St. John's Law Review

Volume 96, 2022, Number 4 Article 12

Keep Your Fingerprints to Yourself: New York Needs a Biometric Privacy Law

Brendan McNerney

KEEP YOUR FINGERPRINTS TO YOURSELF: NEW YORK NEEDS A BIOMETRIC PRIVACY LAW

BRENDAN MCNERNEY[†]

INTRODUCTION

Imagine walking into a store, picking something up, and just walking out. No longer is this shoplifting, it is legal.[1] In 2016, Amazon introduced their "Just Walk Out" technology in Seattle.[2] "Just Walk Out" uses cameras located throughout the store to monitor shoppers, document what they pick up, and automatically charge that shoppers' Amazon account when they leave the store.[3] Recently, Amazon started selling "Just Walk Out" technology to other retailers.[4] Since then, retailers have become increasingly interested in collecting and using customers' "biometric identifiers and information."[5] Generally, "biometrics" is used to refer to "measurable human biological and behavioral characteristics that can be used for identification, or the automated methods of recognizing an individual based on those

[†] Senior Staff Member, *St. John's Law Review*, J.D. 2023, St. John's University School of Law; B.S., 2019, Rensselaer Polytechnic Institute. A special thanks to Professor Jeff Sovern for his guidance in writing this Note. I am also extreemely thankful for my family, Chris, Kelly, Marie, and Rory. It is through their support that all of this is possible.

[1] Amazon, *Introducing Amazon Go and the World's Most Advanced Shopping Technology*, YOUTUBE (Dec. 5, 2016), https://www.youtube.com/watch?v=NrmMk1Myrxc [https://perma.cc/Q2WY-GDPL].

[2] *Id.*

[3] *Id.*

[4] Annie Palmer, *Amazon Brings Its 'Just Walk Out' Cashierless Checkout Tech to Whole Food Stores*, CNBC (Sept. 8, 2021, 12:23 PM), https://www.today.com/food/just-walk-out-amazon-brings-its-cashierless-tech-two-whole-t230385 [https://perma.cc/SU6H-XQ2M].

[5] *See* Kim Hart, *Facial Recognition Surges in Retail Stores*, AXIOS (July 19, 2021), https://www.axios.com/facial-recognition-retail-surge-c13fff8d-72c6-400f-b680-6ae2679955d4.html [https://perma.cc/JSJ8-H39Y]; Elizabeth B. Herrington & Gregory T. Fouts, *Beware of Biometrics: Complying with Illinois' Biometric Information Privacy Act*, MORGAN LEWIS: HEALTH L. SCAN BLOG (Nov. 19, 2021), https://www.morganlewis.com/blogs/healthlawscan/2021/11/beware-of-biometrics-complying-with-illinois-biometric-information-privacy-act [https://perma.cc/2W4W-VCQ7].

characteristics."[6] With the COVID-19 pandemic resulting in more contactless payment, the commercial use of biometric identifiers and information has grown exponentially.[7] As biometric technology is constantly evolving, so is its definition.[8]

Some examples of physical characteristics typically measured are: retina or iris scans, fingerprints, voiceprints, and scans or records of hand or face geometry.[9] Behavioral characteristics can include handwriting samples and signatures, voice recognition, and keyboard stroke and typing habits.[10] Data collected and recorded by measuring an individual's biological characteristics are known as "biometric identifiers."[11] Data derived and conclusions drawn from these biometric identifiers are known as "biometric information."[12]

The use of biometric identifiers and information is not uncommon: law enforcement has been collecting and using fingerprint information for over 100 years to aid investigations[13] and Delta Airlines uses facial recognition during check-in and boarding.[14] Additionally, many employers use a "biometric soft clock," which provides an alternative to the original punch clock by using a palm print, fingerprint, or face scan to track employee hours.[15] While most of the public accepts the collection and use of

---

[6] *See* Michael P. Daly et al., *Biometrics Litigation: An Evolving Landscape*, WESTLAW PRAC. L.: LITIG. (Apr. 2, 2018), https://www.westlaw.com/w-001-8264?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 [https://perma.cc/6NMA-B63Y]; *see also* Susan Gross Sholinsky & Peter A. Steinmeyer, *Expert Q&A on Biometrics in the Workplace: Recent Developments and Trends*, WESTLAW PRAC. L.: LAB. & EMP. (Feb. 15, 2018), https://www.westlaw.com/w-012-5864?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 [https://perma.cc/T5VV-6UUB].

[7] *See* Hart, *supra* note 5.

[8] *See* Daly, *supra* note 6.

[9] *Id.*

[10] Phil Ross, *Biometrics: A Developing Regulatory Landscape for a New Era of Technology*, ROBINSON & BRADSHAW (May 21, 2014), https://theprivacyreport.com/2014/05/21/biometrics-a-developing-regulatory-landscape-for-a-new-era-of-technology/.

[11] Daly, *supra* note 6.

[12] *Id.*

[13] April Glaser, *Biometrics Are Coming, Along with Serious Security Concerns*, WIRED (Mar. 9, 2016, 11:00 AM), https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/ [https://perma.cc/Y9FR-SBD6].

[14] *The Top 9 Common Uses of Biometrics in Everyday Life*, NEC N.Z. (July 07, 2020), https://www.nec.co.nz/market-leadership/publications-media/the-top-9-common-uses-of-biometrics-in-everyday-life/ [https://perma.cc/U478-ZQEC].

[15] Leonardo Sam Waterson, *10 Ways Biometric Technology Is Implemented in Today's Business World*, M2SYS (Nov. 29, 2018), http://www.m2sys.com/blog/biometrictechnology/10-ways-biometric-technology-implemented-business/

their personal data in the public safety and employment context, as this Note will demonstrate, there is reason to scrutinize biometric data's collection for commercial use.[16]

Part I of this Note explains how biometric identifiers and information are used in the commercial context. Part II examines the increased use, due to the COVID-19 pandemic, and the benefits and detriments of the use of biometric identifiers and information. Part III will analyze several state laws and New York City's recently enacted law concerning biometric identifiers' and information's commercial use. Part IV will examine the statutory provisions of Illinois's, Texas's, and Washington's biometric privacy acts ("BPA") and discuss their application. Part V will examine why state legislation is better suited to regulate biometrics compared to federal legislation. Finally, Part VI will advocate for state legislation constraining the use of biometric identifier information by commercial establishments with the optimal statutory construction based on caselaw, observations, and policy.

I. HOW BIOMETRIC TECHNOLOGY IS CURRENTLY USED

Recently, the use of biometric information has become common globally.[17] Biometric information allows companies to become more scalable and efficient; therefore, an array of industries have begun implementing this technology.[18] For example, Juniper Research Group predicted that biometrics will be used to authenticate over $3 trillion of payment transactions in 2025, up from $404 billion in 2020.[19] Notably, Chinese

---

[https://perma.cc/FY22-AD74]; *Biometric Time Clock*, ALLIED TIME USA, https://www.alliedtime.com/Biometric-Time-Clocks-s/1814.htm [https://perma.cc/6PD6-ZPKJ] (last visited Feb. 10, 2023).

[16] *See infra* Section II.B.

[17] *See, e.g.,* Alessandro Mascellino, *UK Plans $550M Budget for Government Digital Identity Update*, BIOMETRIC UPDATE (Sept. 13, 2021), https://www.biometricupdate.com/202109/uk-plans-550m-budget-for-government-digital-identity-update [https://perma.cc/Y7P7-QY6V]; Mariam Kiparoidze, *Russian Opposition Files Lawsuit Against Moscow's Use of Facial Recognition Tech*, .CODA (July 10, 2020), https://www.codastory.com/authoritarian-tech/facial-recognition-moscow/ [https://perma.cc/VZF7-D7MM].

[18] *9 Industries Biometrics Technology Could Transform*, CB INSIGHTS (Dec. 12, 2019), https://www.cbinsights.com/research/biometrics-transforming-industries/ [https://perma.cc/LK2Q-XT79].

[19] Press Release, Juniper Research, Biometrics to Secure over $3 Trillion in Mobile Payments by 2025; Driven by Shift to App-Based MCommerce (Feb. 1, 2021) [hereinafter Juniper Research], https://www.juniperresearch.com/press/biometrics-to-secure-over-3-trillion-in-mobile?ch=biometrics [https://perma.cc/H457-744V].

companies, such as SenseTime, continue to lead the world in developing biometric technology in the commercial sectors.[20]

With the growth of the global economy, borders offer fewer restrictions to the flow of information, technology, and goods.[21] Developments in the digital technology field, such as cloud computing, make issues like data privacy a global concern.[22] Thus, overseas innovation in the biometric information space may have profound effects in the United States.

A. Post-2010 Use of Biometrics Information

A notable example of commercial use of biometric identifier information took place in 2013, when Apple first introduced a fingerprint scanner on iPhones.[23] Since then, the market has exploded.[24] Apple now uses facial recognition and fingerprint technology to secure its devices,[25] Google uses voice recognition technology to limit the use of home assistants to authorized users,[26] and Samsung Pay relies on fingerprint and facial recognition to authenticate transactions.[27] These examples make intuitive sense because they promote security, privacy, and convenience. Naturally, banks were also among the largest early adapters of biometric technology.[28] While people with mobile banking apps are likely familiar with using their fingerprint or facial scan to access their account information, multiple banks have quietly been developing "Voice ID" by analyzing customers'

---

[20] Chris Burt, *SenseTime Sources Legal Opinion Suggesting Limits to US Sanctions Ahead of Planned IPO*, BIOMETRIC UPDATE (Sept. 29, 2021, 3:03 PM), https://www.biometricupdate.com/202109/sensetime-sources-legal-opinion-suggesting-limits-to-us-sanctions-ahead-of-planned-ipo [https://perma.cc/Y7P7-QY6V].

[21] *See generally* THOMAS L. FRIEDMAN, THE WORLD IS FLAT (2005) (discussing how technology encourages global advancements).

[22] *See* Edoardo Celeste & Federico Fabbrini, *Competing Jurisdictions: Data Privacy Across the Borders*, *in* DATA PRIVACY AND TRUST IN CLOUD COMPUTING 43, 44 (Theo Lynn et al. eds., 2021).

[23] Glaser, *supra* note 13.

[24] *Id.*

[25] *The Top 9 Common Uses of Biometrics in Everyday Life*, *supra* note 14.

[26] *See id*.

[27] Juniper Research, *supra* note 19.

[28] Jennifer A. Kingson, *Biometrics Invade Banking and Retail*, AXIOS (Feb. 18, 2020), https://www.axios.com/biometrics-banking-retail-privacy-5238b5f6-f825-4f22-9153-14fae247715e.html [https://perma.cc/E7V5-FDLX].

voices during calls.[29] This quiet development and implementation often goes unnoticed.[30]

B. Pandemic-Accelerated Use

During the COVID-19 pandemic, biometric technology took its "next evolutionary step."[31] By incorporating machine learning algorithms, biometric companies developed technologies in onder to identify people breaking lockdowns and trace close contacts.[32] The pandemic also drove the biometric industry toward contactless technologies, like facial recognition, and away from technologies that rely on contact—like fingerprint or palm scans.[33] In China, facial recognition operations were "retrofitted with new screening software to detect individuals who [were] not wearing protective masks."[34] During the 2021 Olympics, Japan used facial recognition to monitor the identity of spectators and ensure they were wearing facemasks.[35]

Domestic use of biometric information also accelerated during the pandemic. For example, the National Basketball Association ("NBA") required that players wear an "Oura" ring.[36] The ring monitored players' temperature, heart rate, and respiratory rate, calculated an "illness probability score," and alerted the league to anyone that may be in the presymptomatic phase of infection.[37] Additionally, Clear Secure, Inc., a biometric identity verification company, has partnered with several

---

[29] *See id.*; *Security as Unique as Your Voice*, CHASE, https://www.chase.com/personal/voice-biometrics [https://perma.cc/SB96-W2BE] (last visited Feb. 10, 2023).

[30] *See* Cheon Ho-sung, *"A Human Rights Disaster": S. Korean Civic Groups Demand Government Halt Creation of AI Facial ID and Tracking System*, HANKYOREH (Nov. 10, 2021), https://english.hani.co.kr/arti/english_edition/e_national/1018763.html [https://perma.cc/KYA7-V725]. The South Korean government secretly upgraded existing CCTV cameras to collect citizens biometric data and transferred 170 million facial photographs to private entities. *Id.*

[31] Stuart Carlaw, *Impact on Biometrics of Covid-19*, *in* ELSEVIER PUBLIC HEALTH EMERGENCY COLLECTION 8, 8 (2020).

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] Ayang Macdonald, *Japan Turns to Face Biometrics for Safe and Secure Olympics Amid COVID-19*, BIOMETRIC UPDATE (Mar. 22, 2021), https://www.biometricupdate.com/202103/japan-turns-to-face-biometrics-for-safe-and-secure-olympics-amid-covid-19 [https://perma.cc/W723-ZQQM].

[36] Ben Cohen, *Why Every NBA Player Is Getting a Ring*, WALL ST. J. (June 22, 2020, 6:04 AM), https://www.wsj.com/articles/nba-oura-ring-disney-bubble-11592809399 [https://perma.cc/E6N4-28TD].

[37] *Id.*

airlines and sports venues since the start of the pandemic.[38] Clear Secure uses facial scans and iris scans to verify an individual's identity, match the scan with the individual's health and vaccination records, and allow that individual to bypass the health screenings and general admission lines at airports.[39] These examples are indicative of the growth of the U.S. biometric market, which is projected to grow 14.8% every year over the next five years.[40]

II. BENEFITS AND DETRIMENTS OF BIOMETRIC TECHNOLOGY

Naturally, other sectors have observed the increased reliance on biometric data and have joined the biometric identifier and information space.[41] Currently, Albertsons,[42] Macy's, H.E.B. Grocery, and Apple Stores all collect biometric identifiers in their respective stores.[43] While the use of such identifiers and information can be beneficial, it also has several drawbacks.

A. Benefits of Commercial Biometric Use

Retailers primarily justify their use of biometrics by touting its effectiveness in the reduction of shoplifting.[44] Use of biometric identifiers enables retailers to identify previously recorded

---

[38] *See Where We Are*, CLEAR, https://www.clearme.com/where-we-are [https://perma.cc/GL8D-GX9W] (last visited Feb. 10, 2023).

[39] Martin Kaste, *There's an App That Help Prove Vax Status, but Experts Say Choose Wisely*, NPR (Nov. 17, 2021, 11:03 AM), https://www.npr.org/2021/11/15/1055936688/privacy-experts-vaccination-app-clear [https://perma.cc/N32H-3GRP].

[40] *Biometrics – Global Market Trajectory & Analytics*, GLOB. INDUS. ANALYSTS, INC. (July 2021), https://www.researchandmarkets.com/reports/5141259/ biometrics-global-market-trajectory-and?utm_source=GNOM&utm_medium=PressRelease&utm_code=g5nhg4&utm_campaign=1617240+-+Global+Biometrics+Market+Report+2021%3a+Market+to+Reach+%2444.1+Billion+by+2026+-+Increasing+Significance+of+Biometrics+Technology+in+Facilitating+Contactless+Passenger+Journey+Post-COVID-19+Pandemic&utm_exec=chdo54prd [https://perma.cc/QEV7-Z3SB]. The projected growth is largely due to increased demand for contactless technologies and the implementation of iris scans. *Id.*

[41] *See* Hart, *supra* note 5.

[42] Albertsons owns Acme, Safeway, and other regional chains. *See* ALBERTSONS COMPANIES, https://www.albertsonscompanies.com/ [https://perma.cc/R9YT-PZ2S] (last visited Feb. 10, 2023).

[43] *See Store Scorecard*, BAN FACIAL RECOGNITION IN STORES, https://www.banfacialrecognition.com/stores/#scorecard [https://perma.cc/HF8V-LNX3] (last visited Feb. 10, 2023).

[44] *How to Catch a Shoplifter: Retail Theft Prevention Is Real*, RECFACES (Jan. 11, 2021), https://recfaces.com/articles/how-to-catch-shoplifter [https://perma.cc/K9AE-44ZM].

shoplifters and alert security of their presence.[45] Biometric identifiers also offer more security than passwords or Personal Identification Numbers ("PIN") because they are linked to a user's tangible, real-world traits.[46] Unlike misappropriating someone's password, an imposter cannot access someone's account if they do not possess that person's face or fingerprint.[47] The use of biometric identifiers and information is also convenient and fast.[48] Scanning a fingerprint or a face takes only moments.[49] According to Mastercard, this convenience and ease of use has led 93% of their consumers to prefer biometrics over passwords.[50] Finally, many biometrics are immutable.[51] Since one's iris and fingerprints don't change, companies are able to continue using biometric identifier information with low maintenance.[52] Thus, businesses can collect an individual's information once and use it for their lifetime.[53]

B. Detriments of Commercial Biometric Use

Immutability, however, is a double-edged sword. Because some biometrics are immutable, once they are compromised, they are compromised forever.[54] Unlike social security numbers and PINs, biometric data cannot be easily changed.[55] Once an individual's biometric identifier has been compromised, through leak or sale, they have no control over where their biometrics are stored or what will happen to them in the future.[56] Suprema, one

---

[45] *Id.*

[46] *Advantages and Disadvantages of Biometrics*, MITEK SYS. (Mar. 15, 2021), https://www.miteksystems.com/blog/advantages-and-disadvantages-of-biometrics [https://perma.cc/C57T-TVVS].

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] *Biometric Recognition: Definition, Challenge and Opportunities of Biometric Recognition Systems*, IQUII (Mar. 8, 2018), https://medium.com/iquii/biometric-recognition-definition-challenge-and-opportunities-of-biometric-recognition-systems-d063c7b58209 [https://perma.cc/VQQ2-X5DY].

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] *See* Iris Wen, *Biometric Data Security: The Risks and Rewards*, JUMPSTART (Mar. 5, 2021), https://www.jumpstartmag.com/biometric-data-security-the-risks-and-rewards/ [https://perma.cc/8RTW-25ZJ].

[55] *Id.*

[56] *Id.*

of the fifty biggest security providers in the world,[57] suffered a breach to their "AEOS" system in 2019.[58] At the time, AEOS was used by over 5,700 organizations in 83 countries.[59] This breach exposed personal information of employees, unencrypted usernames and passwords, and fingerprints and facial scans to potential bad actors.[60] Accordingly, as the use of biometrics grows exponentially, so does the potential for fraud.[61]

One such example occured in May 2021 when a senior financial controller received a call from her boss instructing her to wire $243,000 to close out an account she had been working on.[62] However, much to her surprise, the person on the other end wasn't her boss, or another person at all: it was a deepfake of her boss's voice, created by artificial intelligence.[63] In the fingerprint context, a man created a method of etching fingerprints into gelatin that fooled fingerprint scanners eighty percent of the time.[64] Someone else was able to unlock an iPhone, two Android phones, a Samsung Galaxy S6, a LG Nexus 5X, and a Microsoft Surface tablet using Play-Doh replica of the owners' fingerprints.[65] The man even posted a video of how to recreate his process online.[66] While these are relatively primitive examples, they serve as a template for how compromised biometrics can be used to access information believed to be

---

[57] *See Who We Are*, SUPREMA, https://www.supremainc.com/en/about/suprema.asp [https://perma.cc/L73U-QBLP] (last visited Feb. 10, 2023).

[58] *Report: Data Breach in Biometric Security Platform Affecting Millions of Users*, VPNMENTOR (Aug. 14, 2019) [hereinafter *Data Breach in Biometric Security*], https://www.vpnmentor.com/blog/report-biostar2-leak/ [https://perma.cc/8EKE-LUXY]; Zak Doffman, *New Data Breach Has Exposed Millions of Fingerprint and Facial Recognition Records: Report*, FORBES (Aug. 14, 2019, 4:31 AM), https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/?sh=5779b13946c6 [https://perma.cc/LQR4-ZXFK].

[59] *Data Breach in Biometric Security*, *supra* note 58.

[60] *Id.*

[61] *Id.*

[62] Dominic David, *Analyzing the Rise of Deepfake Voice Technology*, FORBES (May 10, 2021, 8:00 AM), https://www.forbes.com/sites/forbestechcouncil/2021/05/10/analyzing-the-rise-of-deepfake-voice-technology/?sh=3ac8c8616915 [https://perma.cc/X3J2-9TP9].

[63] *Id.*

[64] John Leyden, *Gummi Bears Defeat Fingerprint Sensors*, REGISTER (May 16, 2002), https://www.theregister.com/2002/05/16/gummi_bears_defeat_fingerprint_sensors/ [https://perma.cc/H2ZV-DKPT].

[65] Jeff John Roberts, *This Guy Unlocked My iPhone with Play-Doh*, FORTUNE (Apr. 7, 2016, 11:55 AM), http://fortune.com/2016/04/07/guy-unlocked-iphone-play-doh/ [https://perma.cc/W88J-HVDV].

[66] *Id.*

secure. Thus, while security, ease of use, convenience, and reduction of theft are clearly desirable benefits, "like most of the exciting inventions [of] the 21st century, the key to truly maximizing the potential of biometric data is minimizing the risk of its misuse."[67]

The scope and prevalence of technology in the modern world has left consumers with no real choice but to accept company policies concerning the use of biometrics.[68] If an individual does not agree to a company's biometric collection terms, their only options are to not use that service or to find a substitute, which would likely be more expensive.[69] Furthermore, if similar policies are widespread in that market, then abstaining from the data collection is also abstaining from using that technology at all.[70] This is likely why ninety-one percent of Americans agree to "legal terms and services conditions without reading them."[71] Statutory obligations that deter collection of biometric information and severely penalize negligent retention are the only effective method for limiting citizens' exposure to the potentially devastating consequences of compromised biometric information.

III. CURRENT STATE EFFORTS TO CURB COMMERCIAL USE OF BIOMETRICS

Some states have already tried to control the commercial use of biometric identifier information within their borders, with varying success.[72] Illinois became the first state to enact a biometric privacy law, with the 2008 passage of the Biometric Information Privacy Act ("BIPA").[73]

---

[67] Wen, *supra* note 54.

[68] Eva-Marie Ghelardi, *Closing the Data Gap: Protecting Biometric Information Under the Biometric Information Privacy Act and the California Consumer Protection Act*, 94 ST. JOHN'S L. REV. 869, 881 (2021).

[69] *Id.*

[70] *Id.*

[71] Caroline Cakebread, *You're Not Alone, No One Reads Terms of Service Agreements*, BUS. INSIDER (Nov. 15, 2017, 7:30 AM), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 [https://perma.cc/DEQ6-SRJ4].

[72] *See e.g.*, 740 ILL. COMP. STAT. ANN. 14/1–99 (West 2008); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017); WASH. REV. CODE ANN. § 19.375.010 (West 2017).

[73] 740 ILL. COMP. STAT. ANN. 14/1 (West 2008).

A. Illinois's Biometric Information Privacy Act

BIPA was passed in response to the bankruptcy of Pay By Touch.[74] Pay By Touch was a biometrics firm that linked customer fingerprints to various financial accounts and allowed consumers to use these accounts by scanning their fingerprints.[75] After the firm declared bankruptcy and ceased operations, many people were concerned Pay By Touch would sell their biometric information as an asset during bankruptcy proceedings.[76] After noting that the use of biometrics was growing in the business sector and major corporations had opened pilot testing sites in Chicago, the Illinois legislature stated: "Biometrics are unlike other unique identifiers [like] social security numbers [and cannot] be changed."[77] Additionally, once biometric information has been compromised, "the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[78]

Moreover, the legislature concluded "[t]he full ramifications of biometric technology are not fully known," and "[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."[79] BIPA's requirements are examined in depth in Part IV, but generally BIPA requires that (1) an individual receive notice from the collecting entity, and give written consent for collection, storage, or distribution of biometric information, and (2) a company to provide a purpose and time span of collection, storage, or distribution of said biometric information.[80] BIPA restricts the collection of biometric identifiers and provides the public with the right to know what is done with their biometric information.[81] This lessens the risk that an individual's biometric information will be compromised and prevents the sale of biometric information in bankruptcy proceedings without consent. BIPA

---

[74] Justin O. Kay, *The Illinois Biometric Information Privacy Act*, ASS'N CORP. COUNS., https://www.acc.com/sites/default/files/2019-02/Drinker-Biddle-2017-1-BIPA-Article-2.pdf [https://perma.cc/JM76-K5M2].

[75] *Id.*

[76] Charles N. Insler, *Understanding the Biometric Information Privacy Act Litigation Explosion*, 106 ILL. BAR J. 34, 34–35 (2018).

[77] 740 ILL. COMP. STAT. ANN. 14/5 (West 2008).

[78] *Id.*

[79] *Id.*

[80] *See infra* Part IV; 740 ILL. COMP. STAT. ANN. 14/15 (West 2008).

[81] 740 ILL. COMP. STAT. ANN. 14/15 (West 2008).

has since become known as the "archetype example of a biometric privacy law" in the United States.[82]

B. Other States' Biometric Privacy Statutes

A few other states have passed biometric privacy statutes attempting to limit biometric use in commercial contexts.[83] Texas passed its BPA, Capture or Use of Biometric Identifier ("CUBI"), in 2009.[84] Generally, CUBI requires that consumers receive notice and give their consent before their biometric identifiers can be captured for a commercial purpose.[85] Additionally, Washington passed its BPA in 2017.[86] The Washington legislature based their bill on findings that increasing collection and marketing of citizen's biometric information without their consent or knowledge is an "increasing concern," and thus warranted legislation limiting the scope of this practice.[87] Washington's BPA requires that a consumer must be given notice, consent, or be provided with "a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose."[88] Texas's and Washington's statutes contain substantial differences from each other and BIPA, which significantly affect the protections afforded to their citizens, as discussed below.[89]

C. Generalized Privacy Laws in the United States

1. Arkansas's and New York's Statutes

Recently, many states have either enacted legislation that touches on biometric information or amended legislation concerning private information.[90] Arkansas passed the Personal

---

[82] Jane Bambauer, *Biometric Privacy Laws: How a Little-Known Illinois Law Made Facebook Illegal*, PROGRAM ON ECON. & PRIV., https://pep.gmu.edu/wp-content/uploads/sites/28/2017/06/Biometric-Privacy-Laws-FINAL_really_6.20-.pdf [https://perma.cc/R3LY-QD39] (last visited Feb. 10, 2023).

[83] *See* statutes cited, *supra* note 72.

[84] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017).

[85] *Id.*

[86] *See* WASH. REV. CODE ANN. § 19.375 (West 2017).

[87] *Id.* § 19.375.900.

[88] *Id.* § 19.375.020.

[89] *See infra* Part IV.

[90] *See CUBI: Everything You Need to Know About Texas' Biometric Law and Beyond*, SEGAL MCCAMBRIDGE (Jan. 28, 2021), https://www.segalmccambridge.com/blog/cubi-everything-you-need-to-know-about-texas-biometric-law-and-beyond/ [https://perma.cc/PQ7R-HACH].

Information Protection Act ("PIPA"), which became effective in 2019.[91] New York also passed the Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act") in 2019.[92] However, these statutes are little more than "breach notification" statutes.[93] The statutes require that once previously collected and stored biometric information is compromised, the entity that suffered the breach must provide notice to the effected individuals.[94] Neither statute provides a private right of action and both allow enforcement only by the state's Attorney General.[95] Furthermore, both Arkansas and New York identify biometric information as a subset of personal information.[96] The statutes also classify social security numbers as personal information and outline *reasonable* precautions that must be taken to protect this personal information.[97] Thus, the *reasonable* precautions requirements necessary to protect social security numbers are the same standards that are applied to biometric information.[98] Despite other legislatures deciding biometric information poses a greater risk to the public if compromised, Arkansas's and New York's current statutes require only the same industry standards necessary to protect social security numbers as they do to protect the public's biometric information.[99]

2. California Consumer Privacy Act

California first passed the California Consumer Privacy Act ("CCPA") in 2018.[100] Like the SHIELD Act and PIPA, the CCPA protected biometric information under the umbrella term "personal information."[101] The CCPA was likely modeled after

---

[91] ARK. CODE ANN. §§ 4-110-10, 1-4-110-108 (West 2019).

[92] N.Y. GEN. BUS. LAW § 899-aa (McKinney 2019).

[93] *See* Angela K. Dinh, *Breach Notification Rule: Where Are We?*, 13 J. HEALTH CARE COMPLIANCE 43, 43–44 (2011); Mary T. Costigan et al., *New York SHIELD Act FAQs*, NAT'L L. REV. (Mar. 11, 2020), https://www.natlawreview.com/article/new-york-shield-act-faqs [https://perma.cc/J9EY-P6MX].

[94] *See* ARK. CODE ANN. § 4-110-103; N.Y. GEN. BUS. § 899-aa.

[95] *See* ARK. CODE ANN. § 4-110-108; N.Y. GEN. BUS. § 899-aa.

[96] The relevant terminology is "personal information" in Arkansas and "private information" in New York. *See* ARK. CODE ANN. § 4-110-103; N.Y. GEN. BUS. § 899-aa. For simplicity, I will refer to both as "personal information."

[97] *See* statutes cited *supra* note 94.

[98] *See* statutes cited *supra* note 94.

[99] *See* statutes cited *supra* note 94.

[100] CAL. CIV. CODE § 1798.130 (West 2022).

[101] N.Y. GEN. BUS. LAW § 899-aa (McKinney 2019); ARK. CODE § 4-110-103 (West 2019); CAL. CIV. CODE § 1798.130.

the European Union's General Data Protection Regulation ("GDPR"),[102] because the CCPA includes the Consumer Right to Delete, Consumer Opt-Out from Sale of Personal Information, Consumer Opt-In for the Sale of Personal Information of Minors, and Non-Discrimination for Exercise of Consumer Rights, like the GDPR does.[103] However, all of these rights can only be exercised after biometric data was collected.[104]

In November 2020, Californians voted to pass Proposition 24, which absorbs and expands the CCPA.[105] Proposition 24 enacts the California Privacy Rights Act ("CPRA"), which creates a new subcategory of personal information—"sensitive personal information."[106] This new subcategory includes biometric data, duties, and restrictions specific to sensitive personal information.[107] CPRA also includes a private right of action, but only when a company fails to implement and maintain "reasonable security procedures and practices" and as a consequence of those failures, the "personal information" is compromised.[108] In other words, unlike BIPA, if a company fails to comply with the statute, it is not subject to penalties until the information is already compromised.[109]

The CPRA also creates the California Privacy Protection Agency ("CPPA"), an enforcement agency that prosecutes violations of the CPRA.[110] However, violations of the CPRA are still punishable only at the CPPA's or the Attorney General's

---

[102] Danny Palmer, *What Is GDPR? Everything You Need to Know About the New General Data Protection Regulations*, ZDNET (May 17, 2019), https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/ [https://perma.cc/F296-JCLG].

[103] *Compare* CAL. CIV. CODE § 1798.130, *with* Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 9(1), 2016 O.J. (L 119) 38 (EU) [hereinafter GDPR].

[104] *See* CAL. CIV. CODE § 1798.130.

[105] Matthew A. Diaz & Kurt R. Hunt, *California Approves the CPRA, a Major Shift in U.S. Privacy Regulation*, NAT'L L. REV. (Nov. 17, 2020), https://www.natlawreview.com/article/california-approves-cpra-major-shift-us-privacy-regulation [https://perma.cc/Y58E-79EE].

[106] *California Proposition 24*, CAL., https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf [https://perma.cc/2HP4-8739] (last visited Aug. 3, 2023).

[107] *Id.*

[108] *Id.*

[109] *Id.* The state can bring charges for bare violations of the statutory obligations. *Id.*

[110] *Id.*

discretion.[111] As commentators point out, these actions will cost prosecutors "substantial amounts of money and time."[112] Therefore, actions will likely only be brought against large companies that would be able to pay large damage awards.[113] A 2019 survey found that the majority of businesses impacted by California's privacy laws would not be prepared to comply by the effective date.[114] Many businesses were intentionally waiting to see how California's laws would be enforced before weighing "the cost of compliance against the risk and cost of being fined."[115] Furthermore, all "administrative fine[s] assessed" and "the proceeds of any settlement" received pursuant to the CPRA, are to be deposited in a fund "with the intent to fully offset any costs incurred by the state courts, . . . the Attorney General, and the [CPPA]."[116]

These generalized privacy statutes are inadequate to provide the protection biometric identifiers and information deserve. In fact, the committees for Texas and Washington found as much when drafts of their respective bills were analyzed.[117] Generalized privacy statutes do nothing to proactively prevent collection and sale, and instead, only react *post hoc*, failing to adequately compensate individuals whose information has been compromised.[118] Additionally, standing to sue in federal court

---

[111] *Id.*

[112] Ghelardi, *supra* note 68, at 891.

[113] *Id.* California's Attorney General brought their first action under CCPA on August 24, 2022 against Sephora for selling consumer information without consumer consent. Andrea Vittorio, *First California Privacy Penalty Flags Consumer Data Sales Peril*, BLOOMBERG L. (Aug. 26, 2022, 5:15 AM), https://news.bloomberglaw.com/privacy-and-data-security/first-california-privacy-penalty-flags-consumer-data-sales-peril [https://perma.cc/5J69-JG2N]. California fined Sephora $1.2 million for their breach. *Id.*

[114] April Berthene, *Majority of Businesses Are Unprepared for California Privacy Act*, DIGIT. COM. 360 (Aug. 26, 2019), https://www.digitalcommerce360.com/2019/08/26/majority-of-businesses-are-unprepared-for-california-privacy-act/ [https://perma.cc/7JZN-FMQX]. The enforcement of the CPRA will begin on July 1, 2023, and will only apply to violations happening on or after July 1, 2023. *CCPA vs CPRA: What's the Difference?*, BLOOMBERG L., https://pro.bloomberglaw.com/brief/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/#:~:text=When%20will%20enforcement%20of%20the,and%20enforceable%20until%20that%20date [https://perma.cc/DY5E-DDM8] (Jan. 23, 2023).

[115] *Id.*

[116] *California Proposition 24*, *supra* note 106, § 17, 1798.1555(b) (emphases omitted).

[117] *See* H.B. 3186-81R30472, 81st Reg. Sess., at 1 (Tex. 2009); H.B. 1493-1807.1, 65th Reg. Sess., at 2 (Wash. 2017).

[118] *See* ARK. CODE ANN. § 4-110-103 (West 2019); N.Y. GEN. BUS. LAW § 899-aa (McKinney 2019); CAL. CIV. CODE ANN. § 1798.150 (West 2022).

under these statutes' private right of action is now in question following the Supreme Court's decision in *TransUnion v. Ramirez*.[119] Thus, a narrower statute adressing the commercial use of biometric identifier and information is needed to adequately protect consumer's privacy. This Note will attempt to develop such a statute in the following sections.

IV. CURRENT STATUTORY PROVISIONS

Each current statute has the same basic framework.[120] They first define what constitutes a biometric identifier, then provide what a business must do in order to legally collect biometric identifiers.[121] Next, the statutes outline what a business can do with the biometrics it has collected and when a business must destroy the information.[122] Finally, each statute specifies who or what has a right to enforce the provision.[123] Each statute also has different exceptions and carveouts as the legislature deemed necessary.[124]

A. Defining "Biometric Identifier"

BIPA, the "archetyp[al] example"[125] of biometric information privacy statutes, defines "biometric identifier" as: "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[126] BIPA then expressly excludes "writing samples, written signatures, photographs, . . . demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color."[127] BIPA limits the covered biometric identifiers to the enumerated categories, containing no "catch-all" provision.[128]

---

[119] TransUnion LLC v. Ramirez, 141 S. Ct. 2190 (2021).

[120] *See* 740 ILL. COMP. STAT. ANN. 14/1 (West 2008); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017); WASH. REV. CODE ANN. § 19.375 (West 2017).

[121] *See* ILL. COMP. STAT. ANN. 14/1; TEX. BUS. & COM. CODE ANN. § 503.001; WASH. REV. CODE ANN. § 19.375.

[122] *See* ILL. COMP. STAT. ANN. 14/1; TEX. BUS. & COM. CODE ANN. § 503.001; WASH. REV. CODE ANN. § 19.375.

[123] *See* ILL. COMP. STAT. ANN. 14/1; TEX. BUS. & COM. CODE ANN. § 503.001; WASH. REV. CODE ANN. § 19.375.

[124] *See* ILL. COMP. STAT. ANN. 14/1; TEX. BUS. & COM. CODE ANN. § 503.001; WASH. REV. CODE ANN. § 19.375.

[125] Bambauer, *supra* note 82.

[126] ILL. COMP. STAT. ANN. 14/10.

[127] *Id.*

[128] *Id.*

CUBI defines biometric identifier nearly identically, limiting it to "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[129] However, CUBI provides neither explicit exclusions nor a "catch-all" provision.[130] Thus, it is likely a court would find only the categories listed, and nothing else, are covered by both BIPA and CUBI.[131]

Washington's statute differs, however, and defines "biometric identifier" as "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."[132] It then excludes "a physical or digital photograph, video or audio recording or data generated therefrom."[133] Notably, Washington's definition does not include facial geometry.[134] This is most likely in response to the facial geometry provision of BIPA becoming the subject of multiple lawsuits against Google,[135] Shutterfly,[136] and Facebook.[137] Each suit was based on the same basic premise: the company violated BIPA when it used an algorithm to scann the facial geometry in uploaded pictures and created and stored a template—a practice known as "scraping".[138] Many businesses, however, see scraping as instrumental to their growth and ability to innovate.[139] Thus,

---

[129] TEX. BUS. & COM. CODE ANN. § 503.001.

[130] *Id.*

[131] *See* Lindh v. Murphy, 521 U.S. 320, 330 (1997) (describing *expressio unius* and the "negative implications raised by disparate provisions"); Tamara Larre, *Misguided Inferences? The Use of Expressio Unius to Interpret Tax Law*, 51 ALTA. L. REV. 497, 500 (2014) (defining *expressio unius*).

[132] WASH. REV. CODE ANN. § 19.375.010 (West 2017).

[133] *Id.*

[134] *Id*.

[135] Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1092 (N.D. Ill. 2017).

[136] *See generally* Norberg v. Shutterfly, Inc., 152 F. Supp. 3d. 1103 (N.D. Ill. 2015) (finding a valid claim when defendant violated BIPA by storing and using millions of individuals' face geometry).

[137] *See generally In re* Facebook Biometric Info. Priv. Litig., 326 F.R.D. 535 (N.D. Cal. 2018) (certifying a claim Facebook collected and stored biometric data in violation of BIPA).

[138] *See Rivera*, 238 F. Supp. 3d at 1090–91; *Norberg*, 152 F. Supp. 3d. at 1104; *In re Facebook Biometric*, 326 F.R.D. at 541.

[139] Adan Janofsky, *Business Groups Push Back Against Proposed Facial-Recognition Bans,* WALL ST. J. (Oct. 30, 2019), https://www.wsj.com/articles/business-groups-push-back-against-proposed-facial-recognition-bans-11572427801 [https://perma.cc/2L6L-99AX]; *see also Coalition Letter on Facial Recognition Technology*, U.S. CHAMBER OF COM. (Oct. 16, 2019), https://www.uschamber.com/letters-congress/coalition-letter-facial-recognition-technology [https://perma.cc/3C92-82HP].

balancing individual's rights with the progress and innovation of business is a central concern when even defining "biometric identifiers."[140]

B. Collection, Notice, and Consent

BIPA provides that no business,

> may collect, capture, purchase, receive through trade, or otherwise obtain a person's [biometric identifier], unless it first: (1) informs the subject . . . in writing that a biometric identifier . . . is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier . . . is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information . . . .[141]

In other words, both notice and consent are required before a consumer's biometric identifier is collected.[142] Texas's CUBI also requires both notice and consent before the collection of one's biometric identifier.[143] Notice and consent are essential to protecting biometric identifier information because it prompts a person to pause and appreciate that they are consenting to their fingerprints and facial scans being collected, analyzed, and sold.[144]

Washington's statute, however, provides "[a] person may not [collect] a biometric identifier in a database for a commercial purpose, without first providing notice, obtaining consent, *or* providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose."[145] The statute continues to specify that the information cannot be used or sold without consent.[146] Thus, a company may be able to collect this information by simply providing notice through a click-wrap provision or boilerplate disclosure consumers may not see.[147] While the collecting company cannot actively sell this

---

[140] Janofsky, *supra* note 139.

[141] 740 ILL. COMP. STAT. ANN. 14/15 (West 2008).

[142] *See id.*

[143] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017).

[144] Claire Park, *How "Notice and Consent" Fails to Protect Our Privacy*, NEW AM. (Mar. 23, 2020), https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/ [https://perma.cc/MY3Z-GD2E].

[145] WASH. REV. CODE ANN. § 19.375.020 (West 2017) (emphasis added).

[146] *Id.*

[147] *See id.*

information without consent, it still leaves the collected data vulnerable to breaches and leaks while the collecting company continues to use it in providing the services originally disclosed.[148] Notice or consent alone fails to adequately protect consumer privacy.

C. Retention

BIPA requires that a company that has collected biometric information promulgate a written policy "establishing a retention schedule and guidelines for permanently destroying biometric identifiers and . . . information."[149] Neither Texas nor Washington included similar public written disclosure requirements.[150]

Under BIPA, a company must permanently destroy collected biometric information after the initial purpose for collecting the information has been satisfied or within three years of the individual's last interaction with the business, whichever happens first.[151] Similarly, CUBI requires that collected information be destroyed within a "reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires."[152] The Washington BPA provides that a business "[m]ay retain the biometric identifier no longer than is reasonably necessary to . . . [p]rovide the services for which the biometric identifier was [collected]."[153]

BIPA contains the superior provision with respect to retention because it gives the clearest requirements for what is acceptable. Moreover, the public disclosure of a written policy substantially increases public awareness, so the public, and watchdogs, know exactly what the information is being used for.[154]

---

[148] *See id.*

[149] 740 ILL. COMP. STAT. ANN. 14/15 (West 2008).

[150] *See* TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017); WASH. REV. CODE § 19.375.020.

[151] ILL. COMP. STAT. ANN. 14/15.

[152] TEX. BUS. & COM. CODE ANN. § 503.001.

[153] WASH. REV. CODE ANN. § 19.375.020.

[154] While the vast majority of the public likely will not read the policy, there will be people that read the fine print and publicize that for others. Matthew S. Schwartz, *When Not Reading the Fine Print Can Cost Your Soul*, NPR (Mar. 8, 2019, 9:55 AM), https://www.npr.org/2019/03/08/701417140/when-not-reading-the-fine-print-can-cost-your-soul [https://perma.cc/R43D-JUHS].

The requirement of destruction after the transaction or three years after the last interaction is the most important requirement because it provides a concrete end date. To date, there has been no judicial decision interpreting what a "reasonable time" is with respect to a BPA. Because there has been no case law, the "reasonable time" provisions in the Washington and Texas statutes are ripe for abuse as collectors will claim all use constitutes "reasonable time."

D. Use

BIPA states that no business "in possession of a biometric identifier . . . may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information."[155] Additionally, no business that possesses biometric identifiers "may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless . . . the subject . . . consents to the disclosure or redisclosure [or] the disclosure or redisclosure completes a financial transaction requested or authorized by the [same] subject."[156] The two provisions try to balance personal privacy with business interests by removing incentives to profit from disclosing biometric data, but also allowing biometric data to be shared between platforms if this exchange is consented to.[157] Permitting transfer with consent allows for a better user experience because it enables businesses to cooperate with other entities to reduce operating costs while restraining the potentially limitless transfer of sensitive information.

CUBI forbids sale, lease, or other disclosure unless "the individual consents to the disclosure for identification purposes in the event of the individual's disappearance or death," or "the disclosure completes a financial transaction that the individual requested or authorized."[158] Outside of these limited circumstances, a business cannot disclose or profit from the collected information.[159] Washington's BPA, on the other hand,

---

[155] ILL. COMP. STAT. ANN. 14/15.

[156] *Id.*

[157] *See* Phil Chang, *The Biometrics Balancing Act: Privacy with Security*, GRANTEK (Sept. 6, 2019), https://grantek.com/the-biometrics-balancing-act-privacy-with-security/ [https://perma.cc/DA3V-KSW4].

[158] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017).

[159] *See id.*

allows for sale, lease, or other disclosures with consent.[160] It also allows for disclosure without consent if the biometric data is "necessary to provide a product or service subscribed to, requested, or expressly authorized by the individual."[161] Furthermore, disclosure without consent is permissible if disclosure is "necessary to effect, administer, enforce, or complete a financial transaction that the individual requested, initiated, or authorized, and the third party to whom the biometric identifier is disclosed maintains confidentiality of the biometric identifier and does not further disclose the biometric identifier."[162] Finally, disclosure without consent is allowed if it is made "to a third party who contractually promises that the biometric identifier will not be further disclosed and will not be enrolled in a database for a commercial purpose inconsistent with the notice and consent described in this [statute]."[163]

In 2018, Google launched its "Art Selfie" feature, that scanned an uploaded selfie and matched it to the face of a painting in a museum.[164] This feature launched in every state except Texas and Illinois.[165] Google cited the BPA in Texas and Illinois as the reason the feature wasn't launched there.[166] Interestingly, the feature was launched in Washington; Google did not deem their feature to be within the scope of Washington's BPA.[167]

E. Right of Action

BIPA is the only statute that provides a private right of action.[168] CUBI and Washington's BPA only allow for action from the state's Attorney General.[169] Consequently, BIPA has been a

---

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

[161] *Id.*

[162] *Id.*

[163] *Id.*

[164] Alix Langone, *You Can't Use Google's New Selfie Art App in These States*, TIME (Jan. 17, 2018, 5:05 PM), https://time.com/5106798/google-selfie-app-not-work-states/ [https://perma.cc/9AFW-WM6V].

[165] *Id.*

[166] *Id.*

[167] *Id.*

[168] 740 ILL. COMP. STAT. ANN. 14/20 (West 2008).

[169] *See* TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017); WASH. REV. CODE ANN. § 19.375.030 (West 2017). Both CUBI and Washington's BPA drafts included a private right of action, which was removed from later versions. *See* H.B. 3186, 81st Reg. Sess., at 1 (Tex. 2009); H.B. 1493, 65th Reg. Sess., at 4 (Wash. 2017).

"hotbed" for litigation,[170] while Texas and Washington have yet to see a judicial decision concerning their statute.

BIPA states "[a]ny person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party."[171] A prevailing party may recover for each violation: liquidated damages of $1,000 or actual damages, whichever is greater for a negligent violation; liquidated damages of $5,000 or actual damages, whichever is greater, for an intentional or reckless violation; reasonable attorneys' fees and costs; and other relief as deemed appropriate.[172] Federal courts have found that a statutory violation of BIPA meets the requirements of Article III standing.[173] In *Fox v. Dakkota Integrated Systems, LLC*, the Seventh Circuit analogized BIPA to the common law tort claim for invasion of privacy.[174] Since suits of this nature typically only make financial sense in a class-action context, most suits wind up in federal court.[175] Thus, the private right of action provides stronger incentive to adhere to the law because of potentially costly consequences of class actions.

F. Exceptions

BIPA, CUBI, and Washington's BPA all provide exceptions that exclude state or local government agencies from liability and also provide carveouts for information for medical purposes.[176]

---

[170] Joseph Lazzarotti, *New York Could Become the Next Hotbed of Class Action Litigation over Biometric Privacy*, JD SUPRA (Jan. 15, 2021), https://www.jdsupra.com/legalnews/new-york-could-become-the-next-hotbed-7531919/ [https://perma.cc/9YYH-8PGH].

[171] ILL. COMP. STAT. ANN. 14/20.

[172] *Id.*

[173] Fox v. Dakkota Integrated Sys., LLC, 980 F.3d 1146, 1153 (7th Cir. 2020) (collecting cases); King v. PeopleNet Corp., No. 21-CV-2774, 2021 WL 5006692, at *4–5 (N.D. Ill. Oct. 28, 2021) (holding that *Fox* is still good law despite *TransUnion*).

[174] *Fox*, 980 F.3d at 1154; *see also* discussion of *TransUnion*, *infra* Section IV.C.

[175] The costs of litigation are often not worth the reward when relatively small statutory damages are recoverable. Margaret M. Zwisler et al., *Overview of Class/Collective Actions and Current Trends*, JD SUPRA (Oct. 7, 2015), https://www.jdsupra.com/legalnews/the-class-actions-global-guide-us-39642/ [https://perma.cc/N3KM-MA73]. These suits wind up in federal court because since the passage of the Class Action Fairness Act, most class action suits meet the requirements for federal jurisdiction (amount in controversy exceeds $5 million and minimum diversity). *Id.*

[176] ILL. COMP. STAT. ANN. 14/25; TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017); WASH. REV. CODE ANN. § 19.375.040 (West 2017). These exceptions are designed to avoid preemption concerns and facilitate the free flow of information in these vital sectors. *See* H.B. 3186, 81st Reg. Sess., at 1 (Tex. 2009).

However, CUBI's 2017 amendment specifically excluded voiceprint collection by financial institutions.[177] While this marginally weakens the statute's protections, it pales in comparison to the "security purpose" exception of Washington's BPA.[178] Washington's BPA provides that "[n]othing in this section requires an entity to provide notice and obtain consent to collect, capture, or enroll a biometric identifier and store it in a biometric system, or otherwise, in furtherance of a security purpose."[179] The statute defines "security purpose" as "the purpose of preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value, including tangible and intangible goods, services, and other purposes in furtherance of protecting the security or integrity of software, accounts, applications, online services, or any person."[180] The security purpose exception is so broad that once an entity collects the biometric information "in furtherance of a security purpose," the statute is inapplicable.[181] Once the information is collected and stored, it is subject to the risk of breach.

V. WHY STATE LEGISLATION IS APPROPRIATE

"It has become commonplace to assert that 'technology outpaces law' and that regulation therefore lags behind, and may indeed be futile if it does not adapt to changing technology-led circumstances."[182] To avoid lagging behind biometric technology and suffering consequences, preemptive legislation is needed before biometric collection progresses beyond legislative control.

A. Attempts to Enact Federal Legislation Have Failed

Despite multiple enacted state laws and bipartisan support for multiple federal bills, no federal biometric legislation exists. In March 2019, Senator Roy Blunt introduced the Commercial Facial Recognition Privacy Act of 2019.[183] The bill was read twice and referred to the Committee on Commerce, Science, and

---

[177] TEX. BUS. & COM. CODE ANN. § 503.001.

[178] WASH. REV. CODE ANN. § 19.375.020(7).

[179] *Id.*

[180] WASH. REV. CODE ANN. § 19.375.010(8).

[181] WASH. REV. CODE ANN. § 19.375.020(7).

[182] Charles Raab & Ivan Szekely, *Data Protection Authorities and Information Technology*, 33 COMPUT. L. & SEC. REV. 421, 423 (2017).

[183] S. 847, 116th Cong. § 1 (2019).

Transportation.[184] Nine industry groups responded by sending a letter in October 2019 to over a dozen House and Senate lawmakers urging them to vote against "strict[er] limits on the use of facial-recognition technology."[185] The letter touted facial recognitions enhancement of customer experience, security operations, and efficiency while warning regulation would hamper innovation.[186] The bill died in the 116th Congress.[187]

In August 2020, Senator Jeff Merkley introduced the National Biometric Information Privacy Act of 2020.[188] The requirements were similar to BIPA and provided a private cause of action.[189] However, the bill was referred to the Committee on the Judiciary and died in the 116th Congress.[190] The industry letter and Congress's actions regarding both proposed laws evince that industry resistance likely prohibits the adoption of federal legislation in the near future. This might not be a bad thing.

B. Why State Legislation is Better Suited to Regulate Biometrics

In the context of biometric protection, gradual state implementation is superior to sweeping federal legislation. State legislators can tailor the scope of their bills to best meet the needs of their constituents and businesses operating within the state borders.[191] This may explain why only four percent of bills introduced in Congress pass in comparison to the twenty-five percent of bills introduced in the state legislatures.[192] Given the rapidly changing landscape of biometrics and the immutable

---

[184] *Id.*

[185] Janofsky, *supra* note 139.

[186] *Id.*

[187] *S. 847 (116th): Commercial Facial Recognition Privacy Act of 2019*, GOVTRACK, https://www.govtrack.us/congress/bills/116/s847 [https://perma.cc/E9UU-9SXR] (last visited Feb. 12, 2023).

[188] S. 4400, 116th Cong. § 1 (2020).

[189] Molly Arranz, *A National Biometric Privacy Law? Laws Protecting "Biometric" Identifiers Continue to Cut a Blazing Trail*, JD SUPRA (Aug. 19, 2020), https://www.jdsupra.com/legalnews/a-national-biometric-privacy-law-laws-80763/ [https://perma.cc/256J-LS3Y].

[190] *S. 4400 (116th): National Biometric Information Privacy Act of 2020*, GOVTRACK, https://www.govtrack.us/congress/bills/116/s4400 [https://perma.cc/8TL8-E6D6] (last visited Feb. 12, 2023).

[191] Daniel C. Vock, *State Labs: Congress Can Learn a Lot from State Legislatures.*, GOVERNING (Aug. 19, 2019), https://www.governing.com/topics/politics/gov-state-labs.html [https://perma.cc/3XW3-KMH6].

[192] *Id.*

characteristics at risk, it is imperative that states quickly enact laws to curb the potentially devastating consequences.[193]

Moreover, passing state laws before federal laws would allow the states to act as laboratories of democracy.[194] This allows the federal and other state law makers to see how the laws are implemented and enforced by different states.[195] Watching implementation and interpretation allows law makers to observe and learn from others' efforts to craft the optimal statutory scheme.

Additionally, it would allow businesses to test the limits of the law on a smaller scale. Instead of implementing sweeping change, there would be a time and place to see how the new duties play out, like Amazon did by introducing the "Just Walk Out" technology in only a handful of stores.[196] Businesses may argue that developing and implementing policies to comply with different laws in many states will be too expensive; however, this argument holds less weight in the privacy context.[197] For example, the initial costs estimated for businesses to comply with the CCPA were likely exaggerated because large businesses were already forced to develop and implement similar policies to comply with the GDPR in Europe.[198] The same will be true with state-by-state biometric privacy laws. The policies that companies developed to comply with state biometric privacy laws can be tweaked to comply with new statutes modeled after existing biometric privacy laws. Therefore, new state laws will not be cost-prohibitive.

---

[193] *See* Paul Bischoff, *Biometric Data: 96 Countries Ranked by How They're Collecting It and What They're Doing With It*, COMPARITECH (Jan. 27, 2021), https://www.comparitech.com/blog/vpn-privacy/biometric-data-study/ [https://perma.cc/4ZCH-62X6].

[194] New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("[A] single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

[195] For a great discussion on "gaps" left in BIPA and CCPA, see Ghelardi, *supra* note 68, at 885–89.

[196] Palmer, *supra* note 4.

[197] *See* Ghelardi, *supra* note 68, at 885.

[198] *See* Lauren Feiner, *California's New Privacy Law Could Cost Companies a Total of $55 Billion to Get in Compliance*, CNBC (Oct. 8, 2019, 10:38 AM), https://www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion.html [https://perma.cc/3PCN-8GEX]. Large companies are likely to be the initial target of enforcement, which places the burden of developing and implementing compliant policies on the party most able to bear the extra cost. *See supra* Section III.C.2.

C. *Why Current Legislation Fails*

The New York SHIELD Act and other breach-notification statutes are insufficient because they do not restrain the collection or sale of biometric identifiers.[199] Breach-notification statutes may be particularly ineffective now given the *TransUnion LLC v. Ramirez* ruling's effect on standing, where the Supreme Court held that inaccurate information in a consumer's credit file did not qualify as a concrete harm.[200] Furthermore, the Court stated "the mere risk of future harm, standing alone, cannot qualify as a concrete harm—at least unless the exposure to the risk of future harm itself causes a separate concrete harm."[201] The Court clarified:

> If the risk of future harm materializes and the individual suffers a concrete harm, then the harm itself, and not the pre-existing risk, will constitute a basis for the person's injury and for damages. If the risk of future harm does *not* materialize, then the individual cannot establish a concrete harm sufficient for standing . . . .[202]

Therefore, it is unclear whether a breach that exposes personal information, where no identity theft has yet happened, is sufficient to create an injury-in-fact.[203] Because of this uncertainty, the only way to sufficiently protect the public is to limit the collection of biometric information as much as reasonably practicable, taking into account the benefits and interests of technological innovation.

VI. THE LAW NEW YORK SHOULD PASS

New York is a center for commercial activity and because of this, it requires stringent regulations on commercial collection of biometric information. New York is also extremely diverse, and facial recognition technology is prone to misidentifying people of

---

[199] *Supra* Section III.C.1.

[200] *See* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2200 (2021). Concrete harm is a requirement for Article III standing. *Id.* at 2203.

[201] *Id.* at 2210–11 (emphasis omitted).

[202] *Id.* at 2211.

[203] *See* Griffey v. Magellan Health Inc., 563 F. Supp. 3d 34, 43 (D. Ariz. 2021) ("[T]he United States Supreme Court has recently recognized that 'disclosure of private information' is one of many '[v]arious intangible harms' that satisfy Article III standing. Thus, the Court finds these allegations sufficient for the purposes of the standing inquiry." (second alteration in original) (citation omitted) (quoting *TransUnion LLC*, 141 S. Ct. at 2204)).

color.[204] Thus, proactive legislation is needed before the consequences are felt. BIPA, CUBI, and Washington's BPA all seek to prevent abuses and unanticipated consequences.[205] To sufficiently protect its citizens' information, New York needs to implement a law that contains a definition of biometric information similar to Washington's, and retention, use, and consent requirements like BIPA. Most importantly, the statute should contain a private right of action.

A. Preamble

To preempt standing challenges, New York should explicitly set out that a person's biometric information is their property and thus, a person has a property right to their biometric information. Creating a property right would allow for easier interpretation by courts by providing a vast common-law background from which they could draw.[206] Furthermore, classifying biometric information as a type of property would dispel any standing issues about concrete harm. Courts would no longer have to justify standing by analogizing to the common law tort of invasion of privacy.[207] Biometric information is a valuable resource that is now being collected and sold by businesses.[208]

---

[204] *See* MITEK SYS., *supra* note 46; *see also* Alex Najibi, *Racial Discrimination in Face Recognition Technology*, HARV. SCI. POL'Y & SOC. JUST. BLOG (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/ [https://perma.cc/5MGF-B4BS].

[205] 740 ILL. COMP. STAT. ANN. 14/5 (West 2008) ("The full ramifications of biometric technology are not fully known."); WASH. REV. CODE § 19.375.900 (2017) ("The collection and marketing of biometric information about individuals . . . is of increasing concern."); H.B. 3186-81R30472, 81st Reg. Sess., at 1 (Tex. 2009) ("There are concerns that biometric data . . . is increasingly becoming a target of identity theft and needs to be safeguarded to protect individual privacy and prevent economic harm to both individuals and businesses.").

[206] Ghelardi, *supra* note 68, at 880, 885. ("While courts have traditionally been reluctant to expand property rights to human bodies . . . . In the modern world, biometric information is an alienable resource that individuals can use to facilitate their lives.") (citing Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1206 (Ill. 2019)).

[207] Fox v. Dakkota Integrated Sys., LLC, 980 F.3d 1146, 1153 (7th Cir. 2020). As an alternative, Massachusetts created a Privacy Bill of Rights and specified that any violation of the bill constitutes an injury in fact. Joseph Jerome, *Private Right of Action Shouldn't Be a Yes-No Proposition in Federal US Privacy Legislation*, IAPP (Oct. 3, 2019), https://iapp.org/news/a/private-right-of-action-shouldnt-be-a-yes-no-proposition-in-federal-privacy-legislation/ [https://perma.cc/B6UD-HS3C].

[208] Nicholas Confessore, *The Unlikely Activists Who Took on Silicon Valley—and Won*, N.Y. TIMES MAG. (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html [https://perma.cc/D228-4NZU].

Therefore, collecting or using an individual's property without consent would be more akin to the tort of conversion.[209] Federal courts would have no issue finding a concrete harm when an individual's biometric information was collected or used without consent and plaintiffs would have Article III standing.

B. Definition of "Biometric Identifier"

New York City's recently enacted Local Law takes significant steps towards protecting New Yorkers.[210] The law is most similar to BIPA, but the city laws lack the greater enforcement power that state laws provide because of comparatively smaller resources.[211] Therefore, New York should pass a state-wide law that defines "biometric identifier" as:

> Data generated by measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, scans of face geometry or other unique biological patterns or characteristics that is used to identify a specific individual. Biometric identifiers do not include writing samples, written signatures, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color.

This is very similar to the Washington BPA definition and explicitly covers the typical categories, but includes face scans and allows room for expansion.[212] It also provides exceptions similar to BIPA.[213] In balancing the interests of individuals and businesses, it is important to consider the massive litigation

---

[209] *See Elements of Conversion*, DIGIT. MEDIA LAW, https://www.dmlp.org/legal-guide/elements-conversion [https://perma.cc/G8H2-PMCQ] (last visited Feb. 12, 2023).

[210] N.Y. ADMIN. CODE § 22-1201 (2021).

[211] *Compare* N.Y.C COMPTROLLER, ANN. STATE OF THE CITY'S ECON. AND FINS. (2021), https://comptroller.nyc.gov/reports/annual-state-of-the-citys-economy-and-finances/ [https://perma.cc/ZH7L-NDFC] (stating the budget for 2021 is $92.02 billion), *with* N.Y. STATE COMPTROLLER, REVIEW OF THE ENACTED BUDGET STATE FISCAL YEAR 2021-2022 (Apr. 2021), https://www.osc.state.ny.us/reports/budget/review-enacted-budget-state-fiscal-year-2021-22 [https://perma.cc/9TKL-ST46] (stating the state budget for 2021 is $212 billion). New York City is authorized to create private rights of action, so long as they are not preempted. *See* N.Y. CONST. art. IX, § 2; *see also* Bracker v. Cohen, 204 A.D.2d 115, 115 (1st Dep't 1994). Though outside the scope of this Note, § 22-1201 is not preempted by the SHIELD Act as the local law is neither expressly preempted nor impliedly preempted. *See generally* N.Y. GEN. BUS. LAW § 899-aa (McKinney 2019).

[212] WASH. REV. CODE ANN. § 19.375.010(1) (West 2017).

[213] 740 ILL. COMP. STAT. ANN. 14/25 (West 2008).

caused by scraping, like the Facebook case,[214] and the reality of commercial use of facial recognition.[215] Here, the interest of protecting citizens' identities outweighs the potential revenues businesses could receive from freely monetizing collected biometric identifiers. Indeed, during litigation, Facebook disabled their automatic facial recognition feature.[216] The company then introduced a written description of how their technology works, what the facial scans are used for, and a screen that required consent or denial before users were allowed back on the program.[217] Thus, the definition of biometric identifier should include facial scans.

C. Collection, Notice, and Consent

New York's statute should also mirror BIPA and CUBI's dual notice consent requirement.[218] Requiring notice and consent ensures that consumers have the opportunity to know the purposes for which their biometric information will be used.[219] It would limit the effectiveness of clickwrap features, and the statute could go so far as to mandate a button similar to CRPA's "do not sell my information" obligation.[220] To address concerns about consumers being left with no real option but to consent,[221] New York should prohibit businesses from denying services to anyone who refuses to give consent.

Notice and consent are essential because even if a plaintiff successfully obtains a monetary judgement from a violating business, their biometrics have already been collected and are vulnerable to breach. "Notice and consent" put the user on alert that their immutable characteristics are being collected and

---

[214] *See generally In re* Facebook Biometric Info. Priv. Litig., 326 F.R.D. 535 (N.D. Cal. 2018) (seeking to certify a class of claimants, including all residents of the state of Illinois, who posted an image on Facebook after 2011).

[215] Palmer, *supra* note 4.

[216] Srinivas Narayanan, *An Update About Face Recognition on Facebook*, META (Sept. 3, 2019), https://about.fb.com/news/2019/09/update-face-recognition/ [https://perma.cc/Q4JL-FT4E]. Facebook implemented this feature without notifying users originally. *Id.*

[217] *Id.*

[218] *See* ILL. COMP. STAT. ANN. 14/20; TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017).

[219] Park, *supra* note 144.

[220] *See id.*; CAL. CIV. CODE ANN. § 1798.130 (West 2022).

[221] *See* Ghelardi, *supra* note 68, at 881.

stored and that there is a possibility that these traits will be compromised.[222]

D. Retention

New York should craft its retention policy like BIPA, including the public disclosure requirement.[223] While failure to publish a written policy is not actionable in federal court,[224] blatant disregard of the statute would reflect poorly on the business, something a public corporation is unlikely to do.[225] Businesses that comply would provide the public with more knowledge on what is happening to their biometric information while simultaneously allowing other businesses to observe their policy and adapt as necessary. Additionally, like BIPA, a New York statute should provide a concrete time for destruction.[226] The requirement that information be destroyed after the initial purpose for collection or three years after the individual's last interaction with the entity is superior to other provisions because it provides fewer avenues of retaining this information than a "reasonable time" requirement.[227] In other words, if a business is still using a customer's biometric information for the initial purpose, there is no need to obtain consent from the customer again. However, if the customer has not requested actions involving their information for three years, the company must destroy the data. The more time biometric information is stored, the greater the risk the information is compromised.

E. Use

Perhaps the most complex provision to craft, New York should mirror BIPA's use provisions.[228] Preventing profit from selling biometrics incentivizes businesses to collect biometric data only when it directly benefits their product or service.

---

[222] *See* Park, *supra* note 144.

[223] *See* ILL. COMP. STAT. ANN. 14/15.

[224] *See* Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 626 (7th Cir. 2020).

[225] *See* Narayanan, *supra* note 216 (showing Facebook chose to publicly disclose their policy despite no legal obligation to do so).

[226] *See* ILL. COMP. STAT. ANN. 14/15.

[227] So long as a consumers' biometric information is still being used for the initial purpose it is collected for, there would be no requirement to provide biometric information a second time. Ted Claypoole & Cameron Stoll, *Developing Laws Address Flourishing Commercial Use of Biometric Information*, BUS. L. TODAY, May 2016, at 1, 2.

[228] *See supra* Section IV.D.

Furthermore, it strikes the correct balance between an individual's interests and a business's interests by allowing businesses to share the information across platforms only with the user's consent. CUBI's use provision, on the other hand, is too narrow because it hampers business disclosing biometric data at all.[229] Conversely, Washington's use provision is effectively a speedbump that could be worked around easily.[230] Under the Washington statute, biometric identifier information can be shared freely, so long as the receiving party agrees to not disclose it, increasing the risk of disclosure through breach each time.[231]

F. Right of Action

Without the private right of action, the statute fails to serve its purpose. Therefore, New York should include a private right of action. A private right of action is the best way to ensure compliance because it allows affected individuals to act as enforcement officers.[232] Private rights of actions lighten the burden on regulatory agencies and prevent corruption of the agencies tasked with enforcing the statute.[233] In fact, California's Attorney General's office has stated that they would likely prosecute only three cases per year under the CCPA and called the private right of action a "critical adjunct to governmental enforcement."[234] The Attorneys General of Texas and Washington, whose BPAs lack a private right of action, have yet to successfully enforce their respective statutes.[235] Therefore, while the private right of action will increase the burden on the court system, this burden is justified by the general deterrence function it would serve.

G. Exceptions

The New York statute should include the exceptions relating to state and local governments and mirror the carveouts for medical purposes common in BIPA, CUBI, and Washington's

---

[229] *See supra* Section IV.D.
[230] *See supra* Section IV.D.
[231] *See supra* Section IV.D.
[232] *See* Jerome, *supra* note 207.
[233] *Id.*
[234] *Id.*
[235] On February 14, 2022, Texas Attorney General Ken Paxton filed a lawsuit against Meta (formerly known as Facebook) for CUBI violations. Plaintiff's Petition, Texas v. Meta Platforms, Inc., No. 22-0121 (71st Judicial District filed Feb. 14, 2022). As of June 2023, the case has remained pending.

BPA.[236] However, the statute should decline to extend an exception to voiceprints by financial institutions like the one CUBI provides.[237] With the growth of artifical intelligence and deepfakes,[238] the use of voiceprints for identification verification is inherently insecure.[239] Therefore, excluding voiceprints from protection increases exposure of consumers to fraud with marginal benefit to businesses.[240]

Importantly, there should be no exclusion for "security purposes" like Washington's BPA.[241] Such a broad exception leaves collection completely within the business's discretion. Collection without notice and consent would effectively eviscerate the statute. While a business still could not transmit or sell the collected information, it would be subject to the same risk of breach while being retained and used internally for security purposes. Therefore, there should be no security purposes exception because it undermines the majority of the statute and increases the risk to consumers.

CONCLUSION

Once biometric information is compromised, monetary damages can never make the plaintiff whole again; their immutable traits are now beyond their control. Therefore, the only appropriate measure is to restrict collection and retention of biometric information to the greatest extent possible without unduly restraining business, innovation, and technology. Consent and notice of collection are essential for the informational purposes they serve and the obligations they impose. Strict retention policies are instrumental to limiting the risk to consumers while allowing businesses to run efficiently. Finally, the classification of biometric information as a right and a private right of action are necessary to provide standing and

---

[236] *See supra* notes 176–82 and accompanying text.

[237] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017).

[238] Deepfake means using machine learning and artificial intelligence to create audio or visual content with a high potential to deceive. Jan Kietzmann et al., *Deepfakes: Trick or Treat?*, 63 BUS. HORIZONS 135, 136 (2020).

[239] *See* David, *supra* note 62.

[240] While increasing efficiency, financial institutions have a multitude of other identification verification options, which they use, for example, when a person is too sick for their voice to be properly identified. *See Security as Unique as Your Voice*, CHASE, https://www.chase.com/personal/voice-biometrics [https://perma.cc/WUA3-MZS7] (last visited Feb. 10, 2023).

[241] WASH. REV. CODE ANN. § 19.375.040 (West 2017).

allow the statute to serve its deterrence function. The provisions suggested above strike the optimal balance between consumer protection and business interests.