Preserving Anonymity, the Virtue of Cities: Weighing the Effectiveness of New York City's Biometric Identifier Law and the Need for Major U.S. Cities to Follow its Lead

*Luke Fischer**

I. INTRODUCTION

As technology advances, the implementation of biometrics in everyday life increases exponentially.[1] Biometrics is broadly defined as "the measurement and analysis of people's physical characteristics."[2] While the innovative use of biometric data creates extensive benefits for businesses and consumers alike, there are also several privacy concerns that accompany the manipulation of physiological information for

*Luke Fischer, J.D., Class of 2023, Seton Hall University School of Law.

[1] Justina Alexandra Sava, *Biometric Technologies – Statistics & Facts*, STATISTA (Mar. 22, 2022), https://www.statista.com/topics/4989/biometric-technologies/#dossierKeyfigures (noting biometric expansion from its initial use as an aid in criminal identifications to its broader use in society. It is estimated that eighty percent of active cell phones in North America, Western Europe, and the Asia Pacific utilize biometric data).

[2] *Id*.

technological purposes.[3] Despite the increasing prevalence of biometric data across numerous industries and its associated risks, no single comprehensive federal law exists to regulate the collection and handling of this type of information.[4] As a result, state and local jurisdictions have begun to enact biometric privacy laws to address consumer concerns – a trend that has been coined "privacy localism."[5]

For example, New York City has recently implemented its own biometric data protection law, primarily focusing on the use of facial recognition technology by businesses within the City's five boroughs.[6] This legislation marks an attempt by the United States' most populous city to comprehensively address biometric data concerns.[7] If effective, this would show that cities may be as successful at regulating consumer data as the state or federal government, thus fueling this growing trend of privacy localism across the United States.[8] This Comment will analyze New York City's new biometric protection law with respect to existing biometric data regulations across the country, and expose the legislation's advantages and disadvantages. Part II of this Comment defines biometric data and explains the numerous ways in which commercial establishments, including retailers, entertainment venues, and casinos, utilize consumer biometric information. Part III discusses the benefits of biometric technologies for both consumers and businesses, as well as the risks that are associated with utilizing this type of data. Part IV provides a legislative analysis that discusses the Illinois Biometric Information Privacy Act ("BIPA"), the preeminent state legislation on this topic, and New York City's biometric data legislation and compares its respective benefits and downfalls.

---

3 Andrew Zarkowsky, *Biometrics: An Evolving Industry with Unique Risks*, HARTFORD (May 20, 2021), https://www.thehartford.com/insights/technology/biometrics (describing privacy concerns such as the sharing or selling of data and the potential for hacking and tracking individuals without their knowledge).

4 *Biometric Data and Privacy Laws (GDPR, CCPA/CPRA)*, THALES (June 16, 2021), https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data.

5 *See* Natalie A. Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020*, NAT'L L. REV. (Jan. 15, 2020), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020; Ira S. Rubinstein, *Privacy Localism*, 93 WASH. L. REV. 1961 (Dec. 1, 2018).

6 Steven Stransky, *NYC Biometric Law Enters into Force*, IAPP, (July 9, 2021) https://iapp.org/news/a/nyc-biometric-law-enters-into-force.

7 *See The 200 Largest Cities in the United States by Population 2022*, WORLD POPULATION REV., https://worldpopulationreview.com/us-cities (last visited Oct. 2, 2022).

8 *Id*.

II. WHAT IS BIOMETRIC DATA?

This section will explain what constitutes biometric data and how organizations' definitions of biometrics encompass different types of information. Next, it will discuss how the three types of businesses subject to New York City's Biometric Law utilize consumer biometric data. Each business type will be discussed in turn, beginning with commercial establishments, then entertainment venues, and finally casinos.

A. Defining Biometrics

Two general types of biometric data are utilized to identify individuals: (1) behavioral characteristics; and (2) physical characteristics.[9] Behavioral biometrics concern the products of an individual's intentional conduct, such as keystrokes, their signature, and voice recognition.[10] Physical biometrics concern the shape or composition of the body, such as facial recognition, fingerprint and iris scanning, and DNA.[11] The Center for Global Development broadly recognizes biometrics as any data that identifies individuals based on distinguishing physical or behavioral characteristics, including "fingerprints, face and hand geometry, gait, voice, DNA and other traits."[12] Likewise, the Biometrics Institute includes a comprehensive set of characteristics in its definition of biometrics. This definition includes DNA, ear shape, iris, retina, face shape, fingerprint, gait, hand shape, odor, typing pattern, hand and scleral veins, voice, and signature recognition.[13] Technological advances have allowed companies to collect and store each of these unique and personal characteristics from their consumers to be utilized later for various business purposes, such as airport and banking security and smartphone access.[14]

---

9 *Biometrics FAQs*, CTR. FOR GLOBAL DEV., https://www.cgdev.org/page/biometrics-faqs (last visited Oct. 2, 2022).

10 *Id*.

11 *Id*.

12 *Id*.

13 *Types of Biometrics*, BIOMETRICS INST., https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/ (last visited Oct. 2, 2022).

14 *The Top 9 Common Uses of Biometrics in Everyday Life*, NEC, https://www.nec.co.nz/market-leadership/publications-media/the-top-9-common-uses-of-biometrics-in-everyday-life/ (last visited Oct. 2, 2022); *What is Biometrics? How is it Used in Security?*, KASPERSKY, https://www.kaspersky.com/resource-center/definitions/biometrics (last visited Oct. 2, 2022).

Civilian facial recognition is one of the most common and well-recognized applications of biometric data[15] and is commonly used for facial classification, verification, and identification.[16] Classification sorts facial data into categories by gender, age, or race.[17] Verification compares a new facial image with stored images and produces a confidence score to determine if the two individuals are the same.[18] Identification compares a newly recorded faceprint to a database of previously stored facial data.[19] Technology companies and others implement facial identification mostly for security purposes.[20] Facial recognition remains the most universally known form of biometrics, as iPhone users across the world use Apple's Face ID daily to unlock phones, make purchases using Apple Pay, and approve purchases from Apple's App Store.[21] This technology provides consumers operational and security benefits, expediting the unlocking process by allowing users to access their devices after simply placing their face in front of the device's camera, which is programmed to only respond to the facial characteristics that have been manually programmed into the device.[22]

Behemoth technology companies like Apple are not the only entities that utilize consumer biometric data for operational benefits. Commercial retailers, entertainment venues, and casinos have implemented biometric technology in their operations, spawning legislative responses throughout many jurisdictions, such as New York City, to regulate the manipulation of citizens' biometric identifiers.[23]

15 Pavel Jirik, *5 Popular Types of Biometric Authentication: Pros and Cons*, PHONEXIA (Sept. 9, 2021), https://www.phonexia.com/en/blog/5-popular-types-of-biometric-authentication-pros-and-cons/.

16 *Id.*; Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L. J. 611, 621 (2019) [hereinafter Wright, *The Future of Facial Recognition*].

17 Wright, *The Future of Facial Recognition*, *supra* note 16.

18 Wright, *The Future of Facial Recognition, supra* note 16.

19 Wright, *The Future of Facial Recognition*, *supra* note 16.

20 Rebecca Heilweil, *How Can We Ban Facial Recognition When It's Already Everywhere?*, VOX (July 6, 2020, 9:15 AM), https://www.vox.com/recode/2020/7/3/21307873/facial-recognition-ban-law-enforcement-apple-google-facebook.

21 *See* Sam Costello, *How to Use Face ID on Your iPhone*, LIFEWIRE (July 8, 2021), https://www.lifewire.com/face-id-4151714.

22 Maggie Tillman, *What is Apple Face ID and How Does It Work?*, POCKET-LINT (Mar. 4, 2022), https://www.pocket-lint.com/phones/news/apple/142207-what-is-apple-face-id-and-how-does-it-work.

23 Philip Yannella & Doris Yuen, *New York City's Biometric Identifier Information Law Takes Effect*, JD SUPRA, (July 16, 2021), https://www.jdsupra.com/legalnews/new-york-city-s-biometric-identifier-4179244/ (reporting that the New York City law creates a

Commercial establishments most commonly use biometric data for the purposes of authentication, security, and customer engagement.[24] However, the operational benefits that businesses receive are accompanied by privacy risks to consumers whose data businesses store and use.

B. Commercial Retailers

Stores and retailers increasingly use biometric data and facial recognition technology for security purposes as well as targeted shopping techniques.[25] Some of the largest retailers in the United States use facial recognition technology to identify shoplifters by comparing security camera images with a database of known petty thieves.[26] This technology attempts to save retailers lost profits by facilitating the investigation process and hopefully identifying the offending shoplifter.[27] The facial recognition software, however, rarely produces a match and often produces a list of possible matches that require further investigation.[28] Additionally, although advances in technology have made strides to improve false identification, "low resolution, poor lighting, motion blur, off-angle faces, facial hair," and other variables impact the reliability of matches.[29] Also, the impact of these factors is not equal, as facial recognition technology falsely identifies minorities—most notably women of color—in significant numbers.[30] The National Institute of Standards and Technology (NIST) has confirmed various statistical studies that have determined that facial recognition technology performs the worst on darker-skinned females, with error rates up to 34 percent higher than those for lighter-skinned males.[31] When used by retailers for theft-identification purposes, this high rate

notice requirement for commercial establishments using biometric data and restricts the sale of such data to other parties).

24 Karen D. Schwartz, *How Biometrics Technology Is Changing Businesses' Security*, ITPRO TODAY (July 27, 2021) https://www.itprotoday.com/identity-management-and-access-control/how-biometrics-technology-changing-businesses-security.

25 *See* Vincent Nguyen, *Shopping for Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 535, 542–43 (2019).

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

27 *Id*.

28 *Id*.

29 *Id*.

30 Alex Najibi, *Racial Discrimination in Face Recognition Technology*, HARV. UNIV.: SCI. IN THE NEWS BLOG (Oct. 24, 2020), http://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

31 *Id*.

of error can perpetuate harmful societal stereotypes, racial bias, and even result in false arrests.[32]

Retailers also connect facial recognition with offline behaviors for consumer engagement and marketing purposes.[33] Retailers use this technology to target consumers by matching consumers' images with information that they provide on social media or through credit card transactions.[34] Retailers combine customer biometric data with the profiles they have created by tracking a customer's online purchases in order to manipulate the cost, availability, and desirability of a product.[35] One advantage consumer biometric data provides for retailers is that it allows retailers to direct products to specific consumers based on their preferences and greatly increases the likelihood of making a sale.[36]

C. Entertainment Venues

Entertainment venues, such as concert halls and stadiums, have also increased their utilization of facial recognition technology.[37] With a massive volume of civilians passing through such venues, facial recognition is used to ensure the safety of guests and lessen venue owners' liability.[38] For instance, the 2001 Super Bowl received additional national attention when the media revealed that Raymond James Stadium worked in tandem with the Tampa Police Department to scan attendees of the game through facial recognition technology.[39]

---

32 *See id*.

33 Chris Frey, *Revealed: How Facial Recognition Has Invaded Shops—and Your Privacy*, GUARDIAN (Mar. 3, 2016), https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto; Sapna Maheshwari, *Stores See a Future Without 'May I Help You?' (They'll Already Have Your Data)*, N.Y. TIMES (Mar. 10, 2019), https://www.nytimes.com/2019/03/10/business/retail-stores-technology.html.

34 *See generally* N.Y.C. ADMIN CODE §§ 22-1202(a) (enacted pursuant to Prop. Int. No.1170-A).

35 *Id.*

36 *Id*.

37 Chris Burt, *Biometrics could make attending large events a new ballgame*, BIOMETRICUPDATE.COM (Dec. 29, 2021, 11:18 AM) https://www.biometricupdate.com/202112/biometrics-could-make-attending-large-event-venues-a-whole-new-ballgame.

38 *See Facial Recognition for Retail, Restaurants, Hospitality & Entertainment Venues*, SERVICEMARK TELECOM, https://servicemark.net/products-services/neoface-surveillance-facial-recognition/for-retail-restaurants-hospitality-and-entertainment-venues (last visited Sept. 5, 2022) [hereinafter *Facial Recognition*, SERVICEMARK TELECOM].

39 Robert H. Thornburg, *Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of Current Uses Under the Fourth Amendment*, 20 J. MARSHALL J. COMPUT. & INFO. L. 321, 326 (2002).

Soon after the Super Bowl, the American Civil Liberties Union (ACLU) and national news outlets, including *The Los Angeles Times*, revealed that the City of Tampa had used the Super Bowl as a testing ground for new and relatively unknown biometric technology.[40] The Tampa Police Department implemented a new video surveillance system to scan, analyze, and cross-reference the faces of one hundred thousand attendees with a database of wanted and suspected criminals created by the Florida Department of Law Enforcement and the FBI.[41] While the department defended its actions by arguing that the surveillance was no more intrusive than the type conducted around banks and government buildings and that they successfully identified nineteen individuals in the crowd with outstanding warrants, it still received backlash from the public, who felt that the face-scanning was unnecessary and intrusive government surveillance.[42] The ACLU of Florida called for public hearings on the implications of this biometric technology on citizens' privacy rights, arguing that attendees were not adequately informed "that their faces were being silently digitized and matched up against the mug shots of criminals and terrorists" and that the government must exercise some regulation over this "rapidly developing use of sophisticated face-identification systems."[43]

Nevertheless, a few months later, the City of Tampa implemented a facial recognition program in the downtown entertainment district of Ybor City to test if the rapidly expanding technology could assist the police in identifying known convicts congregating in certain areas.[44] However, because the software was not advanced enough to make conclusive matches, it provided no real benefits, and the City of Tampa

40 Kaleigh Rogers, *That Time the Super Bowl Secretly Used Facial Recognition Software on Fans*, VICE: MOTHERBOARD (Feb. 7, 2016, 9:13 AM), https://www.vice.com/en/article/kb78de/that-time-the-super-bowl-secretly-used-facial-recognition-software-on-fans; Letter from ACLU of Fla., to Kirby C. Rainsberger, Assistant City Attorney, City of Tampa Police Dept. (Nov. 27, 2001) (on file with ACLU); Charles Piller, Josh Meyer and Tom Gorman, *Criminal Faces in the Crowd Still Elude Hidden ID Cameras*, L.A. TIMES (Feb. 2, 2001, 12:00 AM), https://www.latimes.com/archives/la-xpm-2001-feb-02-mn-20035-story.html; Robert H. Thornburg, *Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of Current Uses Under the Fourth Amendment*, 20 J. MARSHALL J. COMPUT. & INFO. L. 321, 326 (2002).

41 Robert H. Thornburg, *Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of Current Uses Under the Fourth Amendment*, 20 J. MARSHALL J. COMPUT. & INFO. L. 321, 326 (2002).

42 *Id*.; Vickie Chachere, *Biometrics Used to Detect Criminals at Super Bowl*, ABC NEWS (Feb. 13, 2021), https://abcnews.go.com/Technology/story?id=98871&page=1.

43 Press Release, ACLU of Fla., ACLU Calls for Public Hearings on Tampa's "Snooper Bowl" Video Surveillance (Feb. 1, 2001) (on file with ACLU).

44 Thornburg, *supra* note 39, at 326.

ended the program.[45] The Tampa Super Bowl case received great attention because it occurred in the pre-9/11, pre-Snowden era, when biometrics scanning and government surveillance at entertainment venues was inconceivable to most Americans.[46]

Professional sporting events are not the only occasions where biometric software is used to identify crowds.[47] Concert stadiums often scan the faces of attendees, and while these venues have not been heralded for their transparency regarding the use of this technology, they repeatedly cite security concerns as their justification.[48] For instance, Taylor Swift's security team has reportedly used facial recognition software at her concerts in order to protect her from known stalkers.[49] At Swift's 2018 Rose Bowl show, a kiosk displaying her rehearsal clips included a facial-recognition camera that scanned the facial geometry of the attendees watching the videos and compared these attendees to a database of people with a known history of stalking Swift who could pose a threat to her safety.[50] The public was alarmed by the privacy concerns accompanying this technology; specifically, questions arose regarding who owns the photos and how long they will be kept on file.[51]

This use of facial recognition technology is prevalent in the entertainment world.[52] Entertainment and ticket retailers have been known to utilize biometric technology to expedite entry into venues and ease movement throughout venues.[53] In 2018, Ticketmaster invested in Blink Identity, a company that rapidly identifies concertgoers to help VIP fans move through turnstiles and security more efficiently.[54] Despite privacy concerns, entertainment venues enjoy both security and efficiency benefits through the use of this technology.[55]

---

45 Thornburg, *supra* note 39, at 326.

46 Thornburg, *supra* note 39, at 326.

47 Thornburg, *supra* note 39, at 323, 326.

48 *See generally* Sydny Shepard, *Facial Recognition Kiosk at Taylor Swift Concert Brings up Data Security and Privacy Issues*, SECURITY TODAY (Dec. 17, 2018), https://securitytoday.com/articles/2018/12/17/facial-regonition-kiosk-at-taylor-swift-concert-brings-up-data-security-and-privacy-issues.aspx.

49 Steven Knopper, *Why Taylor Swift Is Using Facial Recognition at Concerts*, ROLLING STONE (Dec. 13, 2018), https://www.rollingstone.com/music/music-news/taylor-swift-facial-recognition-concerts-768741/.

50 *Id*.

51 *Id*.

52 *Id*.

53 Christina Lee, *Using Biometrics at Events: Security over Privacy?*, BAYOMETRIC, https://www.bayometric.com/using-biometrics-at-events-security-over-privacy/.

54 Knopper, *supra* note 49.

55 Knopper, *supra* note 49.

D. Casinos

In addition to retailers and entertainment venues, casinos have leveraged facial recognition technology to provide enhanced security and to modernize the gambling industry.[56] Casino security has remained a pressing issue for decades, as surveillance teams work to ensure that gamblers do not cheat and cause the establishments to suffer financial losses.[57] Facial recognition technology has been used in this industry to identify known cheaters and thieves and to notify staff of this information instantaneously.[58] Additionally, since casinos attract a large volume of foot traffic each day, these locations can be popular targets for criminal actors to gather in an effort to go undetected in large crowds.[59] Biometric identifier technology functions as a digital "watchlist" where staff can be instantly notified if known terrorists, wanted criminals, or missing persons enter the facilities.[60] This can greatly assist casino security teams who have the difficult job of surveilling all persons on the premises.[61] Additionally, this technology can have beneficial societal impacts through its identification of "problem gamblers" who show unhealthy or addictive tendencies.[62]

III. BENEFITS AND RISKS IN COMMERCIAL ESTABLISHMENTS

This section will explore the advantages and possible hazards that accompany the utilization of biometric technology in commercial establishments. First, this section will explain the most common benefits that this technology can provide in terms of service, security, and health. Then, this section will discuss the privacy, data breach security, and accuracy risks that often arise when businesses manipulate biometric technology.

56 Sam Kljajic, *Ask the Expert: Casinos, Facial Recognition, and COVID-19*, SAFR, (Apr. 15, 2020), https://safr.com/general/ask-the-expert-casinos-face-recognition-and-covid-19/.

57 *Id.*; Austin Crane, *The Science of Casino Security*, UNTAMED SCI. (Feb. 2020), https://untamedscience.com/blog/science-of-casino-security/.

58 Kljajic, *supra* note 56.

59 Kljajic, *supra* note 56.

60 Kljajic, *supra* note 56.

61 Kljajic, *supra* note 56.

62 Jacob Solis, *How AI and Facial Recognition Tech Could Reshape Las Vegas Casinos*, NEV. INDEPEND., (Jan. 21, 2020, 2:00 AM), https://thenevadaindependent.com/article/how-new-ai-and-facial-recognition-tech-could-reshape-las-vegas-casinos.

A. Benefits

Biometric technology has proven to be a valuable tool for commercial establishments to enhance service, security, and health.[63] The most common rationale commercial establishments cite for their implementation of biometric identifier technology is the bolstering of safety and the enhancement of customer experience within their businesses.[64] The National Retail Federation (NRF) reported that loss from theft and fraud in the retail sector increased from $46.8 billion in 2017 to $50.6 billion in 2018, forcing retailers to find innovative ways to identify shoplifters and minimize their impact.[65] For this reason, facial recognition technology has increased exponentially in the retail sector, as it provides significant surveillance and security benefits.[66] When a customer enters a store that utilizes this technology, his or her facial image is captured from a live video stream.[67] Next, the customer's facial features are extracted from the image, whereby the customer's facial image is then cropped and converted into greyscale.[68] Then, the resulting image is converted into a template that an algorithm uses to cross-reference a larger database.[69] Finally, if the template is matched with a previously identified shoplifter profile within the database, authorities are notified.[70] This technology bolsters store security by "keeping an eye on known troublemakers [and] individuals with a criminal past."[71]

Besides its advantages for security purposes, biometric technology also has customer service benefits for the retail sector.[72] Companies like ServiceMark Telecom purport that facial recognition improves customer interaction by recognizing repeat customers as they enter stores, which provides retailers the opportunity to create more personalized shopping experiences.[73] Also, facial recognition triggers automatic activation of customer promotional programs when someone

63 *See* Schwartz, *supra* note 24.

64 *Facial Recognition*, SERVICEMARK TELECOM, *supra* note 38.

65 Vihar Soni, *Facial Recognition in Retail: Enhance In-Store Customer Experience and Improve Retailer Operations*, EINFOCHIPS (Aug. 11, 2020), https://www.einfochips.com/blog/facial-recognition-in-retail-enhance-in-store-customer-experience-and-improve-retailer-operations/.

66 Soni, *supra* note 65.

67 Soni, *supra* note 65.

68 Soni, *supra* note 65.

69 Soni, *supra* note 65.

70 Soni, *supra* note 65.

71 *Facial Recognition*, SERVICEMARK TELECOM, *supra* note 38.

72 *Facial Recognition*, SERVICEMARK TELECOM, *supra* note 38.

73 *Facial Recognition*, SERVICEMARK TELECOM, *supra* note 38.

enters the store and provides access to customer shopping preferences upon arrival, allowing the staff to individually tailor the customer experience.[74] Lastly, by creating a database of personal shopping records and trends to understand customer wants and needs, this technology improves customer relations and creates a broader consumer community.[75]

Restaurants also benefit from the use of this biometric technology.[76] CaliBurger, a California burger chain, exemplifies how restaurants implement facial recognition technology to enhance customer experience.[77] Upon entering the establishment, customers step in front of a kiosk equipped with a face-scanning camera.[78] The camera examines the customer's face and captures an image, cross-references that image with its database of customers enrolled in the CaliBurger loyalty program, and displays the customer's loyalty profile with his or her past and favorite purchases.[79] The main advantages of biometric technology for Caliburger, and other restaurants that implement this technology, are that it speeds up the ordering process, allowing more customers to cycle through at a faster rate, and it has the potential to lower costs by using automation rather than human workforce, enabling the business to hire less employees to offset the cost of the technology.[80] Outside of the fast-food context, other restaurants have implemented technology such as NeoFace Watch, which helps provide a "VIP" dining experience by recognizing long-term customers and recording favorite menu items, past drink orders, special occasions, and customer allergies.[81]

Likewise, entertainment venues can benefit substantially from the use of such biometric data; since hotels, casinos, and concert halls strive to create the best hospitality for guests in order to beat out competitors.[82] Hotels and venues have used facial recognition to streamline the check in and out process by instantly recognizing prominent and celebrity guests and alerting staff of their presence, which expedites access to fast ticket holders, prevents underage guests from entering age-restricted areas, and tracks known individuals with

74 *See Facial Recognition*, SERVICEMARK TELECOM, *supra* note 38.
75 *See generally Facial Recognition*, SERVICEMARK TELECOM, *supra* note 38.
76 *See* Soni, *supra* note 65.
77 Soni, *supra* note 65.
78 Soni, *supra* note 65.
79 Soni, *supra* note 65.
80 Soni, *supra* note 65.
81 *Facial Recognition*, SERVICEMARK TELECOM, *supra* note 38.
82 *Facial Recognition*, SERVICEMARK TELECOM, *supra* note 38.

criminal pasts.[83] In the Covid-era, with the prevalence of masks and the greater need for hotels and resorts to ensure that their guests are healthy and not spreading the virus on their premises, biometric data technology has been valuable to scan guests' faces, detect mask compliance, and take body temperatures without having a staff member come in close contact with guests.[84]

B. Risks

Despite the benefits that biometric identifier technology provides for commercial establishments, it also poses significant risks to consumers regarding privacy, data breach security, and accuracy issues that lead to bias.

The use of facial image scanning and logging into databases has implications on citizens' privacy rights. While metrics used by stores were previously anonymous tools to aggregate consumer preferences, facial recognition technology used by commercial establishments links faces to the bits of data collected through loyalty programs and sale records.[85] Recognizing consumer fear of matching personal data with facial recognition software, many large retailers have simply declined to comment on their involvement with this technology.[86] The most valuable piece of information for retailers is the "predictive analytics that come[s] from tying that one piece of information, [the customer's] face, to [the customer's] whereabouts, to [the customer's] patterns, to the way [customers] move through space and time."[87] The main risk lies in the vulnerability that this type of consumer information may be compiled and sold without the knowledge or consent of the individuals affected.[88]

One of the most well-known instances of a similar manipulation of personal data was exposed when a whistleblower described how the data firm Cambridge Analytica harvested millions of Facebook profiles to exploit US voters by targeting them with personalized political

83 *Facial Recognition*, SERVICEMARK TELECOM, *supra* note 38; Chris Frey, *Revealed: How Facial Recognition has Invaded Shops–and Your Privacy*, GUARDIAN (Mar. 3, 2016, 7:01 AM), https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto.

84 Dr. Jua Huang, *Elevating Hotel Guest Experiences with Facial Recognition*, HOSPITALITY TECH., (Dec. 14, 2020), https://hospitalitytech.com/elevating-hotel-guest-experiences-facial-recognition.

85 *See* Frey, *supra* note 83.

86 Frey, *supra* note 83.

87 Frey, *supra* note 83.

88 *See* COUNCIL OF CITY OF N.Y., Proposed Int. No.1170-A (Comm. Rep. 2020).

advertisements.[89] In this case, Cambridge Analytica had collected data from millions of Facebook users to determine their political preferences and implicit views on domestic issues.[90] The company then created algorithms to direct users to information that would resonate with them based on their preferences and to place them in echo chambers of one-sided content that the organization hoped would induce them to vote in a certain way.[91] Cambridge Analytica's manipulation of consumer data based on personal viewpoints, with the goal of swaying a presidential election, demonstrates the value of this information and the nefarious ways it can be utilized.[92]

Cambridge Analytica is not the only entity that has been exposed for misusing consumer biometric data. For instance, Ever, a photo storage app, garnered national attention when users discovered that the company was manipulating their images to develop a facial recognition database without users' explicit consent, and selling users' biometric data to third parties, law enforcement agencies, and even the military.[93] Consumers were outraged that the company did not properly disclose its business model within its privacy policy.[94] The American Civil Liberties Union (ACLU) of Northern California determined that Ever's compilation of personal photos to build surveillance technology constituted an "egregious violation of people's privacy."[95] Despite rebranding itself as an Artificial Intelligence company called Ever AI, the company was unable to recover from poor business practices accusations and shut down permanently in August 2020.[96] Additionally, lawsuits have been filed against major retailers, such as Macy's, for using Clearwater software that "actively profits" from biometric data that the

89 Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach* (Mar. 17, 2018, 6:03 PM), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

90 *Id.*

91 *Id.*

92 *Id.*

93 Olivia Solon & Cyrus Farivar, *Millions of People Uploaded Photos to the Ever App. Then the Company Used Them to Develop Facial Recognition Tools*, NBC NEWS (May 9, 2019, 4:10 AM), https://www.nbcnews.com/tech/security/millions-people-uploaded-photos-ever-app-then-company-used-them-n1003371.

94 Sarah Perez, *Ever, Once Accused of Building Facial Recognition Tech Using Consumer Data, Shuts Down Consumer App*, TECHCRUNCH (Aug. 24, 2020, 2:23 PM), https://techcrunch.com/2020/08/24/ever-once-accused-of-building-facial-recognition-tech-using-customer-data-shuts-down-consumer-app/.

95 *Id.*

96 *Id.*

stores use for security and marketing.[97] Leaked documents revealed that a number of other major department stores, including Best Buy, Kohl's, and Walmart, also implement the Clearwater software in their operations.[98] Clearwater compiles a database of facial images from social media accounts and analyzes those images against in-store surveillance footage so that the companies can personally identify customers for various business purposes.[99]

All of these biometric technology tools eliminate the idea that cities are anonymous places where citizens can move around virtually undetected; instead, their movements, habits, and tastes are recorded by retailers and stored in databases by big data biometrics.[100] The *New York Times* conducted its own facial recognition experiment, using security cameras in Bryant Park over the course of a day, to expose the ease at which surveillance footage can be utilized to gather biometric identifier data.[101] The project demonstrated that for under $100, a team could detect 2,750 faces within nine hours and compile a catalog of facial images to match with the individuals' real identities.[102] The results indicated that nearly three thousand individuals could be identified by a private team unsuspectingly while walking around a busy park in one of the most populated cities in America, allowing for numerous possibly perilous uses for that collected data.[103]

Along with privacy concerns, the use of biometric identifier data comes with security risks and the opportunity for data breaches. The implementation of facial recognition technology by businesses to identify customers in public places and track their movement, location, and conduct, often creates large databases of consumer information that most consumers might not be aware of.[104] With such mass amounts of data neatly compiled, there is an inherent risk that these databases are being sold, shared, and used without the consent or knowledge of the

97 Robert Channick, *Macy's Hit with Privacy Lawsuit Over Alleged Use of Controversial Facial Recognition Software*, CHI. TRIB. (Aug. 11, 2020, 11:01 AM), https://www.chicagotribune.com/business/ct-biz-macys-lawsuit-clearview-facial-recognition-20200811-mstcyf7wufdjvbanpv6ehjtvni-story.html.

98 *Id.*

99 *Id.*

100 Rogers, *supra* note 40.

101 Sahil Chinoy, *We Built an 'Unbelievable' (but Legal) Facial Recognition Machine*, NEW YORK TIMES, (Apr. 16, 2019), https://www.nytimes.com/interactive/2019/04/16/opinion/facial-recognition-new-york-city.html.

102 *Id.*

103 *Id.*

104 COUNCIL OF CITY OF N.Y., Proposed Int. No.1170-A (Comm. Rep. 2020).

individuals.[105] Additionally, since most businesses do not employ bulletproof security to protect their catalogs of consumer information, this data is vulnerable to ransomware attacks, leaks by careless or corrupt employees, and foreign intelligence break-ins.[106]

Alternatively, when biometrics are used for access and authentication purposes, the consequences of data theft are much more precarious than those of normal passwords.[107] Unlike word and pin number codes, biometric characteristics are immutable and can never be changed.[108] Thus, when a hacker or thief has a copy of a person's unique biometric identifier, there is no way to ensure that the use of the person's biometrics for authentication will ever be secure.[109] For instance, after hackers stole a database of employee fingerprints from the U.S. Office of Personal Management during a cyberattack, the security of the biometric data of nearly 5.6 million employees was permanently compromised.[110]

Lastly, because this technology continues to evolve, its existing flaws often have unintended consequences for the citizens exposed to it. When facial recognition is used for identification, accuracy issues can negatively and disproportionately impact people of color and women.[111] Recent studies have exposed growing rates of error across demographic groups, noting that the most extreme accuracy issues are among Black females between the ages of eighteen and thirty.[112] In 2018, the "Gender Shades" project tested the accuracy of three facial recognition algorithms on four categories of individuals: darker-skinned females, darker-skinned males, lighter-skinned females, and lighter-skinned males.[113] The National Institute of Standards and Technology (NIST) confirmed that all three algorithms performed the worst on darker-skinned females, with error rates almost thirty-five percent higher than those for lighter-skinned males.[114] Algorithms that have the highest

105 *Id*.

106 *Id*.

107 David Balaban, *4 Drawbacks of Biometric Authentication*, IFSEC GLOBAL (Oct. 21, 2019), https://www.ifsecglobal.com/cyber-security/4-drawbacks-of-biometric-authentication/.

108 *Id*.

109 *Id*.

110 Andrea Peterson, *OPM Says 5.6 Million Fingerprints Stolen in Cyberattack, Five Times as Many as Previously Thought*, WASH. POST (Sept. 23, 2015, 2:00 PM), https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/?noredirect=on.

111 Najibi, *supra* note 30.

112 Najibi, *supra* note 30.

113 Najibi, *supra* note 30.

114 Najibi, *supra* note 30.

rates of error for young black females can have damaging societal repercussions, especially when the technologies are used to identify shoplifters.[115] If retailers and law enforcement rely on this technology to identify known shoplifters, and surveillance footage mistakenly matches a person's image to the database of previous criminals, this flawed technology will cause the arrest of an innocent person and perpetuate harmful stereotypes.[116] This allegedly occurred when a student, Ousmane Bah, was mistakenly linked by a facial recognition system in an Apple store as a shoplifter, resulting in the NYPD arriving at his home to arrest him for crimes he did not commit.[117] He is now suing Apple for $1 billion, indicating the steep liability that companies can face for inaccurate biometric identifier technology.[118]

IV. LEGISLATIVE ANALYSIS

This section will serve as an analysis of the statutes that have been enacted to better protect consumer biometric data. First, it will discuss privacy localism and the trend in smaller jurisdictions of enacting biometric legislation in order to fill in the gaps in biometric protection that Congress has yet to fill. Next, it will analyze the most well-recognized state biometric privacy legislation, Illinois' BIPA, and discuss the reasons it is so protective of citizens' data. Additionally, this section will explore the details of the NYC Biometric Identifier Law and analyze its successes and pitfalls as an example of privacy localism. Finally, it will juxtapose the BII with BIPA, and compare New York City's local privacy protections with the leading state-level legislation on this topic.

A. Privacy Localism

This section will explain the benefits of "privacy localism," which is the term used to describe privacy legislation governed by ordinances, local laws, executive orders, resolutions, regulations, policies, and practices of local governments.[119] Further, this section argues that privacy localism allows cities to experiment with novel data regulation legislation that can be applied more broadly, can tailor policies to fit locally varying circumstances and locally varying preferences, and it can

115 *See* Sigal Samuel, *The Growing Backlash Against Facial Recognition Tech*, VOX (Apr. 27, 2019, 8:00 AM), https://www.vox.com/future-perfect/2019/4/27/18518598/ai-facial-recognition-ban-apple-amazon-microsoft.

116 *See id*.

117 *Id*.

118 *Id*.

119 Rubinstein, *supra* note 5, at 1967.

bring the government closer to the people, giving individual citizens greater influence over policy and greater attachment to the government.

Since the Trump administration withdrew a stream of Obama-era federal privacy legislation, the states and local governments have been left to address the ever-present data privacy issues that are presented by big data and private entities.[120] Local privacy laws and regulations have not received much attention in the study of privacy law in the past because they have not played a large role in regulating this field until recently.[121] Because cities containing large urban centers are "data-rich environments . . . [where] city dwellers generate a vast amount of data through daily interaction with devices and sensors as they crisscross public spaces and utilize city services," they are intrinsically implicated in the battle between data privacy and big commercial data.[122] Cities across the nation have begun to address privacy issues by implementing surveillance ordinances; however, these laws only address police and government data, not consumer data.[123]

As Ira Rubinstein discusses in his article, *Privacy Localism*, privacy legislation enacted by local governments bridges two vital gaps in state and federal privacy regulations.[124] These gaps include what she coins the "Public Surveillance Gap" and the "Fair Information Practices Gap."[125] The Public Surveillance Gap concept recognizes that privacy is threatened due to the "pervasive and invasive" mass surveillance techniques used by private entities today.[126] Rubinstein argues that the Fourth Amendment and federal electronic surveillance laws (ECPA) do not implicate the type of mass surveillance that poses issues today.[127] Thus, cities and counties are able to enact local ordinances that directly target this issue.[128] The Fair Information Practices Gap addresses the problem that most local governments are not required to abide by state and federal privacy laws with regard to fair practices by private

120 *Id.* at 1970; *see also* David Shepardson, *Trump Signs Repeal of U.S. Broadband Privacy Rules*, REUTERS (Apr. 3, 2017, 7:50 PM), https://www.reuters.com/article/us-usa-internet-trump/trump-signs-repeal-of-u-s-broadband-privacy-rules-idUSKBN1752PR (stating that in 2017, Trump signed a narrowly passed bill that repealed the privacy legislation that required internet service providers to take action to protect consumer privacy more than internet websites like Google and Facebook).

121 *See* Rubinstein, *supra* note 5, at 1964.

122 Rubinstein, *supra* note 5, at 1964.

123 Rubinstein, *supra* note 5, at 1966.

124 Rubinstein, *supra* note 5, at 1974.

125 Rubinstein, *supra* note 5, at 1968.

126 Rubinstein, *supra* note 5, at 1974–75.

127 Rubinstein, *supra* note 5, at 1975.

128 *See* Rubinstein, *supra* note 5, at 1966.

companies.[129] These fair information practices, including "rights and responsibilities that are associated with the transfer and use of personal information[,]" can only be applied to such entities if the federal and state acts delineate that they do, or if local governments enact legislation directly implicating them.[130]

B. The Illinois Biometric Privacy Act

In 2008, Illinois became one of the first states to set rules for the use of biometric data by private entities through its legislature.[131] The Illinois legislature enacted the Illinois Biometric Privacy Act ("BIPA") to provide protections for consumers against private entities that collect biometric data and identifiers.[132]

BIPA limits both the means by which private entities obtain biometric data and the methods by which entities manage and store consumer biometric data.[133] To the first point, under BIPA, a private company may not

collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first: (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which it is being collected, stored and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.[134]

Additionally, BIPA requires companies that possess biometric data to develop a public written policy delineating the guidelines and retention schedule for permanently deleting biometric data once the

129 Rubinstein, *supra* note 5, at 1981.

130 Rubinstein, *supra* note 5, at 1981.

131 *See Biometric Information Privacy Act (BIPA)*, ACLU ILL., https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa (last visited Sept. 6, 2022).

132 *See* Dmitry Shifrin & Mary Buckley Tobin, *Past, Present and Future: What's Happening with Illinois' and Other Biometric Privacy Laws*, NAT'L L. REV. (May 28, 2021), https://www.natlawreview.com/article/past-present-and-future-what-s-happening-illinois-and-other-biometric-privacy-laws.

133 *See* Ryan Blaney, Julia D. Alonzo, & Brooke G. Gottlieb, *Litigation Breeding Ground: Illinois' Biometric Information Privacy Act*, NAT'L L. REV., (Mar. 18, 2021), https://www.natlawreview.com/article/litigation-breeding-ground-illinois-biometric-information-privacy-act; Biometric Information Privacy Act, 740 I.L.C.S. 14 (2008).

134 Biometric Information Privacy Act, *supra* note 133.

initial purpose of collection has been satisfied.[135] Private entities must "[s]tore, transmit, and protect from disclosure all biometric" data using the reasonable standard of care within the entity's industry and in a manner that is the same as, or more protective than, other confidential and sensitive information the private entity stores.[136] They are also forbidden from selling, leasing, trading, or otherwise profiting from biometric data, and may not disclose or disseminate biometric information unless the subject of the information consents or the private entity is required by law, valid warrant, or subpoena.[137]

The most significant facet of BIPA for consumers, and the reason that it is recognized as the most consumer-protective biometric legislation, is that it provides a private right of action for individuals that have been harmed by violations of BIPA, as well as allows for statutory damages up to $1,000 for each negligent violation and up to $5,000 for each reckless or intentional violation.[138] There is no statute of limitations in the act, and in 2018, the Illinois Supreme Court held that there is no requirement of actual harm to establish standing to sue under BIPA, so a procedural violation is sufficient to support a private right of action.[139]

C. NYC Biometric Identifier Law

This section will discuss New York City's Biometric Identifier Law. It will explain the various aspects of the law, what it covers, what entities are subject to its provisions, and what remedies individuals are entitled to for violations of the ordinance. Then, this section will cover the ordinance's strengths and the ways in which it can be improved.

In July 2021, the New York City Biometric Identifier Information Act ("BII Law") went into effect pursuant to NYC Administrative Code, § 22-1201-1205.[140] In effect, the law provides strict requirements for "commercial establishments that collect, use or retain biometric identifier information about their clients, customers or patrons."[141]

---

135 Biometric Information Privacy Act, *supra* note 133.

136 Biometric Information Privacy Act, *supra* note 133.

137 Biometric Information Privacy Act, *supra* note 133.

138 Biometric Information Privacy Act, *supra* note 133.

139 Biometric Information Privacy Act, *supra* note 133; *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197, 1205 (Ill. 2019).

140 Anjalia C. Das & Donald J. Brewer Jr., *New York City Introduces Biometric Identifier Information Act*, WILSON ELSER (Aug. 18, 2021), https://www.wilsonelser.com/news_and_insights/insights/4287-new_york_city_introduces_biometric_identifier.

141 *Id*.

The BII Law provides concrete definitions to delineate what is and is not covered within its provisions. The law defines biometric identifier information as

> a physiological or biological characteristic that is used by or on behalf of a commercial establishment, singly or in combination, to identify, or assist in identifying, an individual, including, but not limited to: (i) a retina or iris scan, (ii) a fingerprint or voiceprint, (iii) a scan of hand or face geometry, or any other identifying characteristic.[142]

One of the ways that BII is distinguished from BIPA is that its scope is narrower, regulating only commercial establishments that collect such data, whereas BIPA subjects all private entities to its provisions.[143] A commercial establishment refers to "a place of entertainment, a retail store, or a food and drink establishment."[144] First, the phrase "'food and drink establishment' is an establishment that gives or offers for sale food or beverages to the public for consumption or use on or off the premises, or on or off a pushcart, stand, or vehicle."[145] Next, a "'place of entertainment' is any privately or publicly owned and operated entertainment facility, such as a theater, stadium, arena, racetrack, museum, amusement park, observatory, or other place where attractions, performances, concerts, exhibits, athletic games or contests are held."[146] Lastly, a "'retail store' is an establishment wherein consumer commodities are sold, displayed or offered for sale, or where services are provided to consumers at retail."[147] There is an overabundance of these types of businesses throughout New York City, so even though BII does not cover all private entities like BIPA does, it still regulates a significant number of institutions in its jurisdiction.

The law's purpose is to regulate the collection, use, and retention of biometric identifier information. The provisions state that

> [a]ny commercial establishment that collects, retains, converts, stores or shares biometric identifier information of

142 N.Y. Admin. Code, *Chapter 12: Biometric Identifier Information*, AMERICAN LEGAL PUBLISHING, (Jan. 10, 2021), https://codelibrary.amlegal.com/codes/newyorkcity/latest/NYCadmin/0-0-0-42626 [hereinafter *Chapter 12: Biometric Identifier Information*, AMERICAN LEGAL PUBLISHING].

143 Cameron Argetsinger, Cristina Ferretti & Neil Merkl, *NYC's Biometric Identifier Information Law: Are You Covered?*, JD SUPRA (Nov. 3, 2021), https://www.jdsupra.com/legalnews/nyc-s-biometric-identifier-information-3012307/.

144 *Id*.

145 *Id*.

146 *Id*.

147 *Chapter 12: Biometric Identifier Information*, AMERICAN LEGAL PUBLISHING, *supra* note 142.

> customers must disclose such collection, retention, conversion, storage or sharing, as applicable, by placing a clear and conspicuous sign near all of the commercial establishment's customer entrances notifying customers in plain, simple language, in a form and manner prescribed by the commissioner of consumer and worker protection by rule, that customers' biometric identifier information is being collected, retained, converted, stored or shared, as applicable.[148]

Additionally, the law makes it "unlawful to sell, lease, trade, share in exchange for anything of value or otherwise profit from the transaction of biometric identifier information."[149] These provisions of BII are significant because they provide two key benefits for consumers: transparency and accountability. The sign requirement alerts potential customers that their biometric identifiers will be collected if they enter the establishment; thus, the individual can make an educated decision as to whether they will patronize the business, knowing that their data will be stored, or decide to visit elsewhere.[150] Additionally, the prohibition on profiting from customer data holds establishments accountable by only allowing them to utilize this data for legitimate business purposes. This solves the issue of businesses aggregating and selling consumer data without the consumers' knowledge, and it may even incentivize entities to stop collecting such data if they cannot profit from it.

Another critical component of BII for civilians is that it provides two separate frameworks for individuals to bring a private right of action against commercial establishments for non-compliance.[151] First, if individuals are not provided proper notice by a commercial establishment regarding its use of their biometric data, they must provide written notice of the violation at least thirty days prior to taking legal action.[152] If the violation is cured by the commercial establishment within thirty days of receiving the written notice and prevents further violations, then the individual is barred from commencing legal action.[153] On the contrary, if the commercial establishment does not

148 *Chapter 12: Biometric Identifier Information*, AMERICAN LEGAL PUBLISHING, *supra* note 142.

149 *Chapter 12: Biometric Identifier Information*, AMERICAN LEGAL PUBLISHING, *supra* note 142.

150 *Chapter 12: Biometric Identifier Information*, AMERICAN LEGAL PUBLISHING, *supra* note 142.

151 Stransky, *supra* note 6.

152 Stransky, *supra* note 6.

153 Stransky, *supra* note 6.

cure the violation within the thirty-day period, an individual may bring suit.[154]

Alternatively, regarding the law's transaction prohibition, aggrieved individuals may commence an action at any time.[155] Damages are assessed, starting at $500 for each violation of the notice requirement.[156] A commercial establishment that acts negligently towards the transactional prohibition can also be liable for $500 per violation.[157] For intentional or reckless violations of the transactional prohibition provision, however, an individual can recover damages up to $5,000 per violation.[158]

This facet of BII is significant for two reasons: it greatly benefits consumers, and it mirrors the BIPA's protectiveness. First, providing citizens with a private right of action allows them to receive concrete benefits from a business that violates BII. Unlike in other jurisdictions where consumers can only file complaints in the hopes that the entity will be fined by a governmental agency, the BII allows citizens to be compensated for a business' misuse of their data. Second, the fact that New York City followed Illinois's lead by providing this private right of action is noteworthy because it is so rare. While many states have adopted similar biometric privacy laws to BIPA, Illinois is currently the only state whose statute includes a private right of action for consumers.[159] New York City has shown with its inclusion of this provision that privacy localism can be employed to protect citizens' data when the state and federal legislatures fail to do so. Finally, the last substantial benefit of this is a fairly comprehensive law in that, unlike many other privacy laws, its application is not limited only to large companies with a certain revenue threshold or employee count. Instead, it applies to all commercial establishments within the city, giving it a broader reach.

Despite these benefits, BII is not all-encompassing and still maintains a few drawbacks. First, the law does not require commercial establishments to obtain written consent from customers in order to collect their biometric data.[160] This is a gap in the law because, although it requires commercial establishments to provide consumers notice that they are collecting biometric data, consumers do not explicitly consent.

154 Stransky, *supra* note 6.
155 *See* Stransky, *supra* note 6.
156 Stransky, *supra* note 6.
157 Stransky, *supra* note 6.
158 Stransky, *supra* note 6.
159 Shifrin & Tobin, *supra* note 132.
160 Stransky, *supra* note 6.

Instead, they implicitly consent by acknowledging the notice and still deciding to enter the establishment. Additionally, the "law does not limit the retention period biometric identifier information can be" held by the commercial establishment, "require the implementation of internal data processing policies, or require businesses to adhere to any specific security protocols."[161] This represents another hole in the ordinance because businesses can theoretically store consumer biometric data indefinitely. On top of that, the data is more vulnerable to attacks or hacks since entities are under no obligation under BII to secure the data they have collected. That being said, these requirements, in most cases, already apply to commercial establishments under the NY Stop Hacks and Improve Electronic Data Security Act, so entities still need to abide by some data protection provisions.[162]

Another pitfall of BII is that the notice requirement contained in the biometric law does not apply to the traditional employer-employee context.[163] Employees' biometric data would still be protected under the transactional prohibition provision, however, this part of the law is not overtly limited to the consumer context.[164] Additionally, BII does not apply to financial institutions either, as they are governed by other comprehensive privacy statutes such as the federal Gramm-Leach-Bliley Act.[165] This means that banks, such as the Citi branch store on West 23rd Street, that collect customers' biometric identifier information will not have to abide by the provisions of the BII. Finally, the downside to a private right of action is that it will likely spawn a plethora of litigation suits by individuals, like BIPA did when it first took effect.[166] This will require resources and significant time to settle disputes of this nature. BII, however, creates a clear and fair opportunity for commercial retailers to cure their violations, given the thirty-day window.[167] Thus, litigation will be stayed if the commercial establishment accused of violating BII corrects their violation expeditiously.

161 Stransky, *supra* note 6.

162 Stransky, *supra* note 6.

163 Stransky, *supra* note 6.

164 Stransky, *supra* note 6.

165 *See* Katy Liu, *GDPR Matchup: U.S. Financial Privacy Laws*, IAPP (Oct. 24, 2017), https://iapp.org/news/a/gdpr-matchup-us-financial-privacy-laws/.

166 Mia Farber, David R. Goldner & Eric R. Magnus, *Jackson Lewis Class Action Trends Report 2022: Biometric Privacy*, NAT'L LAW REV. (Feb. 18, 2022), https://www.natlawreview.com/article/jackson-lewis-class-action-trends-report-2022-biometric-privacy.

167 *Chapter 12: Biometric Identifier Information*, AMERICAN LEGAL PUBLISHING, *supra* note 142.

V. CONCLUSION

The use of biometric data has exploded as fast as technology has advanced, and consumers' physiological characteristics can now be utilized for a multitude of innovations.[168] However, the advancements and conveniences that this technology provides are accompanied by a number of risks and privacy concerns for consumers whose personal data is being manipulated.[169] When, and until, Congress decides to prioritize this issue and enact a comprehensive federal law that regulates the collection and use of all U.S. citizens' biometric data, states and local jurisdictions will need to continue to enact biometric privacy laws in order to address consumer concerns.[170] New York City can serve as a model jurisdiction for other large cities feeling the pressure from their constituents to regulate personal, private data. While New York City's biometric identifier law is nowhere near perfect, it is protective of its citizens, it provides for more transparency between citizens and the users of their data, and it provides citizens concrete steps to take if their data has been misused. More cities should be encouraged by the enactment of this legislation and should use it as a basis for enacting similar laws.

168 *See* Sava, *supra* note 1.
169 *See* Zarkowsky, *supra* note 3.
170 *See* Prescott, *supra* note 5.