litigation that has inundated Illinois. The United States needs a uniform national law to provide a standard and prevent problems with a patchwork legal system. The Federal Government should take up and pass an amended version of the bill put forward earlier this year by Senators Sanders and Merkley, which would create a national biometric information protection act with a system for requiring dynamic consent from consumers before covered entities can use their data.[162]

Governments will need to act preemptively to limit the damage that could arise from abuses of biometric data. The need for preemptive action comes from the unique nature of biometric data that distinguishes it from traditional forms of data.[163] Biometric data is immutable and inherently more personal than any other form of data. The government and private entities cannot reissue new retinas or a new heartbeat like they can with other personal information.[164] In the realm of biometrics, the traditional American ideal of letting the free-market act and only stepping in when a problem arises will fail consumers. Preemptive action is the only way to prevent an unfixable problem.

[161] NBC Chicago, *supra*, note 87 (there have been more than 400 class action lawsuits related to BIPA since its passage in Illinois); Jackson, *supra* note 35. (there have been no lawsuits in Washington under its biometric privacy law).
[162] Lazzarotti, *supra* note 68.
[163] Dichter, *supra* note 36 (primarily biometrics' immutable nature. "Biometrics are tricky… [I]f a biometric is compromised, you're done. You can't get a new ear") (Quoting an interview with Stanford University Associate Professor of Law Woodrow Hartzog).
[164] *Id.*