Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 30 *XXX*
Number 3

Article 7

2020

The Prison of Convenience: The Need for National Regulation of Biometric Technology in Sports Venues

Kirsten Flicker
Fordham University School of Law, kflicker@law.fordham.edu

The Prison of Convenience: The Need for National Regulation of Biometric Technology in Sports Venues

Cover Page Footnote

J.D. Candidate, Fordham University School of Law, 2021; B.A. History, New York University, 2017. I would like to thank Professor Olivier Sylvain for his guidance and advice, as well as the IPLJ Editorial Board and staff for their feedback and editing.

The Prison of Convenience: The Need for National Regulation of Biometric Technology in Sports Venues

Kirsten Flicker*

In recent years, biometric data has crept its way into sports venues. In 2015, Major League Baseball began to use fingerprinting at stadium entrances. More recently, reporters have alerted spectators to the use of facial recognition technology in arenas such as Madison Square Garden. Proponents of these developments insist that the technology conveniences spectators, increases venue security, and enhances the overall spectator experience. Yet these claims fail to take into account the possibility of irremediable data breaches, the inaccuracies in facial recognition technology, and the privacy and unfair and deceptive trade practice concerns this technology raises. Further, there is an overarching concern about the lack of regulation of biometric data. This Note examines the benefits and concerns of biometric technology as well as the options for regulating it. Ultimately, this Note finds that national regulation of biometric technology would best serve sports spectators. In particular, this Note recommends a uniform standard for venues in all states that requires transparency of biometric data policies, and protection of spectator data.

* J.D. Candidate, Fordham University School of Law, 2021; B.A. History, New York University, 2017. I would like to thank Professor Olivier Sylvain for his guidance and advice, as well as the IPLJ Editorial Board and staff for their feedback and editing.

INTRODUCTION

Going to a Mets game used to begin with a long line and an usher checking paper tickets. For blacklisted fans, it meant passing through the gates, unnoticed.[1] A Mets game used to mean vendors parading through the grandstands and exchanging cracker jacks and beer for cash. Now, in the modern era of biometrics, going to a Mets game begins with having your fingerprint taken at a CLEAR booth.[2] Facial recognition identifies blacklisted fans and denies them entry.[3] Beer is purchased at a cashier-less, artificial intelligence ("AI")-powered kiosk.[4] Without many even realizing it, biometric technology has redesigned the experience of going to a ballgame from start to finish.

Major League Baseball ("MLB") is not the only professional sports league whose stadiums have embraced biometric technology.

---

1 A blacklisted fan is a fan who is banned from the venue due to disreputable behavior. *See Blacklist*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/blacklist [https://perma.cc/G25P-MXUS].

2 *See Sports*, CLEAR, https://www.clearme.com/sports [https://perma.cc/C8B7-CZNC].

3 *See* Steve Lasky, *Fear Strikes Out*, SECURITY INFO WATCH (Aug. 24, 2018), https://www.securityinfowatch.com/access-identity/access-control/article/12426642/security-at-citi-field-ups-its-game-with-a-blend-of-technology-and-staff-experience [https://perma.cc/5QM8-HCDP].

4 *See Mets Add Self-Checkout Kiosk to Citi Field*, BALLPARK DIG. (Sept. 24, 2019), https://ballparkdigest.com/2019/09/24/mets-add-self-checkout-kiosk-to-citi-field/ [https://perma.cc/3N6T-VUAU].

From Madison Square Garden for the New York Knicks and New York Rangers[5] to CenturyLink Field for the Seattle Seahawks,[6] sports venues around the country use biometrics such as fingerprints and facial recognition to reimagine the sports spectator experience.[7] Ticketing and concession sales are powered by fingerprinting,[8] and advertisements and music are selected using facial recognition.[9] As biometric technology continues to advance, sports venues continue to find innovative ways to integrate the technology into the game-going experience. Many of these uses may seem glamorous, such as reduced time spent waiting in lines, and enhanced security.[10] Yet, the personal and irreplaceable nature of biometric data makes it particularly sensitive to breaches.[11] Further, evidence of inaccuracies in facial recognition raises serious questions about this technology's effectiveness.[12]

This Note highlights how biometric data such as fingerprints and facial recognition is being used in sports venues, and, at present, is largely unregulated. Part I explains what biometric data is and how sports venues utilize it. This Part focuses on current fingerprinting and facial recognition uses, as well as uses that venues are expected to implement in the near future. Part II examines the advantages and disadvantages of biometric technology in sports venues. First, it discusses the benefits of increased convenience, security, and innovative spectator experience. Next, it comments on the proof of

---

5 *See* Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, N.Y. TIMES (Mar. 13, 2018), https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html [https://perma.cc/8S9M-L4HD].

6 *See CLEAR Partners with Seattle Seahawks, Sounders & Mariners to Launch Industry-Leading Biometric Payments & ID Check for Fast, Frictionless Concessions*, BUS. WIRE (Aug. 6, 2018, 3:39 PM), https://www.businesswire.com/news/home/20180806005577/en/CLEAR-Partners-Seattle-Seahawks-Sounders-Mariners-Launch [https://perma.cc/R87N-93E3] [hereinafter *CLEAR Partners with Seattle Seahawks*].

7 *See* Draper, *supra* note 5.

8 *See Sports*, *supra* note 2.

9 *See* Jessica Golden & Eric Chemi, *Sports Teams Are Using Facial Recognition to Learn More About Their Fan Bases*, CNBC (Apr. 21, 2018, 11:42 PM), https://www.cnbc.com/2018/04/21/facial-recognition-helps-teams-and-advertisers-learn-about-fans.html [https://perma.cc/3GSH-LVE6].

10 *See infra* Part II.A.

11 *See infra* Part II.B.1, 3.

12 *See infra* Part II.B.2.

inaccuracy in facial recognition, and the privacy, security, and unfair and deceptive trade practice concerns that have been noted about the use of this technology.

Part III then reviews the existing biometric statutes and regulations and examines some proposed regulations. This Part first considers the recent urge for a moratorium on facial recognition. Then, it discusses the proposed federal statute, federal guidelines, the European Union ("EU") statute, and current and proposed state statutes. In particular, this Part focuses on how these statutes and regulations address transparency, security exceptions, data protection, deletion, and remedies for violations. Finally, Part IV recommends national regulation of biometrics in sports venues in order to maximize the technology's benefits and minimize its detriments. Overall, this Note recommends that this nationwide regulatory scheme emphasize data protection and meaningful notice and consent for all uses of biometrics.

I. BIOMETRIC DATA IN SPORTS VENUES

A. What is Biometric Data?

Biometrics are the "measurement and analysis of unique physical or behavior characteristics."[13] Common forms of biometric data include fingerprints, eyes (specifically irises and retinas), DNA, heart rates, and facial features.[14] Biometric data is a type of personally identifiable information ("PII"), defined by the Office of Management and Budget as "information which can be used to distinguish or trace an individual's identity."[15] Wearable technology

---

[13] *Biometrics*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/biometrics [https://perma.cc/7JMR-L7G8].

[14] *See Biometric*, LEXICO, https://www.lexico.com/en/definition/biometric [https://perma.cc/5HCJ-FMPB]; *Types of Biometrics*, BIOMETRICS INST., https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/ [https://perma.cc/TEJ4-YLLQ]; Lauren Stewart, *Big Data Discrimination: Maintaining Protection of Individual Privacy Without Disincentivizing Businesses' Use of Biometric Data to Enhance Security*, 60 B.C. L. REV. 349, 356 n.49 (2019).

[15] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, MEMORANDUM FROM CLAY THOMPSON III, DEPUTY DIRECTOR FOR MANAGEMENT, SAFEGUARDING AGAINST AND RESPONDING TO THE BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (May 22, 2007). In fact, on July 26, 2019, New York Governor Andrew Cuomo signed the Stop Hacks and

such as Fitbits,[16] DNA tests such as 23andMe,[17] and iris scans like NEXUS Global Entry at airports[18] measure these "unique, permanent and collectable" biological characteristics.[19]

Biometric data both identifies individuals and verifies individual identities.[20] Identification answers the question "who is this person?" whereas verification answers the question "is this person who they say they are?"[21] When used to identify, an individual's biometric data is compared to a database to determine if it matches any of the existing profiles.[22] Law enforcement employs this technique routinely.[23] For example, border security uses live facial recognition to identify threats in real-time.[24] Alternatively, individuals use verification when they need to prove their identity.[25] This technique is a part of everyday tasks, like unlocking a smartphone

---

Improve Electronic Data Security ("SHIELD") Act, which includes biometric data in its definition of PII. *See* S.B. S5575B, 2019–20 Leg. Sess. (N.Y. 2019); Philip Gordon & Jennifer Taiwo, *The New York SHIELD Act: What Employers Need to Know*, SHRM (Aug. 28, 2019), https://www.shrm.org/resourcesandtools/legal-and-compliance/state-and-local-updates/pages/new-york-shield-act.aspx [https://perma.cc/3H6J-UJTE].

16 *See Our Technology*, FITBIT, https://www.fitbit.com/technology [https://perma.cc/379Z-QNFC].

17 *See How It Works*, 23ANDME, https://www.23andme.com/howitworks/ [https://perma.cc/VYL3-QPRG].

18 *See NEXIS Iris Scan Locations*, U.S. IMMIGR. VISA & TRAVEL, https://usa.immigrationvisaforms.com/travel/nexus-iris-scan-locations [https://perma.cc/9CP9-AWZP].

19 Kim Porter, *Biometrics and Biometric Data: What Is It and Is It Secure?*, NORTON, https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html [https://perma.cc/3HB8-GLY2].

20 *See* Stephen Mayhew, *Explainer: Verification vs. Identification Systems*, BIOMETRIC UPDATE, https://www.biometricupdate.com/201206/explainer-verification-vs-identification-systems [https://perma.cc/UVK3-UD7H]; *see also Biometrics: Authentication and Identification—2020 Review*, GEMALTO, https://www.gemalto.com/govt/inspired/biometrics [https://perma.cc/R3Z6-AQH5].

21 Mayhew, *supra* note 20.

22 *See id*.

23 *See id*.

24 *See id*.

25 *See id*.

using face unlock.[26] Law enforcement also uses this method to authenticate documents such as passports.[27]

Beyond identification and verification, entities can use biometric data for a third purpose: classification. This use of facial recognition is common; as facial recognition software scans a crowd, the computer program measures characteristics such as spacing of the eyes and bridge of the nose.[28] The technology then uses these characteristics to create a "digitally recorded representation" of people's facial features.[29] These "faceprints" are then used to determine certain characteristics such as gender and age.[30]

B. Use of Biometric Data in Sports Venues

1. Fingerprinting

MLB has pioneered biometric ticketing through the use of fingerprinting. CLEAR, the "official biometric identity and ticketing partner of the MLB," operates special security clearance checkpoints at thirteen of the thirty MLB ballparks.[31] CLEAR lanes expedite the check-in process by using fingerprints to identify ticketed fans.[32] CLEAR expanded its biometric ticketing to three

---

[26] *See What Is Facial Recognition on a Phone?*, XFINITY DISCOVERY HUB (Jan. 31, 2019), https://www.xfinity.com/hub/mobile/facial-recognition-on-phone [https://perma.cc/H353-HZES].

[27] *See* GEMALTO, *supra* note 20.

[28] *See Facial Recognition: Top 7 Trends*, GEMALTO (last updated Jan. 22, 2020), https://www.gemalto.com/govt/biometrics/facial-recognition [https://perma.cc/KHW4-4UFP].

[29] *Faceprint*, COLLINS DICTIONARY, https://www.collinsdictionary.com/us/dictionary/english/faceprint [https://perma.cc/FN7P-4RE5].

[30] *Id.*; *see also* FED. TRADE COMM'N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHS. (Oct. 2012), *available at* https://www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies [https://perma.cc/9NZ5-DBU8] [hereinafter FTC, BEST PRACTICES].

[31] *See Sports*, *supra* note 2; *see also* Alan Levin & Jonathan Levin, *Sports Stadiums and Arenas Increase High-Tech Security Tools*, CHI. TRIB. (Jan. 1, 2017, 10:01 AM), https://www.chicagotribune.com/sports/breaking/ct-stadium-security-spt-20170101-story.html [https://perma.cc/VY2L-YCHD]. CLEAR is a biometric security platform that operates expedited security checkpoints in over sixty airports, stadiums, and other venues around the United States. *See Where We Are*, CLEAR, https://www.clearme.com/where-we-are [https://perma.cc/8JYZ-CQHW].

[32] *See About Us*, CLEAR, https://www.clearme.com/about-us/ [https://perma.cc/FEN7-3MPA].

Major League Soccer arenas, two National Football League ("NFL") stadiums, and four National Basketball Association arenas.[33] CLEAR aims to provide "frictionless fan entry,"[34] and, according to its website, serves as a safe, simple, and secure alternative to traditional paper ticketing.[35]

In the spectator sports market, CLEAR has higher aspirations than just arena entry—it is expanding to concession sales.[36] In 2018, the Seattle Seahawks, Mariners, and Sounders FC implemented CLEAR for concession purchases.[37] Fingerprints serve as a means both to pay and to verify age.[38] The goal is to optimize time spent watching the game and to reduce time spent waiting in lines[39] by "creat[ing] a fully walletless experience."[40] Seattle fans' positive reception of biometric concessions has laid the groundwork for biometric concessions in stadiums around the country,[41] starting with the Mets' Citi Field.[42] Citi Field took this technology a step further by opening a "Walk Thru Bru" store that eliminates the need

---

33 *See Sports*, *supra* note 2.

34 Stephen Mayhew, *More MLB Stadiums Deploy CLEAR Biometric Tech for Frictionless Fan Entry*, BIOMETRIC UPDATE (Apr. 4, 2019), https://www.biometricupdate.com/201904/more-mlb-stadiums-deploy-clear-biometric-tech-for-frictionless-fan-entry [https://perma.cc/4GP5-ZWDB].

35 *See About Us*, *supra* note 32.

36 *See CLEAR Partners with Seattle Seahawks*, *supra* note 6.

37 *See id*.

38 *See CLEAR Adds Biometrics to Safeco Field Admissions, Concessions*, BALLPARK DIG. (Aug. 9, 2018), https://ballparkdigest.com/2018/08/09/clear-adds-biometrics-to-safeco-field-admissions-concessions/ [https://perma.cc/AA9U-RDZ7].

39 *See id*.

40 Joe Favorito, *Getting a CLEAR Picture of Biometric Data in Sports Business*, SPORTS MARKETING & PR ROUNDUP (July 13, 2018), https://joefavorito.com/2018/07/13/getting-a-clear-picture-of-biometric-data-in-sports-business/ [https://perma.cc/8VMD-ZH6H].

41 *See* Jared Dubin, *Seahawks Will Allow Fans to Buy Beer, Concessions Using Only Their Fingerprint*, CBS SPORTS (Aug. 7, 2018, 2:32 PM), https://www.cbssports.com/nfl/news/seahawks-will-allow-fans-to-buy-beer-concessions-using-only-their-fingerprint/ [https://perma.cc/J9S2-99GP].

42 *See* Chris Burt, *Clear to Provide Biometrics for Concessions Purchases at New York's Citi Field*, BIOMETRIC UPDATE (Sept. 24, 2019), https://www.biometricupdate.com/201909/clear-to-provide-biometrics-for-concessions-purchases-at-new-yorks-citi-field [https://perma.cc/EJ96-BMLH]. Further, although currently CLEAR only uses fingerprinting at sports venues, it has the capacity to use iris scans. CLEAR uses iris scans in airports, which raises the possibility that it will expand this practice to stadiums and arenas. *See You Are the Best ID*, CLEAR, https://www.clearme.com [https://perma.cc/C238-GZWZ].

for both wallets and cashiers.[43] Fans select their items, place them on an AI-powered self-checkout kiosk, and pay using CLEAR's fingerprinting machine.[44] Additionally, the New York Jets, the San Francisco 49ers, and Barclays Center (home of the Brooklyn Nets) all partner with IDEMIA, the company behind TSA PreCheck.[45] IDEMIA's IdentoGO strives to use biometric data to provide "fast pass"[46] entrance for "trusted fans."[47]

Biometric payment may seem like a recent phenomenon, but companies have previously attempted to use biometric payment to no avail. In 2002, Pay By Touch created a payment processing system that combined biometric identification with electronic financial transactions.[48] Prominent public figures, including five former NFL quarterbacks, funded the company.[49] However, frequent consumer misidentifications and false rejections undermined confidence in the technology.[50] Thus, Pay By Touch's efforts never came to fruition, and the company declared bankruptcy in

---

43 *Mets Add Self-Checkout Kiosk to Citi Field*, *supra* note 4.

44 *See id*.

45 *See Idemia to Bring TSA Pre✓ Services to Fenway Sports Group*, BIG12FANATICS (May 11, 2018), https://big12fanatics.com/idemia-to-bring-tsa-pre✓-services-to-fenway-sports-group/ [https://perma.cc/2PV8-3643]; *IDEMIA to Bring Its IdentoGO Program to Barclays Center*, IDEMIA (Mar. 15, 2018), https://www.idemia.com/press-release/idemia-bring-its-identogo-program-barclays-center-2018-03-15 [https://perma.cc/5BXS-R2RB]; Draper, *supra* note 5. TSA PreCheck is a program that allows "low-risk" travelers to pass through expedited security checkpoints when traveling through United States airports. The U.S. Transportation Security Administration ("TSA") of the U.S. Department of Homeland Security operates this program. The TSA conducts background checks of all applicants before it grants them access to the program. Julia Kagan, *TSA PreCheck*, INVESTOPEDIA (last updated Sept. 18, 2019), https://www.investopedia.com/terms/t/tsa-pre.asp [https://perma.cc/ER8Y-74VZ].

46 *Idemia to Bring TSA Pre✓Services to Fenway Sports Group, supra* note 45.

47 Michael Loré, *IdentoGO by IDEMIA Makes Your Game Day Experience Safer and More Efficient*, CULTURE TRIP (Jan. 4, 2018), https://theculturetrip.com/north-america/usa/articles/identogo-by-idemia-makes-your-game-day-experience-safer-and-more-efficient/ [https://perma.cc/MVE9-3NKW].

48 *See Failure Story: What Happened to Pay By Touch?*, MEDICI (Apr. 20, 2015), https://gomedici.com/failure-story-what-happened-to-pay-by-touch [https://perma.cc/P7WX-2CJP].

49 *See id*.

50 *See id*.

2007.[51] Over the past decade, biometric identification technology has improved, and the idea of biometric payment has been revived.[52]

2. Facial Recognition

Though fingerprinting is a relatively new practice in the spectator sports world, stadiums have used facial recognition as early as the turn of the century.[53] In 2001, the Raymond James Stadium in Tampa Bay, Florida hosted Superbowl XXXV.[54] Unbeknownst to spectators, the Tampa Police Department used a surveillance system called FaceTrac to scan the crowds and identify criminals and criminal suspects.[55] Although the police department did not arrest anybody, FaceTrac reported nineteen matches with its criminal database.[56] Though the police department's intention of providing optimal security for the fans may have been honorable, many civilians were disconcerted to learn that the police had effectively spied on them.[57] The American Civil Liberties Union ("ACLU") contributed to the criticism of this "Orwellian" experiment by labeling the event the "Snooper Bowl."[58]

---

51 *See id*.

52 For example, it is easier to capture high-quality face images as image sensors become smaller and cheaper. *See* Anil K. Jain, Karthik Nandakumar & Arun Ross, *50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities*, PATTERN RECOGNITION LETTERS 79, 89–90 (Jan. 12, 2016).

53 *See Super Bowl Snooping*, N.Y. TIMES (Feb. 4, 2001), https://www.nytimes.com/2001/02/04/opinion/super-bowl-snooping.html [https://perma.cc/MKN2-Z33F].

54 *See* Mary Huhn, *Just a Face in the Crowd?—Superbowl Kicked Off the Use of Face Recognition Software—But Is This an Invasion of Privacy?*, N.Y. POST (June 26, 2001), https://nypost.com/2001/06/26/just-a-face-in-the-crowd-superbowl-kicked-off-the-use-of-face-recognition-software-but-is-this-an-invasion-of-privacy/ [https://perma.cc/DR94-8ULE].

55 *See Super Bowl Snooping*, *supra* note 53.

56 *See* Lev Grossman, *Welcome to the Snooper Bowl*, TIME (Feb. 4, 2001), http://content.time.com/time/magazine/article/0,9171,98003,00.html [https://perma.cc/9M2X-ND45].

57 *See* Dana Canedy, *Tampa Scans the Faces in Its Crowds for Criminals*, N.Y. TIMES (July 4, 2001), https://www.nytimes.com/2001/07/04/us/tampa-scans-the-faces-in-its-crowds-for-criminals.html [https://perma.cc/6HXU-ZUER].

58 Grossman, *supra* note 56; *see also* Huhn, *supra* note 54.

Despite this initial backlash, sporting arenas continue to use facial recognition.[59] For example, a handful of venues use this technology to improve security. Madison Square Garden, for instance, installed crowd scanners at entrance security checkpoints.[60] Additionally, the American Airlines Center in Dallas, Texas uses facial recognition outside team locker rooms and throughout the arena.[61] The Sacramento Kings' Golden 1 Center's practice facility uses facial recognition for players and staff, but the arena has not yet expanded this technology to spectators.[62]

As mentioned, use of facial recognition is not limited to identification—it also verifies people.[63] For example, JetBlue recently opened its first "e-gate" in the John F. Kennedy ("JFK") airport in Queens, New York.[64] Instead of a boarding pass and passport, travelers use their faces to board flights.[65] U.S. Customs and Border Protection operates this verification system.[66] Once the system verifies the traveler, it deletes the information from the system within a few hours.[67] Jet Blue's JFK e-gate follows the example of other airports, such as Atlanta, Georgia's Hartsfield-Jackson Airport, where Delta operates an entire "biometric terminal."[68] Delta's biometric terminal uses facial recognition at check in, bag drop,

---

59 *See* Draper, *supra* note 5.

60 *See id.*

61 *See id*.

62 *See id*.

63 *See* Melissa Locker, *Major League Baseball Tickets Are Going Biometric in 2019*, FAST CO. (July 12, 2018), https://www.fastcompany.com/90201535/major-league-baseball-tickets-are-going-biometric-in-2019 [https://perma.cc/N5EK-CZRQ].

64 Geoffrey A. Fowler*, Don't Smile for Surveillance: Why Airport Face Scans Are a Privacy Trap*, WASH. POST (June 10, 2019), https://www.washingtonpost.com/technology/2019/06/10/your-face-is-now-your-boarding-pass-thats-problem/ [https://perma.cc/D7QB-2UL7].

65 *See id*.

66 *See* Jummy Olabanji, *'Very Unsettling': Facial Recognition Technology at Airports Sparks Privacy Concerns*, NBC N.Y. (Apr. 24, 2019, 2:27 PM), https://www.nbcnewyork.com/news/local/Facial-Recognition-Technology-at-Airports-Sparks-Privacy-Concerns-508974851.html [https://perma.cc/6HMV-YGS5].

67 *See id*.

68 Fowler, *supra* note 64 (quoting Lori Aratani*, Your Face Is Your Boarding Pass at This Airport*, WASH. POST (Dec. 4, 2018, 2:25 PM), https://www.washingtonpost.com/nation/2018/12/04/your-face-is-your-boarding-pass-this-airport/ [https://perma.cc/9NUU-37N5]).

security, and boarding.[69] While CLEAR's fingerprint verification currently dominates sports venue biometric ticketing, facial recognition ticketing is another viable possibility in this area.[70]

Sports stadiums could also be the next venue for Amazon's "just walk out technology."[71] Amazon is gradually creating a chain of cashierless stores.[72] To enter the store, customers scan the QR code in their Amazon Go app.[73] Then, cameras placed around the store determine what items customers select and the app charges them as they exit, which allows customers to forego checkout.[74] Though there were rumors that these cameras use facial recognition,[75] Amazon denies this claim.[76] Moreover, RBC Capital Markets analysts estimate that cashierless stores bring in approximately 50% more revenue than conventional stores.[77] Amazon is not the first company to use this technology—startups such as Zippin also operate cashierless stores.[78] Promising that automated checkout will improve profit margins, these startups have already pitched their technology to sports stadiums.[79] These developments suggest that cashierless, checkout-free concessions could soon become a reality at sports stadiums throughout the United States.

---

69 *See id*.

70 *See* Locker, *supra* note 63.

71 Maggie Tillman, *What Is Amazon Go, Where Is It, and How Does It Work?*, POCKET-LINT (Feb. 18, 2019), https://www.pocket-lint.com/phones/news/amazon/139650-what-is-amazon-go-where-is-it-and-how-does-it-work [https://perma.cc/F6XB-2VFL].

72 *See* Sebastian Herrera, *Silicon Valley Takes on Amazon's Cashierless 'Go' Stores*, WALL STREET J. (Oct. 14, 2019, 5:30 AM), https://www.wsj.com/articles/silicon-valley-takes-on-amazons-cashierless-go-stores-11571045401 [https://perma.cc/VQ2B-F9BV].

73 *See* Tillman, *supra* note 71.

74 *See id*.

75 *See id*.

76 *See* Drew Harwell & Abha Battaral, *Inside Amazon Go: The Camera-Filled Convenience Store that Watches Your Back*, WASH. POST (Jan. 22, 2019, 6:00 PM), https://www.washingtonpost.com/news/business/wp/2018/01/22/inside-amazon-go-the-camera-filled-convenience-store-that-watches-you-back/ [https://perma.cc/DF5U-L92W].

77 *See* Rani Molla, *Amazon's Cashierless Go Stores Could Be a $4 Billion Business by 2021, New Research Suggests*, VOX (Jan. 4, 2019, 10:33 AM), https://www.vox.com/2019/1/4/18166934/amazon-go-stores-revenue-estimates-cashierless [https://perma.cc/KK5E-38TN].

78 *See* Tillman, *supra* note 71.

79 The startups also promised sports stadiums that automated checkout will reduce theft. *See* Herrera, *supra* note 72.

3. Market for User Data

Uses of biometric data in sports venues extend beyond security and a frictionless spectator experience—there is also a market for user data among vendors and advertisers. Every producer desires information about their consumers so as to better target advertisements and consequently generate business.[80] While it is possible to track the characteristics of initial ticket purchasers, that data becomes moot once tickets enter the secondary market.[81] Using facial scanning even just to identify simple characteristics such as the age and gender of spectators can profoundly impact the advertisements shown at venues.[82] Fancam, one of the largest companies that sells this technology, states that collecting this data can be used to attract sponsors and allow them to effectively plan their advertisements.[83] Teams such as the New York Rangers and New England Patriots already use Fancam technology for advertising in their venues.[84] Additionally, teams use facial recognition technology to profile spectators to determine what music to play.[85] For example, if the technology notes that the fans at a particular game are younger and disproportionately female, the team can adjust the music accordingly.[86] Further, if concession and merchandise purchases are tracked using fingerprinting, vendors can target advertisements at consumers based on their purchase patterns.[87] Facial scanning can track a customer's facial expressions when deciding what concessions and merchandise to buy.[88] This information about

---

80 *See* Draper, *supra* note 5.

81 *See id*.

82 *See id*. Age is detected by mapping out a series of facial points, such as corners of the eyes and lips. These points are then run through an algorithm to determine that person's age. *See Age Detection*, ACTI, https://www.acti.com/technologies/age-detection [https://perma.cc/9JYR-BMWG].

83 *See* Golden & Chemi, *supra* note 9.

84 *See id*.

85 *See id*.

86 *See id*.

87 *See* Barry Levine, *Viant Adds Purchase-Based Targeting for CPG Ads*, MARTECH TODAY (Aug. 22, 2018, 3:42 PM), https://martechtoday.com/viant-adds-purchase-based-targeting-for-cpg-ads-223129 [https://perma.cc/9HX5-RX9K].

88 *See* 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, 632 (2019).

consumer reactions could be just as important as actual purchases when determining what to sell and how to advertise these products.[89]

Targeted advertisements are not a new phenomenon. Online advertisers are able to collect data and target advertisements based on individual consumer behavior.[90] They base these advertisements on a variety of data points including demographics and browsing behavior.[91] As technology advances, advertisers have the capacity to extend targeted advertisements beyond the internet and into real-time.[92] For example, beginning in 2012, Nomi Technologies used media access control ("MAC") addresses in mobile devices to track customers in stores.[93] This allowed Nomi to collect data points such as the length of a customer's stay in the store and whether or not that customer had visited the store before.[94] Biometric data can similarly provide useful consumer data points. For example, purchase trends and crowd demographics can be tracked using both fingerprints and facial scanning.[95] Then, teams can use this data to attract particular advertisers,[96] and the advertisers can use these data points to select

---

89 *See id*.

90 *See* Rebecca Walker Reczek, Christopher Summers & Robert Smith, *Targeted Ads Don't Just Make You More Likely to Buy—They Can Change How You Think About Yourself*, HARV. BUS. REV. (Apr. 4, 2016), https://hbr.org/2016/04/targeted-ads-dont-just-make-you-more-likely-to-buy-they-can-change-how-you-think-about-yourself [https://perma.cc/WF67-GTRH].

91 *See* Cydney Hatch, *How Targeted Advertising Works*, DISRUPTIVE ADVERT. (Dec. 13, 2018), https://www.disruptiveadvertising.com/marketing/targeted-advertising/ [https://perma.cc/DDV9-XVST]; Reczek, Summers & Smith, *supra* note 90.

92 *See* Draper, *supra* note 5.

93 *See* Press Release, Fed. Trade Comm'n, Retail Tracking Firm Settles FTC Charges It Misled Consumers About Opt Out Choices (Apr. 23, 2015), https://www.ftc.gov/news-events/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers [https://perma.cc/5FVE-NYEF] [hereinafter FTC Press Release 2015].

94 *See id*. However, not everybody viewed Nomi's services favorably. The FTC charged Nomi with misleading consumers by promising opt-out mechanisms in stores. The FTC and Nomi reached a settlement in 2015, agreeing that Nomi was prohibited from future misrepresentations. *See id*.

95 *See* Draper, *supra* note 5.

96 *See* Golden & Chemi, *supra* note 9.

the best advertisements for that event's unique crowd.[97] Since effective advertising increases profit, access to this data is invaluable.[98]

II. SHOULD SOMEBODY INTERVENE?

Biometric data's "unique, permanent" nature and ability to identify, verify, and classify individuals have many advantages in sports venues, but this technology also raises numerous concerns.[99] Biometric identifiers can reduce time spent waiting in lines, provide heightened security, and enable a customized experience. However, biometric identifiers are personal metrics susceptible to deceitful or unfair trade practices,[100] and breaches of biometric data can have sobering implications.[101] Additionally, recent studies have revealed the inaccuracies of facial recognition.[102] Part II.A details how this technology can improve the sport spectator experience, while Part II.B addresses the threats that could result from unregulated use of biometric data.

---

97 Stores such as Target have experimented with using biometric data for advertising purposes. Some stores have even merged their security and advertising departments since both can use the same technology. *See* Nick Tabor, *Smile! The Secretive Business of Facial-Recognition Software in Retail Stores*, N.Y. MAG. (Oct. 20, 2018), http://nymag.com/intelligencer/2018/10/retailers-are-using-facial-recognition-technology-too.html [https://perma.cc/V2TG-VVC2].

98 *See* Jeremy Bradley, *The Impact of Advertising & Sales Promotion in Revenue*, CHRON, https://smallbusiness.chron.com/impact-advertising-sales-promotion-revenue-59840.html [https://perma.cc/UX8X-6LLY]. Many news sources describe data as "the oil of the digital era." *The World's Most Valuable Resource Is No Longer Oil, But Data*, ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [https://perma.cc/8L5K-RBHT]; *see also* Gabriel J.X. Dance, Michael LaForgia, & Nicholas Confessore, *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html [https://perma.cc/P8T3-TTGH].

99 Porter, *supra* note 19.

100 *See infra* Part II.B.4.

101 *See infra* Part II.B.1.

102 *See infra* Part II.B.2.

A. Benefits of Biometric Data in Sports Venues

1. Biometrics Increase Spectator Convenience

The Seattle Mariners boast that using CLEAR's biometric products maximizes the amount of time that fans spend in their seats and minimizes the amount of time that fans spend waiting in lines.[103] CLEAR advertises frictionless entry,[104] and IDEMIA promotes its fast-pass entrance at Barclays Center in Brooklyn, New York.[105] Without wallets, fans do not fumble for tickets, credit cards, or IDs.[106] Further, while fans can forget to bring these items, they cannot forget to bring their biometric traits.[107] These identifiers are intrinsic in every human; thus, using biometric identifiers eliminates the need to remember multiple items, such as tickets and credit cards, just to attend a game.[108] Walletless lines also reduce the burden on the venue's gate staff.[109] Overall, biometric ticketing and concessions minimize the long lines traditionally characteristic of attending a sporting event.

2. Biometric Technology Promotes Safety and Security

Private security companies and law enforcement are increasing their use of biometric data. For example, in 2018, police used DNA from a genealogy database to close a four-decades-old investigation.[110] The investigators used DNA to piece together a family tree

---

[103] *See CLEAR Adds Biometrics to Safeco Field Admissions, Concessions*, *supra* note 38 (interviewing the Mariners' Senior Vice President of Baseball Operations, Trevor Gooby).

[104] *See CLEAR Adds Biometrics to Safeco Field Admissions, Concessions*, *supra* note 38 (interviewing CLEAR CEO Caryn Seidman Becker).

[105] *See Idemia to Bring TSA Pre✓Services to Fenway Sports Group*, *supra* note 45.

[106] *See generally* Dubin, *supra* note 41.

[107] *See* Porter, *supra* note 19.

[108] *See id*.

[109] *See* David Broughton, *NYC Biometric Security Firm Helps Sports Venues Speed Fans Through Gates*, N.Y. BUS. J., (Dec. 1, 2017, 12:12 PM), https://www.bizjournals.com/newyork/news/2017/12/01/nyc-biometric-security-firm-helps-sports-venues.html [https://perma.cc/6NNR-7UG8].

[110] *See* Justin Jouvenal, *To Find Alleged Golden State Killer, Investigators First Found His Great-Great-Great-Grandparents*, WASH. POST (Apr. 30, 2018), https://www.washingtonpost.com/local/public-safety/to-find-alleged-golden-state-killer-investigators-first-found-his-great-great-great-grandparents/2018/04/30/3c865fe7-dfcc-4a0e-b6b2-0bec548d501f_story.html [https://perma.cc/7VS5-HL2H].

and arrest a notorious burglar, rapist, and murderer nicknamed the Golden State Killer.[111] In addition to DNA, law enforcement officers across the country are using facial recognition technology to solve crimes thought to have gone cold.[112] For example, the police recently caught an attempted murderer in Central Indiana with the aid of facial recognition.[113] Clare Garvie, a scholar from the Georgetown Law Center on Privacy & Technology, relied on internal police documents to determine that from 2010 through 2016, facial recognition technology assisted police in arresting over 2,800 people.[114] This technology is also used internationally. In 2018, Iraqi authorities used fingerprints and facial data to identify "three high-level terrorist suspects."[115] Similar technology is utilized at arenas to increase security at sporting events.

Sports venues employ facial recognition to identify criminals and criminal suspects. For example, in 2018, facial recognition technology in the Nanchang International Sports Center in Jiangxi province, China led to the arrest of a suspect wanted by the police.[116] Additionally, heavily populated venues are prominent targets for shooters and terrorists.[117] In an era of frequent shootings and

---

111 *See id*.

112 *See* Julie Bosman & Serge. F. Kovaleski, *Facial Recognition: Dawn of Dystopia, or Just the New Fingerprint?*, N.Y. TIMES (May 18, 2019), https://www.nytimes.com/2019/05/18/us/facial-recognition-police.html [https://perma.cc/Q2N7-VH3D].

113 *See id*.

114 *Id*.

115 *Biometrics and Battlefield Data Help Police to Identify Terrorists*, INTERPOL, https://www.interpol.int/en/Crimes/Terrorism/Identifying-terrorist-suspects [https://perma.cc/9ATK-EEJ5].

116 *See* Amy B Wang, *A Suspect Tried to Blend in With 60,000 Concertgoers. China's Facial-Recognition Cameras Caught Him*, WASH. POST (Apr. 13, 2018, 3:25 PM), https://www.washingtonpost.com/news/worldviews/wp/2018/04/13/china-crime-facial-recognition-cameras-catch-suspect-at-concert-with-60000-people/ [https://perma.cc/5SB8-QXGN].

117 *See* JOHN D. WOODWARD, JR., SUPERBOWL SURVEILLANCE: FACING UP TO BIOMETRICS 3 (RAND 2001). Some notable examples include the bombing at Ariana Grande's concert at the Manchester Arena in London, England, the shooting at the Route 51 Harvest festival in Las Vegas, Nevada, and the bombings at the 1996 Summer Olympics at Centennial Olympic Park in Atlanta, Georgia. *See Ariana Grande Breaks Down Talking About Manchester Arena Attack*, BBC (Aug. 19, 2018), https://www.bbc.com/news/newsbeat-45239228 [https://perma.cc/LZG6-QRD8]; Andrew Blankstein, Pete Williams, Rachel Elbaum & Elizabeth Chuck, *Las Vegas Shooting: 59 Killed and More Than 500 Hurt Near Mandalay Bay*, NBC NEWS (last updated Oct. 2, 2017, 10:33 PM),

terrorist attacks, effective security measures at public venues are of paramount importance.[118] Facial recognition systems help minimize security risks by scanning crowds to identify criminals and criminal suspects before an attack occurs.[119]

These systems also capture smaller-scale criminals, such as merchandise thieves.[120] Facial recognition systems serve as advanced surveillance systems that can both document the theft and identify the culprit.[121] Many retail stores already use facial recognition to prevent shoplifting.[122] FaceFirst, a facial recognition software company,[123] states that it reduced retailer losses by up to 34% and in-store violence by up to 91%.[124] Even if no crimes are actually committed, knowledge that a venue uses a facial recognition system by itself could deter would-be lawbreakers from committing crimes, especially if venues actively notify attendees that facial recognition technology is being utilized.[125]

---

https://www.nbcnews.com/storyline/las-vegas-shooting/las-vegas-police-investigating-shooting-mandalay-bay-n806461 [https://perma.cc/6RRT-SM94]; *Olympic Park Bombing Fast Facts*, CNN (Aug. 11, 2019), https://www.cnn.com/2013/09/18/us/olympic-park-bombing-fast-facts/index.html [https://perma.cc/TEC3-9GHP].

118 *See* Bonnie Berkowitz et al., *More and Deadlier: Mass Shooting Trends in America*, WASH. POST (Aug. 5, 2019), https://www.washingtonpost.com/nation/2019/08/05/more-deadlier-mass-shooting-trends-america/?noredirect=on [https://perma.cc/83DX-TN95]; *see also* Jorge Martinez, *Major League Security: Overcoming Legal Challenges of Sporting Event Security Systems*, 2 U. MIAMI NAT'L SEC. & ARMED CONFLICT L. REV. 197, 200 (2012).

119 *See Super Bowl Snooping*, *supra* note 53.

120 *See* Tabor, *supra* note 97. Venues also use facial recognition to detect "courtsiders" who assist bettors and data brokers by transmitting data faster than official data. Ryan Rodenberg, *Sports Betting and Big Brother: Rise of Facial Recognition Cameras*, ESPN (Oct. 3, 2018), https://www.espn.com/chalk/story/_/id/24884024/why-use-facial-recognition-cameras-sporting-events-the-rise [https://perma.cc/6TYP-L7ZD].

121 *See Face Recognition Technology*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology [https://perma.cc/RLC4-DHQT].

122 *See* Tabor, *supra* note 97.

123 *See Company Overview*, FACEFIRST, https://www.facefirst.com/company-overview/ [https://perma.cc/3M2D-E478].

124 Jesse Davis West, *3 Ways That Face Recognition Will Impact Future Retail Stores in 2019*, FACEFIRST (Mar. 7, 2019), https://www.facefirst.com/blog/face-recognition-will-impact-future-retail-stores/ [https://perma.cc/QE2U-38X6].

125 *See* WOODWARD, *supra* note 117, at 10.

Further, venues use facial recognition to identify, eject, and ban unruly fans. Incidents warranting eviction range from pouring beers to throwing punches at other spectators.[126] Thus, keeping these problematic fans out of the stadium can not only improve the spectator experience, but also keep fans safe. Violence is a proven issue for teams such as the San Francisco 49ers. In a single season, over two hundred fights and twenty-three felony arrests occurred at home games.[127] Teams such as Danish football club Brondby IF report success stories of using facial recognition technology to keep "blacklist[ed]" fans out of their stadium.[128] Prior to implementing this system, Brondby used printed photographs of banned fans, a system they described as "very, very difficult" and "not very efficient."[129]

Additionally, biometric identifiers are an efficient, convenient, and secure method of verification.[130] These identifiers authenticate spectators at record speed.[131] Further, since traits like fingerprints are intrinsic in every individual, they cannot be stolen or lost like an ID card, or forgotten[132] or guessed like a password.[133] According to Verizon, hackers who stole or uncovered weak passwords accounted for 81% of data breaches in 2016.[134] Alternatively, biometric data

---

126 *See* Dave Sheinin & Mike Hume, *When Fans Get Banned for Life From Sports Stadiums*, WASH. POST (Oct. 7, 2016, 1:46 PM), https://www.washingtonpost.com/news/sports/wp/2016/10/07/when-fans-get-banned-for-life-from-sports-stadiums/ [https://perma.cc/3KFX-R9CM].

127 *See* West, *supra* note 124.

128 Adam Janofsky, *Stadium Weeds Out Disruptive Fans With Facial Recognition*, WALL STREET J. (Sept. 5, 2019, 11:30 AM), https://www.wsj.com/articles/stadium-weeds-out-disruptive-fans-with-facial-recognition-11567589403 [https://perma.cc/GE96-QAW8].

129 *Id*.

130 *See Biometrics Offers Advantages and Controversy*, RAND CORP., https://www.rand.org/natsec_area/products/biometrics.html [https://perma.cc/JDZ8-XRNR].

131 *See* Samir Nanavati, *Biometrics Allow for Better Bank Security and Customer Convenience*, N.Y. TIMES (July 5, 2016, 3:21 AM), https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-allow-for-better-bank-security-and-customer-convenience [https://perma.cc/69RT-HMC3].

132 *See* Tracy V. Wilson, *How Biometrics Works*, HOW STUFF WORKS, https://science.howstuffworks.com/biometrics.htm [https://perma.cc/542H-VC69].

133 *See Biometrics Offers Advantages and Controversy*, *supra* note 130.

134 *See* Fahmida Y. Rashid, *Annual Verizon Security Report Says Sloppiness Causes Most Data Breaches*, INFOWORLD (Apr. 27, 2017), https://www.infoworld.com/article/3193028/annual-verizon-security-report-says-sloppiness-causes-most-data-breaches.html [https://perma.cc/JZ8G-RBSG]

is much more difficult to recreate.[135] Using biometric data can improve security for venues as a whole, as well as for individual spectators.

3. Use of Biometric Data Creates a Customized Spectator Experience and Promotes Innovation

New technology inspires innovation. Many fans today believe that high-quality television and internet access make watching games at home more enjoyable than watching games live.[136] In response, sporting venues have sought to leverage technology to entice fans to come back to the venue.[137] Rapid technological advancement leads fans to expect digital, convenient customer service.[138] Thus, venues created the "Smart Stadium."[139] These stadiums provide a spectator experience centered around technology.[140] For example, many stadiums have phone applications ("apps") that boast a variety of functions, which include directing fans to the shortest lines and providing access to instant replays.[141] Further, teams and sponsors can interact with fans on social media.[142] In addition to apps, Smart Stadiums use digital signs at concession stands that rotate content, including to announce when a fresh batch of food is ready.[143] Smart Stadiums also partner with

---

135 *See* Olivia Solon, *The End of Passwords: Biometrics Are Coming But Do Risks Outweigh Benefits?*, GUARDIAN (Dec. 8, 2015, 8:00 AM), https://www.theguardian.com/technology/2015/dec/08/the-end-of-passwords-biometrics-risks-benefits [https://perma.cc/EGS4-RPTV].

136 *See generally Smart Connected Stadiums Smart Venues. Revolutionary Experiences*, INFOSYS (2018), https://www.infosys.com/engineering-services/white-papers/Documents/smart-connected-stadiums.pdf [https://perma.cc/885R-XW4Q].

137 *See id*.

138 *See Smart Stadiums Take the Lead in Profitability, Fan Experience, and Security*, INTEL 2 (2016), *available at* http://docplayer.net/18213468-Smart-stadiums-take-the-lead-in-profitability-fan-experience-and-security.html [https://perma.cc/4ER4-YV5S].

139 *Id.* at 1.

140 *See id.* at 2.

141 *See id*.

142 *See id.* at 4.

143 *See id.* at 24.

advertisers to run personalized, real-time advertisement campaigns.[144] These intelligent stadiums can also generate reports and determine the success of particular advertisements.[145]

Biometrics can take the personalized fan experience to the next level. Merchants can use faceprints to track what a fan purchases—i.e., a certain drink or type of clothing[146]—and then use that information to display "hyper-personalized" advertisements.[147] While the technology is not fully developed, many technology companies envision a future that integrates biometric data into advertisements at venues. For example, "in the not-too-distant" future, facial recognition devices will identify fans individually as they enter the venue.[148] If the device recognizes the attendee as a returning fan, the venue will already know that person's food preferences and can offer free food or similar perks tailored to that specific individual.[149] Technology companies such as Fancam are already able to determine how much attention fans pay to digital advertisements.[150] Knowing what time during the game and which advertisements attract the most attention can assist venues when selling advertisement space.[151] Further, having more information about potential

---

144 *See Smart Connected Stadiums Smart Venues, Revolutionary Experiences*, *supra* note 136.

145 *See id*. Yet, advertisements can only be personalized within the constraints of the stadium design. For example, every spectator sees the same jumbotron and thus the same advertisements.

146 *See* Matthew Hastings, *The Future of Biometrics: Identifying Target Markets at the Source*, AVER (Oct. 18, 2018), http://www.aver.com/AVerExpert/biotmetrics-targeting-the-market-at-the-source [https://perma.cc/882C-FFA2].

147 *Biometrics and Their Place in the Marketing World*, IEVO (Nov. 15, 2018, 12:07 PM), https://ievoreader.com/biometrics-and-their-place-in-the-marketing-world/ [https://perma.cc/QJZ4-B5JU].

148 Eric Fisher, *Facing the Data*, SPORTS BUS. J. (Mar. 5, 2018), https://www.sportsbusinessdaily.com/Journal/Issues/2018/03/05/In-Depth/Facial-recognition.aspx [https://perma.cc/A7C9-L7EN].

149 *See id*.

150 Recent advances in cameras, camera processing, and imaging have increased Fancam's ability to simply and accurately gather information about individual fans. *See id.* Digital advertisements are displayed throughout stadiums and arenas; for example, in the outfield of a baseball stadium and on jumbotrons above half-court in a basketball arena. *See How to Use Stadium Advertising and Arena Marketing to Grow Brand Awareness*, LINCHPIN SEO (last updated Dec. 25, 2019), https://linchpinseo.com/guide-to-sports-stadium-arena-marketing/ [https://perma.cc/8EQ4-4DPA].

151 *Cf. Biometrics and Their Place in the Marketing World*, *supra* note 147.

consumers enhances customer service.[152] Thus, in addition to benefiting advertisers, targeted advertisements benefit fans by guiding them to products they are more likely to enjoy.[153]

B. The Risks of Unregulated Use of Biometric Data

1. Recovery from Security Breaches Could Be Unattainable

The prevalence of security breaches and identity theft has grave consequences. Breaches expose personal identifiers such as addresses and phone numbers, as well as access to password-protected sites and bank accounts.[154] In the past two years alone, major breaches included Facebook's Cambridge Analytica scandal, the Marriott hack, the Equifax hack, the Capital One breach, and the discovery of unencrypted MoviePass records.[155] Yet many of these breaches can be remedied. Individuals can change passwords, replace credit cards, and thereby recover security.[156] However, after a biometric data breach, affected individuals cannot similarly recover their stolen biological data nor remedy the breach because there is no way to replace such data.

When it comes to security, the unique and unchangeable nature of biometric identifiers is a double-edged sword.[157] On the plus side, these permanent characteristics preclude biometric identifiers from being forgotten, stolen,[158] or guessed like a password.[159] Yet, just

---

[152] *See id*. For example, facial recognition has also been used to identify VIPs who enter the stadium. This allows venues to provide that VIP with the proper service. *See* Raffie Beroukhim, *What's "More Personal" Than Your Face?*, NEC TODAY (Aug. 24, 2018), https://nectoday.com/tag/stadiums/# [https://perma.cc/ZL9W-85FH].

[153] *See* David Kirkpatrick, *Study: 71% of Consumers Prefer Personalized Ads*, MARKETING DIVE (May 9, 2016), https://www.marketingdive.com/news/study-71-of-consumers-prefer-personalized-ads/418831/ [https://perma.cc/V689-NLRG].

[154] *See* Shelby Brown, *Equifax, MGM Resorts and Beyond: Every Major Security Breach and Data Hack*, CNET (Feb. 20, 2020, 7:48 AM), https://www.cnet.com/how-to/equifax-mgm-resorts-beyond-every-major-security-breach-and-data-hack-update/ [https://perma.cc/5TG2-GUYV].

[155] *See id*.

[156] *See* Robee Krishan & Reza Mostafavi, *Biometric Technology: Security and Privacy Concerns*, 22 J. INTERNET L. 19, 19 (2018).

[157] *Id*.

[158] *Id*.

[159] *See id.* at 19.

like all other forms of data on the internet, biometric information is still "vulnerable to international cybersecurity attacks."[160]

In August 2019, Biostar 2 suffered a massive breach of twenty-three gigabytes of data consisting of over thirty million records.[161] The records included standard data such as passwords and photographs, as well as biometric data such as facial recognition information and over a million fingerprints.[162] This breach was both quantitatively and geographically massive. Biostar 2 is a web-based biometric lock system that uses fingerprints and facial recognition to identify people trying to gain access to buildings.[163] Suprema, a "global Powerhouse in biometrics, security and identity solutions," owns Biostar 2.[164] Entities such as the United Kingdom metropolitan police, defense contractors, and banks all use Suprema.[165] Biostar 2 had recently merged with another security company, AEOS, which 5,700 companies across eighty-three countries use.[166]

Biostar 2's breach is particularly concerning because, "unlike passwords being leaked, when fingerprints are leaked, you can't change your fingerprint."[167] One of the hackers commented that "biometric information such as fingerprints could never be made private again once lost."[168] Though recovering from standard data breaches and identity theft is not trivial, biometric data's irreplaceable nature heightens security concerns. Overall, Biostar 2 has a widespread database, and the consequences of this breach,

---

160 *Id.* at 20.

161 *See* Chris Baraniuk, *Biostar Security Software 'Leaked a Million Fingerprints'*, BBC (Aug. 14, 2019), https://www.bbc.com/news/technology-49343774 [https://perma.cc/4PAX-2DG4].

162 *See id*.

163 *See* Josh Taylor, *Major Breach Found in Biometrics System Used by Banks, UK Police and Defence Firms*, GUARDIAN (Aug. 14, 2019, 3:11 AM), https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms [https://perma.cc/M3Q5-XQYR].

164 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/ [https://perma.cc/FWE3-MTJ4].

165 *See id*.

166 *See id*.

167 Taylor, *supra* note 163.

168 Baraniuk, *supra* note 161.

while still unclear, could be disastrous. Criminal activities stemming from this data could irreparably harm not only companies, but also their employees and clients.[169] Once a hacker has access to this irreplaceable data, individuals cannot regain their exclusive control over their biometric identities. Thus, this breach could lead to unbounded identity theft.

2. Inaccuracies in Facial Recognition

Recent studies illuminate another problem with biometrics: the high rates of inaccuracy in facial recognition. On October 21, 2019, the ACLU of Massachusetts published results from a study that used Amazon's Rekognition facial recognition software to run the faces of 188 professional athletes from the Boston Celtics, Boston Bruins, Boston Red Sox, and the New England Patriots against a database of public arrest photos.[170] The technology incorrectly identified twenty-seven of these athletes as criminals.[171] The ACLU of California conducted a similar study which revealed that inaccuracies skewed towards certain demographics—namely, women and people of color.[172]

Other studies show similar results.[173] For example, test results from July 2019 revealed that Idemia's algorithms are more likely to

---

169 *See id*.

170 *See Facial Recognition Technology Falsely Identifies Famous Athletes*, ACLU MASS. (Oct. 21, 2019, 2:00 PM), https://www.aclum.org/en/news/facial-recognition-technology-falsely-identifies-famous-athletes [https://perma.cc/D6BS-VKD5]. This test was part of the ACLU of Massachusetts' "Press Pause on Face Surveillance" campaign. *Id*.

171 *See id*.

172 *See id*. Though this Note will not discuss it, inaccuracies in facial recognition technology can also amplify bias. For example, the Electronic Privacy Information Center alleges that recruiting technology company HireVue's face-scanning software is biased by race and gender. *See* Ben Kochman, *FTC Should Probe AI Screening Co. HireVue, Advocates Say*, LAW360 (Nov. 7, 2019, 8:40 PM), https://www.law360.com/articles/1217648/ftc-should-probe-ai-screening-co-hirevue-advocates-say [https://perma.cc/LZQ3-YFJE].

173 *See* Larry Hardesty, *Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems*, MIT NEWS (Feb. 11, 2018), https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212 [https://perma.cc/R65N-57KL] (noting that three programs produced 0.8% error rates for light-skinned men, but error rates ranging from 20% to over 34% for dark-skinned women); *see also* Tom Simonite, *The Best Algorithms Struggle to Recognize Black Faces Equally*, WIRED (July 22, 2019, 7:00 AM),

misidentify black women's faces than any other gender and race combination.[174] These findings are problematic for both commercial and security uses of facial recognition. Advertisers cannot properly target advertisements and security forces cannot correctly identify criminals if facial recognition does not accurately identify individuals. Further, a fan's entire gameday experience can be ruined if he is barred from entering a stadium after security incorrectly identifies him as being on the venue's blacklist. Thus, inaccurate facial recognition technology has the potential to adversely affect a fan's experience at a game from the time he or she arrives at the venue to the time he or she leaves.

3. Biometric Data is Inherently Private

Biometric technology has a history of infringing on personal data. In 2012, San Francisco tech startup SceneTap planned to use basic facial identification such as jaw and skeletal structure to identify the age and gender of people at bars.[175] SceneTap would then share this information with potential guests so they would know the scene at the bar before they arrived.[176] Chief Executive Officer Cole Harper did not view SceneTap as facial recognition but rather "facial detection."[177] He stated that the software was not invasive because it only classified people by age and gender.[178] Yet that explanation did not satisfy wary San Francisco residents.[179]

---

https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/ [https://perma.cc/VTT2-4ASZ].

174 *See* Simonite, *supra* note 173.

175 *See* Violet Blue, *San Francisco Hates Your Startup: SceneTap*, ZDNET (May 15, 2012, 9:50 AM), https://www.zdnet.com/article/san-francisco-hates-your-startup-scenetap/ [https://perma.cc/6GMX-6RSZ].

176 *See* Adi Robertson, *SceneTap Cameras Hit San Francisco Bars, Use Facial Recognition to Find Parties and Privacy Concerns*, VERGE (May 15, 2012 10:33 AM), https://www.theverge.com/2012/5/15/3021628/scenetap-face-detecting-camera-san-francisco-bar-launch [https://perma.cc/KB5R-J38A].

177 Paula Forbes, *Creepy SceneTap App CEO Insists It's Not Creepy at All*, EATER (May 21, 2012, 10:45 AM), https://www.eater.com/2012/5/21/6584743/creepy-scenetap-app-ceo-insists-its-not-creepy-at-all [https://perma.cc/5X56-TPBG].

178 *See id*.

179 *See* Blue, *supra* note 175.

Civilians criticized SceneTap's privacy implications, and the company fizzled out of existence.[180]

Health insurance company Vitality's use of biometric data also raises privacy concerns. Vitality partners with wearable technology brands to promote a healthy lifestyle for its customers.[181] The company is unique in that it aims to pay for its customers' wellness, not sickness.[182] Vitality offers incentives for healthy behavior, which it tracks through wearable technology such as Apple Watches.[183] First, each member receives an Apple Watch for an initial activation fee and tax.[184] Then, the amount that member actually pays for the watch depends on how many workouts the member completes per month.[185] Additional rewards include discounts on healthy food.[186] Insurance company John Hancock has fully embraced Vitality;[187] in 2015, John Hancock started offering the option to add Vitality to its life insurance policies.[188] On September 19, 2018, after observing "remarkable results," such as a 30% decrease in hospitalization costs of Vitality policyholders, John Hancock announced that all of its life insurance policies would come with Vitality.[189] While the intent to promote wellness is noble, biometric data such as blood pressure

---

180 *See id*.

181 *See* Bernard Marr, *This Health Insurance Company Tracks Customers' Exercise and Eating Habits Using Big Data and IoT*, FORBES (May 27, 2019 12:22 AM), https://www.forbes.com/sites/bernardmarr/2019/05/27/this-health-insurance-company-tracks-customers-exercise-and-eating-habits-using-big-data-and-iot/#2bd96cbd6ef3 [https://perma.cc/PNN5-ULPL].

182 *See id*.

183 *See Active Rewards with Apple Watch*, VITALITY, https://www.vitalitygroup.com/the-vitality-difference/active-rewards-apple-watch/ [https://perma.cc/4FCR-ENLN].

184 *See id*.

185 *See id*.

186 *See* MARCO HAFNER, JACK POLLARD & CHRISTIAN VAN STOLK, INCENTIVES AND PHYSICAL ACTIVITY iv (RAND 2018).

187 *See* John Hancock, *John Hancock Leaves Traditional Life Insurance Model Behind to Incentivize Longer, Healthier Lives*, CISION PR NEWSWIRE (Sept. 19, 2018, 9:10 AM), https://www.prnewswire.com/news-releases/john-hancock-leaves-traditional-life-insurance-model-behind-to-incentivize-longer-healthier-lives-300715351.html [https://perma.cc/6CB5-4M24].

188 *See id*.

189 *Id*.

and cholesterol levels are private metrics that many people would prefer to keep private.[190]

Similar privacy concerns arise when using facial recognition at sports venues.[191] Because many people covet their anonymity, the thought of venues using persistent identifiers such as fingerprints and facial recognition to track fans' entire spectator experience is chilling.[192] Entrances using fingerprints reveal who attends the game, concessions using fingerprints for purchases reveal what fans are consuming, and facial recognition throughout the stadium reveals spectators' every move.[193] The potential for a breach to cause irremediable repercussions raises strong concerns about venues possessing such extensive, personal data about their attendees.[194]

4. The Risk of Unfair and Deceptive Trade Practices

Use of biometric data may be an unfair or deceptive trade practice. Section 45 of the Federal Trade Act codifies the illegality of unfair and deceptive trade practices. The Federal Trade Commission ("FTC" or "Commission") defines deceptive practices as those "involving a material representation, omission or practice that is

---

190 *See* Marr, *supra* note 181.

191 Though this Note will not discuss it in depth, there are also Fourth Amendment concerns with the use of biometric data at sports venues. These concerns revolve around "an individual's reasonable expectation of privacy," as addressed in *Katz v. United States*, 389 U.S. 347, 360–61 (1967). *See* Roberto Iraola, *New Detection Technologies and the Fourth Amendment*, 47 S.D. L. REV. 8, 16 (2002). Courts have discussed similar Fourth Amendment concerns regarding non-biometric technology as well. *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (holding that unrestricted access to cell-site records is not permitted by the Fourth Amendment).

192 *See* Daniel Susser, *Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't*, 9 J. INFO. POL'Y 37, 50 (2019).

193 In addition to the chilling effect of this intrusion of privacy, capturing biometric data could raise problems under the common law right to privacy. This right prohibits appropriation of a person's likeness. *See* RESTATEMENT (SECOND) OF TORTS §§ 652A, C (AM. LAW. INST. 1977). The Northern District of Illinois mentioned in dicta that using biometric data gathered from photographs to target advertisements could be an appropriation of one's likeness. *See* Rivera v. Google, Inc., 366 F. Supp. 3d 998, 1014 (N.D. Ill. 2018).

194 *See supra* Part II.B.1.

likely to mislead a customer acting reasonably in the circumstances."[195] The Commission describes an act or practice as unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by the customers themselves and not outweighed by countervailing benefits to consumers or to competition."[196] Once the FTC believes that an entity has violated 15 U.S.C. § 45, the FTC can issue a complaint charging that entity with an unfair or deceptive trade practice.[197] This complaint can be pursued through administrative or judicial enforcement.[198]

Sports arenas and biometric technology companies may claim that expedited lines,[199] the potential for heightened security,[200] and the customized spectator experience[201] outweigh the privacy[202] and data protection concerns of collecting biometric data.[203] However, the unchangeable, irreplaceable nature of biometric characteristics[204] and the inaccuracies associated with facial recognition technology[205] create too great a likelihood that spectators will suffer substantial injury. Short of opting out of having their data collected, an option that venues do not currently offer, spectators cannot reasonably avoid these harms.

Given the associated security and privacy implications that accompany the technology, it is likely that at least some spectators would want to opt out of participating in biometric identification. It is not challenging to offer entrances or concession booths without fingerprinting. However, if a venue uses facial scanning technology, it would be near impossible to have individual people opt in or out. Instead, at a minimum, stadiums could disclose use of facial

---

195 *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N (last revised Oct. 2019), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/U7ET-8MF5].

196 *Id*.

197 *See id*.

198 *See id*.

199 *See supra* Part II.A.1.

200 *See supra* Part II.A.2.

201 *See supra* Part II.A.3.

202 *See supra* Part II.B.3.

203 *See supra* Part II.B.1.

204 *See supra* Part II.B.1.

205 *See supra* Part II.B.2.

recognition on their website. Further, a solution many venues already employ is adding a contract to all tickets purchased.[206] However, online notice and ticket contracts could raise issues of unfair and deceptive trade practices and contracts of adhesion, as discussed further below.

A recent example of a technology-based deceptive trade practice is the FTC's settlement with Nomi Technologies. In 2015, the FTC found Nomi's promise of an in-store opt-out from its mobile tracking technology deceptive.[207] This practice was deceptive because, in fact, there was no way to opt-out in the stores; consumers could only opt-out online.[208] The FTC charged Nomi with misleading consumers, and the 2015 settlement prohibited Nomi from future misrepresentations.[209] This case forewarns spectator-sport venues of the repercussions that could result from misrepresenting opt-out clauses in their technology-use policies.

Additionally, contracts on tickets could be considered adhesion contracts. An adhesion contract is a "standard-form contract[]" that deprives an individual of bargaining power.[210] These contracts "introduce[] the serpent of uncertainty into the Eden of contract enforcement" by preventing the assurance of a "manifestation of the parties' intent."[211] Generally, large companies present these contracts to individuals on a "take-it-or-leave-it" basis.[212] Courts typically uphold these contracts unless the company uses "high pressure tactics," "deceptive language," or the contract is unconscionable.[213] The language of the ticket contract could be deceptive,[214] and not allowing somebody into the stadium unless they

---

206 *See* Golden & Chemi, *supra* note 9. These contracts also claim rights to spectators' likeness. *See id*.

207 *See* FTC Press Release 2015, *supra* note 93.

208 *See id*.

209 *See id*.

210 Klos v. Lotnicze, 133 F.3d 164, 168 (2d Cir. 1997); *see also* Edwin W. Patterson, *The Delivery of a Life Insurance Policy*, 33 HARV. L. REV. 198, 222 (1919).

211 *Klos*, 133 F.3d at 168.

212 *Id.* (internal citations omitted).

213 *Id.*; *see also* Carnival Cruise Lines, Inc. v. Shute, 499 U.S. 585, 593 (1991).

214 For example, the FTC charged Nomi with deceptive trade practice when Nomi misrepresented to consumers its in-store notice policy. *See* Complaint at 3, In the Matter of Nomi Techs., Inc., Docket No. C-4538 (F.T.C. Sept. 3, 2015).

agree to the terms allowing the use of their biometric data could be a "high pressure tactic." As for the third exception, courts have not yet determined whether capture, use, or dissemination of biometric data is unconscionable. However, scholars have addressed concerns about this ethical dilemma, particularly relating to Facebook's use of facial recognition for photograph tagging.[215] One scholar opines that Facebook's one-sided terms and conditions that permit use of facial recognition technology impose an "unreasonable and unfair" risk to users.[216] Despite this concern, privacy issues are not typically addressed through contract law; instead, they are usually regulated by the FTC.[217] Part III.B.2 will discuss the FTC's stance on the use of biometric data.

III. OPTIONS FOR REGULATING BIOMETRIC DATA

There is no national law in the United States regulating the use of biometric data. However, there are federal best practice guidelines in place. Additionally, several states have already enacted biometric privacy laws and some states have similar laws pending. There is also an EU statute governing the use of biometric data. These statutes and guidelines could provide a basis for a statute or regulation that would apply to sports venues. This Part will first address if using biometric data in sports venues should be regulated at all. Then, it will discuss the components of the current and proposed biometric regulations that could be applied to sports venues.

A. No Regulation

Allowing unrestricted use of biometric data in stadiums and arenas invites opportunities for increased spectator convenience and amplified security.[218] Lines will move quicker,[219] tickets cannot be

---

215 *See* Rosie Brinckerhoff, *Social Network or Social Nightmare: How California Courts Can Prevent Facebook's Frightening Foray into Facial Recognition Technology from Haunting Consumer Privacy Rights Forev*er, 70 FED. COMM. L.J. 105, 116 (2018).

216 *Id*.

217 *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 586 (2014).

218 *See supra* Part II.A.

219 *See CLEAR Adds Biometrics to Safeco Field Admissions, Concessions*, supra note 38.

lost,[220] advertisements will reach their optimal audience,[221] and fans will maximize the amount of time they spend watching the game.[222] Yet at this point in biometric technology's development, there is a shocking lack of empirical evidence to support these claims. They sound logical based on the personal, identifiable nature of biometrics, but it may be too soon to tell if these ambitious utilities will translate into reality. Additionally, spectators may be reluctant to relinquish control of their privacy for these alleged benefits.[223]

Even if spectators are willing to concede their data, they might be concerned about being misidentified due to the known inaccuracies of facial recognition technology.[224] Thus, it may be most advantageous to compromise and permit the use of biometric data conditioned on regulations. As mentioned above and expanded upon below, there is currently no nationwide regulation that applies to the use of biometric data in sports venues.[225] The FTC issued guidelines for use of facial recognition, yet only a few states have statutes in place.[226] As these few frameworks suggest, biometric regulations should focus on transparency, security exceptions, data protection, deletion, and remedies for when entities breach these regulations.[227]

B. Current Biometric Regulations and Propositions

1. Moratorium

Recently, many organizations and scholars have advocated for a moratorium on the use of facial recognition. The ACLU criticized the use of facial recognition as early as the 2001 Super Bowl, and its disdain for this technology has not dwindled.[228] In June 2019, the ACLU piloted an effort to encourage Congress to place a federal

---

220 *See* Favorito, *supra* note 40.
221 *See* Draper, *supra* note 5.
222 *See CLEAR Adds Biometrics to Safeco Field Admissions, Concessions*, *supra* note 38.
223 *See supra* Part II.B.3.
224 *See supra* Part II.B.2.
225 *See infra* Part III.B.2.b.
226 *See infra* Part III.B.2.
227 *See infra* Part III.B.2.
228 *See* Grossman, *supra* note 56.

moratorium on facial recognition for law enforcement.[229] In its letter, the ACLU emphasized how federal agencies use facial recognition technology "largely in secret," despite the fact that neither the federal nor state legislatures explicitly authorize law enforcement to use this technology.[230] Moreover, the ACLU's letter highlighted evidence of inaccuracy with this technology; namely, that the technology erroneously identifies women of color 30% of the time.[231] Thus, the ACLU requested that the U.S. House and Oversight Reform Committee place a moratorium on face recognition technology until Congress decides what uses should be permitted.[232]

The New York State Assembly seems to agree with the ACLU's stance. On June 20, 2019, just weeks after the ACLU sent its letter, the New York State Assembly passed a bill that prohibits the use of biometric identifiers in New York schools until July 1, 2022.[233] The bill directs the State Department of Education's chief privacy officer to study and recommend to the legislature which uses of biometric technology are appropriate and, if any, "what restrictions and guidelines should be enacted to protect individual privacy interests."[234] The bill highlights particular issues that the privacy

---

[229] *See* Letter from The American Civil Liberties Union, et al., to The Honorable Elijah Cummings, Chairman of the U.S. House Oversight and Reform Comm., the Honorable Jim Jordan, Ranking Member of the U.S. House Oversight and Reform Comm. (June 3, 2019) [hereinafter Letter from ACLU]. The ACLU asked for this moratorium to apply to immigration enforcement as well. Sixty groups accompanied the ACLU in signing this letter.

[230] *Id*.

[231] *Id*.

[232] *See id*. The ACLU also commenced a suit on October 31, 2019, against the U.S. Department of Justice, Federal Bureau of Investigation, and the Drug Enforcement Administration for failing to produce public records relating to use of biometric data, as is required under the Freedom of Information Act (5 U.S.C. § 552). *See* Complaint, ACLU v. United States Dep't of Justice, No. 1:19-cv-12242 (D. Mass. Oct. 31, 2019), ECF No. 1; Chris Villani, *ACLU Sues Feds Seeking Info on Facial Recognition Tech*, LAW360 (Oct. 31, 2019, 4:02 PM), https://www.law360.com/articles/1215653/aclu-sues-feds-seeking-info-on-facial-recognition-tech [https://perma.cc/2T4D-QYD2].

[233] *See* Annie McDonough, *School Facial Recognition Pause Passed in Assembly*, CITY & ST. N.Y. (June 21, 2019), https://www.cityandstateny.com/articles/policy/technology/school-facial-recognition-pause-passed-in-assembly.html [https://perma.cc/URN6-J9WH]. This bill is possibly a response to the Lockport City School District's move towards implementing a facial recognition security system.

[234] N.Y. Legis. Assemb. A06787 § 2-e(2)(a), Reg. Sess. 2019–20 (N.Y. 2019). The New York City Council also demonstrated concern about the use of biometric data in housing.

officer should consider, including the privacy implications, security uses, risk of false identifications, length of time the data should be stored, risks of breach, and processes for schools to notify the public that they are using biometric identifiers.[235] The New York Senate recessed for the year before determining whether to pass this bill.[236] The bill's sponsor expects the Senate to "take it up again" during the next session.[237]

Scholars such as Evan Selinger[238] and Woodrow Hartzog[239] support a ban on facial recognition.[240] They opine that use of facial

---

Council Member Brad Lander proposed the Keep Entry to Your Home Surveillance-free Act ("KEYS") to prohibit landlords from mandating use of technology-based keys and surveillance of buildings. *See New York City Council Legislation Would Protect Tenants From Racial Recognition & "Smart" Key Surveillance*, N.Y. CITY COUNCIL (Oct. 7, 2019), https://council.nyc.gov/brad-lander/2019/10/07/new-city-council-legislation-would-protect-tenants-from-facial-recognition-smart-key-surveillance/ [https://perma.cc/7NCS-UZ7L]. Senator Cory Booker proposed a similar bill, the No Biometric Barriers to Housing Act, that would ban the U.S. Department of Housing and Urban Development from using facial recognition in public housing. *See* Anthony Kimery, *Sen. Booker Latest to Propose Regulating Government's Use of Biometrics*, BIOMETRIC UPDATE (Nov. 4, 2019), https://www.biometricupdate.com/201911/sen-booker-latest-to-propose-regulating-governments-use-of-biometrics [https://perma.cc/S3T3-UUKR].

235 *See* N.Y. Legis. Assemb. A06787 § 2-e(2)(a).

236 *See* Ryan Whalen, *Wallace's Facial Recognition Moratorium Didn't Pass, But She's Asking NYSED to Do It Anyway*, SPECTRUM NEWS (July 16, 2019, 4:51 PM), https://spectrumlocalnews.com/nys/central-ny/politics/2019/07/16/facial-recognition-software [https://perma.cc/98N5-EPJX].

237 *Id*. Without a state-wide ban, Lockport City schools continued to "inch closer to using facial recognition cameras." *Lockport Schools Inch Closer to Using Facial Recognition Cameras*, WGRZ (last updated Nov. 28, 2019, 6:37 AM), https://www.wgrz.com/article/news/education/lockport-schools-inch-closer-to-using-facial-recognition-cameras/71-0f778827-c0d9-420b-97df-c05565d12083 [https://perma.cc/X8EH-V4JK]. On January 2, 2020, the school district activated its facial recognition system. Lockport stated that no student data would be stored in its system, and the Education Department did not object to the activation. *See* Thomas J. Prohaska, *Lockport Schools Activate Facial Recognition System*, BUFFALO NEWS (Jan. 3, 2020), https://buffalonews.com/2020/01/03/lockport-schools-activate-facial-recognition-system/ [https://perma.cc/W36S-UD9C].

238 Selinger is a professor and author who focuses on tech-ethics and privacy. *See Bio*, EVAN SELINGER, http://eselinger.org/bio/ [https://perma.cc/T2QQ-YFPA].

239 Hartzog is a professor of law, computer science, privacy, and data protection. *See Woodrow Hartzog*, NE. U. SCH. L., https://www.northeastern.edu/law/faculty/directory/hartzog.html [https://perma.cc/DP3Z-D57V].

240 *See* Evan Selinger & Woodrow Hartzog, *What Happens When Employers Can Read Your Facial Expressions?*, N.Y. TIMES (Oct. 17, 2019), https://www.nytimes.com/2019/10/17/opinion/facial-recognition-ban.html [https://perma.cc/TJY9-A68N].

recognition should be banned in both the public and private sectors because regulations that improve transparency and accountability and reduce systemic bias still cannot adequately protect privacy and freedom.[241] Selinger and Hartzog also distinguish facial recognition from other forms of biometric data by noting that faceprints are easier to capture than biometrics such as fingerprints and DNA which entities can only obtain through contact or samples.[242] Additionally, they state that faces are "central to our identities" and therefore deserve heightened protections.[243] Selinger and Harzog conclude that a ban on all use of facial recognition technology is essential to preserve civil rights and privacy.[244]

In contrast to Selinger and Hartzog, the ACLU and New York State Assembly only call for a temporary moratorium. They seem to recognize that the government cannot halt the use of biometric technology forever, and instead suggest that the government implement regulations before innovation proceeds.[245] Federal and state governments have begun to address similar concerns with the use of biometrics, and some regulations are already in place.

2. Existing Regulations

a) Common Concerns

As seen in the above-referenced New York State Assembly education bill,[246] currently enacted and proposed statutes frequently

---

241 *See id*.

242 *See id*.

243 *See id*.

244 *See id*. The U.S. cities of San Francisco, Somerville, Oakland, Berkeley, Brookline, and San Diego have already banned facial recognition. *See* Bruce Schneier, *We're Banning Facial Recognition. We're Missing the Point.*, N.Y. TIMES (Jan. 20, 2020), https://www.nytimes.com/2020/01/20/opinion/facial-recognition-ban-privacy.html [https://perma.cc/5PFX-386J]. On January 27, 2020, Senator Brad Hoylman introduced a bill in the New York Senate that would ban law enforcement from using biometric surveillance technology. *See* Massarah Mikati, *NY Senate Bill Would Ban Police Facial Recognition Technology*, NNY360 (Jan. 27, 2020), https://www.nny360.com/top_stories/ny-senate-bill-would-ban-police-facial-recognition-technology/article_265b0d77-f773-5e77-a037-7a02a50f0fbf.html [https://perma.cc/CV6C-W4NQ].

245 *See* Letter from ACLU, *supra* note 229; *see also* N.Y. Leg. Assemb. A06787 § 2-e(2)(a), Reg. Sess. 2019–20 (N.Y. 2019).

246 *See supra* Part III.B.1.

incorporate the following attributes: transparency, consent, security, and remedies. Transparency can be achieved by first requiring notice that an entity is using biometric identifiers.[247] Then, the entity should obtain consent for that use.[248] Finally, all policies regarding the data should be available to the public.[249] It is important to note, however, that many statutes do not require notice and consent when the information is used for security purposes.[250] Additionally, protection of data is of the utmost concern. Data protection standards can include elements such as retention and deletion policies, and the right for individuals to review their own data.[251] Finally, there must be a remedy for when an entity breaches the imposed standards.[252] Congress, the FTC, and many international countries and states have already implemented plans or legislation to regulate biometrics.[253] Importantly, current statutes do not directly address the inaccuracies of facial recognition technology. Yet it is crucial for regulators to keep in mind the high false identification rates in facial recognition.[254] Frequently inaccurate results diminish the value of facial data for both commercial and security purposes.

b) Federal Regulation

As yet, there is no federal statute that regulates the use of biometric data. In March 2019, Senator Roy Blunt introduced the Commercial Facial Recognition Act of 2019 ("CFRA") into

---

247 *See, e.g.*, 740 ILL. COMP. STAT. 14/15(b)(1)–(2) (2008); TEX. BUS. & COM. CODE ANN. § 503.001(b) (West 2019); WASH. REV. CODE § 19.375.020(1) (2017).

248 *See, e.g.*, *supra* note 247.

249 *See, e.g.*, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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), 2016 O.J. (L 119/1) Ch. 3, Art. 15 [hereinafter GDPR].

250 *See, e.g.*, WASH. REV. CODE § 19.375.020(7); TEX. BUS. & COM. CODE ANN. § 503.001(a).

251 *See, e.g.*, GDPR at Ch. 3, Art. 17 and Ch. 2, Art. 7(3); 740 ILL. COMP. STAT. 14/15(a); TEX. BUS. & COM. CODE ANN. § 503.001(c)(3).

252 For example, Illinois's BIPA allows private actions, whereas Texas's Capture or Use of Biometric Data statute only allows public actions to be brought by the attorney general. *Compare* 740 ILL. COMP. STAT. 14/20, *with* TEX. BUS. & COM. CODE ANN. § 503.001(d).

253 *See infra* Parts III.B.2.b–d.

254 *See supra* Part II.B.2.

Congress.[255] This Senate bill is limited in scope because it only applies to facial recognition technology and not biometric data generally.[256] Though it is not likely to pass the first hurdle toward enactment—getting out of committee[257]—the bill does provide insight into how some members of Congress believe certain biometric data should be regulated.[258] In particular, the CFRA requires entities[259] to notify individuals and obtain "affirmative consent" for all uses of facial recognition technology.[260] Affirmative consent requires "individual, voluntary, and explicit consent" for the collection and use of data.[261] The CFRA also has a notice-and-consent exception for security purposes.[262] The bill defines "security application" as "loss prevention and any other application intended to detect or prevent criminal activity, including shoplifting and fraud."[263] This bill delegates regulatory power to state attorneys general and the FTC.[264] As seen below, this delegation to the FTC would really be an extension of the regulatory power that the FTC already enjoys.

---

255 *See generally* Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. (2019).

256 *See generally id.* §§ 2(5)–(6).

257 *See* 116 Legislative Outlook S. 847; *see also S. 847: Commercial Facial Recognition Privacy Act of 2019*, GOVTRACK, https://www.govtrack.us/congress/bills/116/s847 [https://perma.cc/4YHQ-7Q49].

258 *See* Taylor Hatmaker, *Bipartisan Bill Proposes Oversight for Commercial Facial Recognition*, TECHCRUNCH (Mar. 14, 2019, 7:25 PM), https://techcrunch.com/2019/03/14/facial-recognition-bill-commercial-facial-recognition-privacy-act/ [https://perma.cc/XVK4-GMDY]. It should be noted that many members of Congress may not even know how biometric technology works. Topics related to technology, such as the 2018 Facebook hearings and bitcoin, have "baffled an elderly Congress." Avi Selk, *'There's So Many Different Things!': How Technology Baffled an Elderly Congress in 2018*, WASH. POST (Jan. 2, 2019, 12:38 PM), https://www.washingtonpost.com/lifestyle/style/theres-so-many-different-things-how-technology-baffled-an-elderly-congress-in-2018/2019/01/02/f583f368-ffe0-11e8-83c0-b06139e540e5_story.html [https://perma.cc/3FJT-85J9].

259 S. 847 § 2(3). The CFRA defines a "covered entity" as people, including corporations but excluding government, law enforcement, national security, and intelligence agencies. *Id*.

260 *Id.* § 3(a).

261 *Id.* § 2(1). Even with consent, if harm to the user is reasonably foreseeable, the statute requires "meaningful human review" of the data before it is used. *Id.* § 3(c).

262 *Id.* § 2(3)(B).

263 *Id.* § 2(9).

264 *See id.* § 4.

The FTC is likely "the broadest and most influential regulating force on information privacy in the United States."[265] The Commission investigates privacy breaches and protects consumers by ending unfair and deceptive trade practices.[266] Most of the FTC's actions conclude in an administrative settlement instead of litigation.[267] Though the settlements are not binding precedent, they perform a similar function in guiding companies' actions.[268] Despite contract law's potential to govern privacy policies,[269] the FTC has become the de facto enforcer of privacy rights.[270]

The Federal Trade Commission Act authorizes the FTC to regulate unfair or deceptive acts affecting commerce.[271] The FTC currently has some deference when regulating biometric data in commerce because, at present, the statute does not explicitly reference this new technology, and, in the past, the FTC has taken the initiative on regulating novel technologies, even when such technologies are not explicitly regulated by the Federal Trade Commission Act, as demonstrated below.

Currently, there are few precedential actions regulating biometric data; however, actions relating to similar technologies can inform how the FTC will opt to regulate the use of biometric data. For example, in 2011, the FTC required Google Buzz to "implement a comprehensive privacy program" as part of a settlement for use of deceptive tactics when consumers joined its social network platform.[272] This was the first time the FTC mandated that a company enact such a policy.[273] The FTC is also likely to bring a

---

265 Solove & Hartzog, *supra* note 217, at 585.

266 *See What We Do*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/what-we-do [https://perma.cc/5B3F-N5VX].

267 *See* Solove & Hartzog, *supra* note 217, at 589.

268 *See id.*

269 *See supra* Part II.B.4.

270 *See* Solove & Hartzog, *supra* note 217, at 600–01.

271 *Cf.* 15 U.S.C. §§ 41–58 (2012); *Federal Trade Commission Act*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act [https://perma.cc/4M5E-FNSH].

272 *See* Press Release, Fed. Trade Comm'n, FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network (Mar. 31, 2011), https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz [https://perma.cc/4BJK-5U5Z].

273 *See id*.

suit against companies who make deceptive statements to obtain personal information from consumers.[274] Additionally, the FTC typically requires notice and choice.[275] In 2012, the FTC required Facebook to "giv[e] consumers clear and prominent notice and obtain[] express consent" for all components of its privacy settings.[276] In *In re Gateway Learning Corp.*, the FTC described "express affirmative . . . consent" as opting-in.[277] In this situation, Gateway changed its policy for selling data to third parties after many consumers already purchased the product.[278] By requiring an opt-in to the changed policy, it seems that the FTC was emphasizing the importance of consumers knowing exactly how their data was being used before electing to use that product.

Though there are limited cases addressing biometric technology, the FTC has issued some guidance directly dealing with regulating facial recognition.[279] In 2012, the same year as the Facebook settlement, the FTC recommended "best practices for common uses of facial technology" ("Best Practices").[280] In regards to notice and consent, the FTC advised that companies provide notice and "affirmative express consent"[281] when using facial recognition

---

[274] *See* Press Release, Fed. Trade Comm'n, District Court Bars the Sale of Consumers Telephone Records to Third Parties (Jan. 28, 2008), https://www.ftc.gov/news-events/press-releases/2008/01/district-court-bars-sale-consumers-telephone-records-third [https://perma.cc/4YVJ-BFPC].

[275] "Notice and choice" is the current archetype for digital data collection and use. It is the heart of the GDPR and the California Consumer Privacy Act. *See* Richard Wagner & Robert Sloan, *Beyond Notice and Choice: Privacy Norms, and Consent*, 14 J. HIGH TECH. L. 370, 379 (2013); GDPR at Ch. 2, Art. 7(1).

[276] Press Release, Fed. Trade Comm'n, FTC Approves Final Settlement with Facebook (Aug. 10, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook [https://perma.cc/5PTY-X25R].

[277] Press Release, Fed. Trade Comm'n, Gateway Learning Settles FTC Privacy Charges (July 7, 2004), https://www.ftc.gov/news-events/press-releases/2004/07/gateway-learning-settles-ftc-privacy-charges [https://perma.cc/XYS4-5T82]. The FTC banned Gateway from sharing its consumers' personal information without express affirmative consent. *See id*.

[278] *See id*.

[279] *See* FTC, BEST PRACTICES, *supra* note 30, at iii.

[280] *Id*.

[281] *Id.* The FTC opines that entities should obtain "affirmative consent" "at least" in situations where biometric data is collected in a "materially different manner" than the entity represented when it originally collected the data. This includes disseminating information to sources that would not otherwise have access to that data. *Id*.

technology in order to promote "privacy and safety."[282] The FTC's Best Practices also comment on data protection.[283] The guidelines acknowledge that "biometric data may be susceptible to breaches and hacking."[284]

The FTC addressed these two points via a case study where a digital sign determined the "age range and gender of the customer standing in front" of it and "display[ed] a targeted advertisement" accordingly.[285] Here, the FTC recommended a "sliding scale approach to notice and consent."[286] For example, providing notice so that consumers can avoid the sign might be okay when the sign only detects age and gender and does not retain any information; however, this might not constitute "meaningful" affirmative consent if the sign identifies particular individuals.[287] Additionally, the FTC recommended that the company controlling the sign "implement reasonable data security protections" to prevent third parties from hacking the sign's software.[288] The Best Practices also recommended that entities delete data when the original purpose for collection is complete and, in the case of social media, when users delete their accounts and therefore withdraw their consent.[289] Instructively, the guidelines also note the known inaccuracies of facial recognition technology.[290]

The FTC has applied the Best Practices in a few recent actions.[291] In July of 2019, Facebook and the FTC reached a

---

282 *Id*.
283 *See generally id*.
284 *Id.* at 7.
285 *Id.* at 13.
286 *Id*. at 16.
287 *Id.*
288 *Id*. at 13.
289 *See id.* at 18.
290 *See id.* at 3.
291 *See, e.g.*, Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions [https://perma.cc/9WL2-TWCC]; Press Release, Fed. Trade Comm'n, Five Companies Settle FTC Allegations That They Falsely Claimed Participation in the UE-U.S. Privacy Shield (Sept. 3, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/five-companies-settle-ftc-allegations-they-falsely-claimed [https://perma.cc/A42E-8FAQ].

settlement[292] over allegations that Facebook mishandled user data.[293] In addition to a $5 billion fine,[294] Facebook agreed to implement new, "unprecedented"[295] regulations.[296] One of these regulations requires Facebook to "provide clear and conspicuous notice of its use of facial recognition technology, and obtain affirmative express user consent prior to any use that materially exceeds its prior disclosures to users."[297] Further, the settlement requires that Facebook "establish, implement, and maintain a comprehensive data security program."[298] Shortly after Facebook and the FTC reached this settlement, Facebook removed its automatic suggested tagging feature.[299] While the suggested tagging feature still exists, users must now opt-in to using this feature.[300] Though the settlement did not explicitly state that opt-in is necessary to achieve "affirmative express user consent" that conforms to FTC standards, Facebook's new opt-in policy ultimately may set an industry standard.[301]

More recently, in September 2019, the FTC settled its claim against facial recognition software provider 214 Technologies, Inc.

---

[292] This case was brought in reaction to the Cambridge Analytica scandal, when Cambridge Analytica improperly obtained data from Facebook to construct voter profiles in 2016. *See* Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html [https://perma.cc/V6GG-XYH9]; *see also* FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, *supra* note 291.

[293] *See* Ben Gilbert, *Alongside a $5 Billion Fine, the US Government Just Imposed a Bunch of Restrictions on What Facebook Can and Can't Do: Here's the Full List*, BUS. INSIDER (July 24, 2019, 10:44 AM), https://www.businessinsider.com/facebook-hit-with-regulations-in-ftc-settlement-full-list-2019-7 [https://perma.cc/9VYY-CRNP].

[294] This is the largest fine the FTC has ever imposed for a consumer privacy violation. *See* FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, *supra* note 291.

[295] *Id*.

[296] *See* Gilbert, *supra* note 293.

[297] *Id*.

[298] FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, *supra* note 291.

[299] *See* Gilbert, *supra* note 293.

[300] *See id*.

[301] FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, *supra* note 291.

("214 Tech").[302] The FTC alleged that 214 Tech falsely claimed it certified itself under the EU-U.S. Privacy Shield framework.[303] As part of the consent agreement, the FTC prohibited 214 Tech from misrepresenting its participation in privacy or data security programs.[304]

The Facebook and 214 Tech settlements, along with the FTC's 2012 guidelines, suggest that the FTC is likely to find misrepresentations and omissions about use of facial recognition, and possibly other forms of biometric data, not just deceptive, but also unfair.[305] Further, the two facial recognition enforcement actions against Facebook and 214 Tech occurred within three months of each other and are quite recent.[306] Thus, these actions could signify a continuing trend of rigorous FTC monitoring and penalizing improper uses of biometrics.

c) International Regulation

A prominent international regulation is the EU's General Data Privacy Regulation ("GDPR").[307] Implemented on May 25, 2018, this comprehensive, first-of-its-kind data privacy regulation strives to "protect all EU citizens from privacy and data breaches in today's

---

302 *See* Five Companies Settle FTC Allegations That They Falsely Claimed Participation in the UE-U.S. Privacy Shield, *supra* note 291.

303 *See id*. The EU-U.S. Privacy Shield is a framework of data protection requirements created by the U.S. Department of Commerce and the European Commission and Swiss Administration. This framework protects data transferred during transatlantic commerce. *See Welcome to the Privacy Shield*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/welcome [https://perma.cc/B6VT-WK39].

304 *See* Five Companies Settle FTC Allegations That They Falsely Claimed Participation in the UE-U.S. Privacy Shield, *supra* note 291.

305 The FTC considers egregious deceptive practices unfair. *See* Solove & Hartzog, *supra* note 217, at 631. This is bolstered by commissioner J. Thomas Rosch's dissenting statement in the 2012 guidelines where he disagrees with the majority's "insistence that the 'unfairness' prong, rather than the 'deception' prong . . . should govern practices relating to facial recognition technology." FTC, BEST PRACTICES, *supra* note 30 (Rosch, J., dissenting).

306 The Facebook order was issued in July 2019 and the Tech Order 214 in September 2019. *See* FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, *supra* note 291; Five Companies Settle FTC Allegations That They Falsely Claimed Participation in the UE-U.S. Privacy Shield, *supra* note 291.

307 *See* EU GDPR, https://eugdpr.org [https://perma.cc/FE8N-ARDT].

data-driven world."[308] The GDPR requires consent before businesses process consumer data.[309] When businesses request that consent, the request must be "intelligible and easily accessible."[310] Further, consumers can withdraw consent "at any time."[311] Consumers are also able to obtain information about whether third parties are using their data and where and for what purpose their data is being used.[312] Additionally, businesses must provide consumers with copies of their personal data.[313] In regards to security exceptions, the EU gives its Member States considerable leeway.[314] Namely, the GDPR is "not applicable to criminal prosecution," and all related data processing "by competent authorities" is exempt.[315] Further, the GDRP does not apply to Member States processing data "regarding national and common security."[316]

To protect consumer data, the GDPR contains a deletion policy.[317] There are two routes for deletion. First, companies must delete data once they achieve their original purpose for collecting the data.[318] Second, individuals can withdraw consent and therefore have personal data deleted.[319] In the event of a violation, the GDPR permits both public enforcement and private litigation.[320] While "supervisory authorities" regulate companies that fall under the

---

308 *GDPR Key Changes*, EU GDPR, https://eugdpr.org/the-regulation/ (last visited Sept. 12, 2019); GDPR at Ch. 4, Art. 35 (requiring a "data protection impact assessment" to help prevent data breaches).

309 *See* GDPR at Ch. 2, Art. 7(1).

310 *Id.* at Ch. 2, Art. 7(2).

311 *Id.* at Ch. 2, Art. 7(3).

312 *Id.* at Ch. 3, Art. 15(1)(a)–(d).

313 *Id.* at Ch. 3, Art. 15(3).

314 *See id.* at Rec. 16, 19.

315 *Id.* at Rec. 19. Note that there is a separate Directive that governs data processing for criminal enforcement. *See* Directive (EU) 2016/680, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 119) 89.

316 GDPR at Rec. 16.

317 *See id.* at Ch. 3, Art. 17; *id.* at Ch. 2, Art. 7(3).

318 *See id.* at Ch. 3, Art. 17.

319 *See id.* at Ch. 2, Art. 7(3).

320 *See id.* at Ch. 8, Sect. 82.

GDPR, private individuals are permitted to "lodge a complaint with a supervisory authority."[321] For example, on the day that the GDPR went into effect, "European privacy advocate" Max Schrems[322] filed suits against Google and Facebook, seeking a combined $8.8 billion in damages.[323] Schrems alleged that the companies violated Article 6 of the GDPR by forcing consent before consumers could use their services.[324] In January 2019, the French data protection authority fined Google $57 million, thus demonstrating Member States' willingness to enforce the GDPR soon after its enactment.[325]

d) State Regulations

i. Enacted Regulations

a. Illinois

In 2008, Illinois became the first state to regulate biometric data with its Biometric Information Privacy Act ("BIPA").[326] Through BIPA, the Illinois legislature aims to serve "public welfare, security, and safety"[327] by regulating "biometric identifiers" such as fingerprints and face geometry.[328] The act has a two-step process to ensure transparency between "private entit[ies]" and consumers.[329] First,

---

321 *Id.* at Ch. 8, Art. 77.

322 *Where Are We Now? Six Months Into the GDPR*, XPAN L. GROUP (Jan. 15, 2019), https://xpanlawgroup.com/where-are-we-now-six-months-into-the-gdpr/ [https://perma.cc/M4X3-264A] [hereinafter *Where Are We Now?*].

323 *See* Russell Brandom, *Facebook and Google Hit With $8.8 Billion in Lawsuits on Day One of GDPR*, VERGE (May 25, 2019, 10:21 AM), https://www.theverge.com/2018/5/25/17393766/facebook-google-gdpr-lawsuit-max-schrems-europe [https://perma.cc/4WGT-6HMJ].

324 *See Where Are We Now?*, *supra* note 322.

325 *See* Adam Satariao, *Google Is Fined $57 Million Under Europe's Data Privacy Law*, N.Y. TIMES (Jan. 21, 2019), https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html [https://perma.cc/4WGT-6HMJ].

326 *See* Thomas F. Zych, Steven G. Stransky & Brian Doyle-Wenger, *State Biometric Privacy Laws: What You Need to Know*, LEXOLOGY (Sept. 5, 2019), https://www.lexology.com/library/detail.aspx?g=ebc0e01c-45cc-4d50-959e-75434b93b250 [https://perma.cc/BJE7-8CVE].

327 740 ILL. COMP. STAT. 14/5(g) (2008).

328 *Id.* 14/10. Face geometry is measured through metrics such as distance between eyes and distance from forehead to chin. *See* Steve Symanovich, *How Does Facial Recognition Work?*, NORTON, https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html [https://perma.cc/F8ZV-9H78].

329 740 ILL. COMP. STAT. 14/15(b).

BIPA requires entities to disclose in writing that biometric information is being collected or stored, and for what specific purpose and length of time this information is being collected, stored, and used.[330] Then, the "subject of the biometric identifier" must provide written release for the stated uses.[331] Additionally, no information can be sold or disseminated without consent.[332]

The notice and consent policies in this statute strive to wholeheartedly protect the privacy interests of individuals.[333] BIPA achieves this protection by requiring private entities to obtain notice and consent for any use of individuals' biometric data.[334] The act defines "private entity" as any individual, partnership, corporation, limited liability company, association, or other group, however organized, but explicitly excludes "[s]tate and local government agencies."[335] Therefore, the statute's notice and consent requirements exclude government-supported security systems, yet apply to private security companies.[336] BIPA also recognizes the importance of data protection by requiring that "private entities . . . store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry."[337] Further, BIPA mandates "permanent destruction" of the information once the initial purpose of the collection is complete, or "within 3 years of the individual's last interaction with the private entity, whichever occurs first."[338]

The most notable feature of BIPA, however, is its private cause of action to remedy breaches.[339] This private cause of action allows an individual to recover damages after a breach.[340] An individual can recover up to $1,000 or actual damages for a negligent

---

330 *See id.* 14/15(b)(1)–(2).
331 *Id.* 14/15(b)(3).
332 *See id.* 14/15(c)–(d).
333 *See generally id.* 14/15.
334 *Id.*
335 *Id.* 14/10.
336 *See id.*
337 *Id.* 14/15(e)(1).
338 *Id.* 14/15(a).
339 *See id.* 14/20.
340 *See id.*

violation,[341] or up to $5,000 for a reckless or intentional violation,[342] as well as attorney fees,[343] and other relief, such as an injunction.[344]

One of the first major cases to be brought under BIPA was against Facebook in 2016.[345] The plaintiffs alleged that Facebook's "tag suggestions" violated BIPA due to Facebook's failure to provide notice that it collected biometric data, failure to provide a retention schedule and deletion guidelines, and failure to obtain written consent from users.[346] After being removed from Illinois state court to the Northern District of California, the district court issued an opinion in 2018.[347] The court did not dispute that clicking a box to agree to the "Terms of Use" and "Privacy Policy" constituted written consent;[348] the heart of the issue was whether a photograph fell within BIPA's definition of biometric data.[349] Facebook maintained that because the statute includes the word "scan" but not the word "photograph[]," this must mean that "face geometry" could only be collected in person.[350] The Northern District of California disagreed; it viewed Facebook's "cramped interpretation" as inconsistent with BIPA's purpose.[351] The Northern District of California then certified the class in 2018.[352] Facebook appealed the certification and claimed that the plaintiffs did not achieve Article III

---

341 *See id.* 14/20(1).

342 *See id.* 14/20(2).

343 *See id.* 14/20(3).

344 *See id.* 14/20(4).

345 *See generally In re* Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1159 (N.D. Cal. 2016).

346 *Id.*

347 This case was originally filed in Illinois state court, but Facebook removed it to federal court under the Class Action Fairness Act. *See* Patel v. Facebook Inc., 290 F. Supp. 3d 948, 951 (N.D. Cal. 2018).

348 *Id.* at 1163; *see also* Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 12, 13–14 (2d Cir. 2017) (stating that viewing terms and conditions on the screen and clicking "continue" qualifies as written consent under BIPA).

349 *See In re Facebook*, 185 F. Supp. 3d at 1159, 1170.

350 *Id.* at 1171 (quoting Defendant's Motion to Dismiss at 12–13, *In re Facebook*, 185 F. Supp. 3d 1155, ECF No. 69).

351 *Id.*; *see also* Monroy v. Shutterfly, No. 16 C 10984, 2017 WL 4099846 at *3 (N.D. Ill. Sept. 15, 2017) (holding that biometric data Shutterfly obtained from photographs constitutes "biometric data" under BIPA).

352 *See In re* Facebook Biometric Info. Privacy Litig., 326 F.R.D. 535, 549 (N.D. Cal. 2018); *cf.* Rivera v. Google, Inc., 366 F. Supp. 3d 998, 1003, 1014 (N.D. Ill. 2018), where the Northern District of Illinois dismissed a BIPA suit, reasoning that "feeling offended"

standing.[353] In August 2019, the Ninth Circuit rejected Facebook's argument and affirmed the district court's decision which held that Facebook violated the plaintiffs' "concrete privacy interests" protected by BIPA.[354] The Ninth Circuit issued this decision a little over half a year after the Supreme Court of Illinois decided *Rosenbach v. Six Flags*.[355]

Rosenbach v. Six Flags addressed whether actual harm is necessary to achieve Article III standing under BIPA.[356] Plaintiff Rosenbach's mother sued Six Flags for failing to obtain her consent to collect her son's fingerprints, which were used to issue a repeat-entry pass.[357] The court grappled with the question of whether a plaintiff must claim "actual injury or adverse effect" to bring suit.[358] The court decided that question in the negative: "violation of [one's] rights under" BIPA is sufficient to achieve standing.[359] The court reasoned that "procedural protections are particularly crucial in our digital world," thus violating a privacy statue results in "real and significant" injury.[360] Since the court filed this "highly anticipated"

---

that Google Photos collected data using facial recognition technology did not qualify as "concrete injuries for Article III purposes." *Id.* at 1003, 1014. In 2019, the plaintiffs filed appeals to the U.S. Court of Appeals for the Seventh Circuit, but the appeals remain pending. *See id.*, *appeals docketed*, No. 19–1182 (Jan. 28, 2019), No. 19–1942 (Feb. 8, 2019).

353 *See* Patel v. Facebook, Inc., 932 F.3d 1264, 1267 (9th Cir. 2019), *cert. denied*, No. 19–706, 2020 WL 283288 (Jan. 21, 2020). In January of 2020, Facebook settled the biometric information privacy suit for $550 million. The money will cover the plaintiff's legal fees, and the rest will go to eligible Illinois users. *See* Natasha Singer and Mike Isaac, *Facebook to Pay $550 Million to Settle Facial Recognition Suit*, N.Y. TIMES (Jan. 20, 2020) https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html [https://perma.cc/SNH8-RT5U].

354 *Patel*, 932 F.3d at 1275.

355 Both of these cases determined that a violation of rights under BIPA achieves Article III standing. *See* Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1207 (Ill. 2019); *Patel*, 932 F.3d at 1274–75.

356 *See generally Rosenbach*, 129 N.E.3d 1197.

357 *See id.* at 1200–01.

358 *Id.* at 1207.

359 *Id*.

360 *Rosenbach*, 129 N.E.3d at 1206 (quoting Patel v. Facebook Inc., 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018)).

decision in January of 2019, there has been an influx of lawsuits,[361] and many more suits are likely to follow.[362]

b. Texas

Following Illinois' lead, Texas passed the Capture or Use of Biometric Identifier Act ("CUBI") in 2009.[363] CUBI prohibits the capture, sale, or disclosure of an individual's "biometric identifiers" such as fingerprints and face geometry[364] "for commercial purpose"[365] unless the collecting entity notifies the individual and that individual consents.[366] This requirement is distinct from BIPA because it (1) targets data collected for "commercial purpose,"[367] as opposed to any private entity that possesses biometric information,[368] and (2) requires consent, though not necessarily written consent,[369] unlike BIPA which requires written consent.[370] Since CUBI only applies to information used for "commercial purposes," this could encompass private security forces.[371] Like BIPA, CUBI's data protection clause establishes a reasonable care standard.[372] It mandates that biometric data be "stor[ed], transmit[ed] and protect[ed] from disclosure . . . using reasonable care."[373] Additionally, CUBI's deletion policy calls for destruction of data "within a reasonable time, but not later than the first anniversary of the date

---

361 Quinn Emanuel Urquhart & Sullivan, LLP, *June 2019: The Rise of Biometrics Laws and Litigation*, JD SUPRA (June 28, 2019), https://www.jdsupra.com/legalnews/june-2019-the-rise-of-biometrics-laws-82168/ [https://perma.cc/4FJN-Z948].

362 *See* Christine E. Skoczylas & Dana Amato Sarros, *No Harm, No Foul? Not So Fast: The Illinois Supreme Court Allows BIPA Lawsuits Without Allegations of Actual Injury*, NAT'L L. REV. (June 5, 2019), https://www.natlawreview.com/article/no-harm-no-foul-not-so-fast-illinois-supreme-court-allows-bipa-lawsuits-without [https://perma.cc/FVT6-CSBN]. This increase is expected as a reaction to multiple recent decisions holding that violating BIPA satisfies the actual harm required to achieve Article III standing under *Spokeo v. Robins*, 136 S. Ct. 1540 (2016). *See id.*; *see also Patel*, 932 F.3d at 1274–75.

363 *See generally* TEX. BUS. & COM. CODE ANN. § 503.001 (West 2019).

364 *Id.* § 503.001(a).

365 *Id.* § 503.001(b)–(c).

366 *See id.* § 503.001(b).

367 *Id.*

368 *See* 740 ILL. COMP. STAT. 14/15 (2008).

369 *See* TEX. BUS. & COM. CODE § 503.001(b).

370 *See* 740 ILL. COMP. STAT. 14/15(b)(3).

371 TEX. BUS. & COM. CODE § 503.001(b)–(c).

372 *See* 740 ILL. COMP. STAT. 14/15(e)(1); TEX. BUS. & COM. CODE § 503.001(c)(2).

373 TEX. BUS. & COM. CODE § 503.001(c)(2).

the purpose for collecting the identifier expires."[374] Finally, CUBI's mandated remedy is a civil penalty brought by the attorney general.[375] This publicly enforceable remedy is much more restrictive than BIPA's private cause of action.[376]

c. Washington

Most recently, in 2017, Washington passed legislation regulating biometric identifiers such as fingerprints and "other unique biological patterns or characteristics."[377] Like CUBI, Washington's statute regulates data collection for commercial purposes,[378] and requires notice and consent for the collection, sale, and disclosure of biometric information.[379] The statute specifies that commercial purpose means "in furtherance of [a] sale," or via "disclosure to a third party" for marketing purposes.[380]

Similar to the proposed federal act, Washington's biometric information statute exempts notice and consent when data is collected for security purposes.[381] The statute defines "security purposes" as "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."[382] Additionally, the statuterequires that those knowingly in possession of biometric data "take reasonable care to guard against unauthorized access to and acquisition" of that data.[383] The Washington statute also protects consumer data through its retention policy, which allows entities to retain the data only as long as retention is "reasonably necessary" to: (1) "comply with a court order, statute, or public records"; (2) protect against security and other related threats; or (3) provide the services for which the

---

374 *Id.* § 503.001(c)(3).
375 *See id.* § 503.001(d).
376 *See id.* § 503.001(d); *cf.* 740 ILL. COMP. STAT. 14/20 (2008).
377 WASH. REV. CODE § 19.375.010(1) (2017).
378 *See id.* § 19.375.020(3).
379 *See id.* § 19.375.020(1), (3). Written consent is not necessarily required. *See id.*
380 *Id.* § 19.375.010(4).
381 *Id.* § 19.375.020(7).
382 *Id.* § 19.375.010(8).
383 *Id.* § 19.375.020 (4)(a).

information was originally collected.[384] Lastly, like CUBI, this Washington statute is "enforced solely by the attorney general."[385]

d. California

In June 2018, California governor Jerry Brown signed the California Consumer Privacy Act ("CCPA").[386] The Act went into effect January 1, 2020.[387] It is the first U.S. statute modeled on the EU's GDPR.[388] A major component of the statute is its disclosure requirements.[389] The CCPA requires companies to notify consumers about what information it is collecting and why it is collecting that data.[390] Consumers also have the right to request that a business disclose the categories of information it collects, the sources that the information came from, the purposes it collects the information for, the categories of third parties the company shares the information with, and specific pieces of information the company collected.[391] This Act is expected to significantly increase the transparency obligations that California organizations owe consumers.[392] Notably, these transparency requirements apply to all "business purposes," including "security incidents."[393]

The Act also allows consumers to request that a company delete their information.[394] Further, companies must present consumers with an easy way to opt-out of having their information sold to third parties.[395] Additionally, the law provides heightened safeguards for minors: children under sixteen must affirmatively opt-in and

---

384 *Id.* § 19.375.020(4)(b).

385 *Id.* § 19.375.030(2).

386 *See generally* Mark G. McCreary, *California Consumer Privacy Act: What You Need to Know*, N.J. L.J. (Dec. 1, 2018), https://www.law.com/njlawjournal/2018/12/01/the-california-consumer-privacy-act-what-you-need-to-know/?src=EMC-Email&et=CustomAlerts&bu=ALM&pt=CustomAlerts [https://perma.cc/3N44-G9HQ].

387 *See id*.

388 *See id*.

389 *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (2018).

390 *See id.* § 1798.100(b).

391 *See id.* § 1798.100(a).

392 *See Your Readiness Roadmap for the California Consumer Privacy Act (CCPA)*, PWC, https://www.pwc.com/us/en/services/consulting/cybersecurity/california-consumer-privacy-act.html [https://perma.cc/5J6M-QLZK].

393 CAL. CIV. CODE § 1798.105(d)(2).

394 *See id.* § 1798.105(a).

395 *See id.* § 1798.120(a).

children under thirteen must obtain parental consent to have their personal information sold to third parties.[396] Finally, now that the CCPA is in effect, its private cause of action will likely contribute to the increase in litigation spurred by BIPA.[397]

ii. Proposed Regulations

e. New York

New York is also contemplating regulating biometric data.[398] Currently, a bill establishing a biometric privacy act is in the New York Senate's Consumer Protection Committee.[399] The Senate bill proposes regulation of the use of biometric data such as retinas and iris scans, fingerprints, and face geometry[400] by private entities.[401] The bill requires written notice and consent for any collection, storage, or dissemination of data.[402] It also requires a written policy conveying the company's reason for collecting the information and its retention schedule and guidelines for destruction.[403] The bill states that destruction must occur when the original purpose for obtaining the data has been fulfilled or "within three years of the individual's last interaction with the private entity, whichever

---

396 *See id.* § 1798.120(d).

397 *See* Alston & Bird, *The CCPA Could Reset Data Breach Litigation Risks*, JD SUPRA (Aug. 20, 2019), https://www.jdsupra.com/legalnews/the-ccpa-could-reset-data-breach-14801/ [https://perma.cc/M46Q-BYTL].

398 This bill is different than the New York bill discussed in Part III.B.1 because that bill only changes the Education Law. *See* N.Y. Legis. Assemb. A06787 § 2-e, Reg. Sess. 2019–20 (N.Y. 2019). There is also a bill pending in the New York City Council. This bill applies to all privately or publicly owned facilities where athletic games are held. It requires a "clear and conspicuous sign" that states what information is being collected. It also requires online notice of the amount of time the data is collected for, the type of information collected, any privacy policy, and whether the information is sent to third parties. Government agencies are excluded from this bill, and there is both a private and public cause of action. *Requiring Businesses to Notify Customers of the Use of Biometric Identifier Technology Before the Comm. on Consumer Affairs and Bus. Licensing*, N.Y.C. Council 2018 Reg. Sess., Int. No. 1170 (N.Y.C. 2018).

399 *See generally* S.B. S1203, 2019–2020 Leg. Sess. (N.Y 2019), *available at* https://www.nysenate.gov/legislation/bills/2019/s1203 [https://perma.cc/V58J-HSQB].

400 *Id.* § 676-a.

401 *Id.* § 676-b. Note that government agencies are explicitly excluded from this bill, thus raising the issue of how effective this bill will be. *See id.* § 676-a(4).

402 *See id.* § 676-b.

403 *See id.*

occurs first."[404] Additionally, to protect data, companies must use a "reasonable standard of care" to "store, transmit, and protect" information from disclosure.[405] Finally, the bill proposes a private cause of action.[406] New York legislators have been considering this bill for three years, so it appears unlikely that the legislators will pass it.[407]

IV. THE FUTURE OF BIOMETRICS IN SPORTS VENUES: A NATIONAL REGULATION?

This Note has commented on the benefits and concerns of using biometric data in sports venues. While this Note recognizes the benefits of using biometric data, including convenience, safety and security, and customer experience,[408] these benefits are likely outweighed by significant accuracy, security, and privacy concerns.[409] The unique and permanent nature of biometric data makes privacy and security breaches irreparable in a way that does not apply to other data breaches, such as credit card and password breaches.[410] This heightened risk necessitates some degree of monitoring. Though biometric technology can shorten lines,[411] enhance security,[412] and aid advertisers in placing advertisements effectively,[413] these rewards do not outweigh the risks of data breaches[414] and inaccurate technology.[415] Further, regulation must be enacted with urgency to preempt these risks from soon becoming a reality.

A. The FTC's Expertise in Privacy Regulation

The FTC's historic role as the United States' most influential privacy regulator[416] makes it the natural choice as the regulator of

---

404 *Id.*
405 *Id.* § 676-b(5)(A).
406 *See id.* § 676-c.
407 *See* Quinn Emanuel Urquhart & Sullivan, LLP, *supra* note 361.
408 *See supra*, Part II.A.
409 *See supra*, Part II.B.
410 *See* Krishan & Mostafavi, *supra* note 156, at 19.
411 *See supra* Part II.A.1.
412 *See supra* Part II.A.2.
413 *See supra* Part II.A.3.
414 *See supra* Part II.B.1.
415 *See supra* Part II.B.2.
416 *See* Solove & Hartzog, *supra* note 217, at 585.

biometric data, an inherently consumer-centric metric.[417] Sports spectators double as fans and consumers, and thus it is the mission of the FTC to protect them.[418] The FTC's expertise in technology, privacy regulation, and unfair and deceptive trade practices generally makes it the preferred regulator of biometric data. The Commission regulates other technologies such as websites,[419] and has already begun to regulate biometric information.[420] Thus, it should be the FTC, not courts, that enforces misuses of biometric data.[421] Further, the private cause of action that statutes such as BIPA contain has resulted in numerous lawsuits that place a burden on the judiciary's limited time and resources.[422] Additionally, these cases would likely result in a low amount of actual damages for the individuals that bring suits. Thus, bringing a suit is likely not worth the time and money spent on the litigation. Limiting regulation to a designated federal watchdog with expertise in the area—the FTC—would curtail the number of suits and therefore promote judicial economy. Considering the number of people who attend sporting events, and therefore the number of people who could bring suits against venues, the potential for an overwhelming number of lawsuits is substantial.

B. The Importance of Uniformity

Further, this proposed regulatory scheme should be administered at a national level to achieve uniformity across venues in all states. The current ease of nationwide travel makes uniformity particularly important. Inconsistency could inconvenience spectators who would not know what to expect when visiting other states. For example, a devoted member of the Mets 7 Line Army may travel

---

417 *See* Porter, *supra* note 19.

418 *See About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc [https://perma.cc/MZ9V-ANET].

419 *See supra*, Part III.B.2.b.

420 *See supra*, Part III.B.2.b.

421 *See* Trevor Timm, *Technology Law Will Soon Be Reshaped by People Who Don't Use Email*, GUARDIAN (May 3, 2014, 7:30 AM), https://www.theguardian.com/commentisfree/2014/may/03/technology-law-us-supreme-court-internet-nsa [https://perma.cc/E7HA-NBST] (commenting that the Supreme Court's lack of technological knowledge will be detrimental when deciding new issues about technology).

422 *See Judicial Economy Law and Legal Definition*, US LEGAL, https://definitions.uslegal.com/j/judicial-economy/ [https://perma.cc/2ZPD-VW5W].

to the Citizens Bank Park in Philadelphia to attend a Mets-Phillies game.[423] If Citizens Bank Park has different standards than Citi Field for using and regulating biometric technology, that Mets fan will likely not be familiar with the Phillies' stadium standards.[424] Ideally, Congress will pass a national legislation.

However, Congress's first attempt at creating biometric data oversight—the Commercial Facial Recognition Act—is not likely to become law.[425] Further, this Act would only be a partial solution since it only addresses a single type of biometric identifier: commercial facial recognition.[426] Moreover, passing any legislation is a notoriously prolonged process. Due to the many concerns about using biometric data and the grave implications of an insufficient regulation,[427] regulation must be implemented as fast as possible.[428] Thus, until Congress codifies a nationwide legislation, the most practical solution is to defer oversight of biometric technology to the FTC and encourage the Commission to augment its enforcement efforts.[429] The FTC should draw upon its prior decisions in technology privacy cases, as well as the existing state biometric statutes that are paving the way of biometric regulation. In particular, the FTC should encourage maximum protection against data breaches and emphasize meaningful notice and consent, as expanded upon below.

---

423 The 7 Line Army is a group of Mets fans that attend home and away Mets games. *See About Us*, 7 LINE, https://the7line.com/pages/about-us [https://perma.cc/9QLB-5PVH].

424 Citizens Bank Park is the ballpark of the Philadelphia Phillies. *See Citizens Bank Park*, MLB, https://www.mlb.com/phillies/ballpark [https://perma.cc/63AU-93BE].

425 *See* 116 Legislative Outlook S. 847, *supra* note 257; *S. 847: Commercial Facial Recognition Privacy Act of 2019*, *supra* note 257.

426 *See S. 847: Commercial Facial Recognition Privacy Act of 2019*, *supra* note 257.

427 *See supra* Part II.B.

428 Amazon CEO Jeff Bezos supports regulation of facial recognition technology. He states that the technology has "really positive uses, so you don't want to put the brakes on it." Jason Del Ray, *Jeff Bezos Says Amazon Is Writing Its Own Facial Recognition Laws to Pitch to Lawmakers*, VOX (Sept. 26, 2019, 12:55 AM), https://www.vox.com/recode/2019/9/25/20884427/jeff-bezos-amazon-facial-recognition-draft-legislation-regulation-rekognition [https://perma.cc/U7W7-BH48].

429 The recent FTC settlements regarding biometric data could be an indication that the FTC is already increasing its enforcement. *See supra* Part III.B.2.b.

C. Venues Must Protect Spectators from Data Breaches

When venues collect biometric data, they must take all reasonable measures to ensure that data is protected from breaches. Biometric data is an irreplaceable, personal identifier.[430] Once that data becomes public, it cannot be made private again.[431] Thus, like most of the state regulatory schemes currently in effect, the FTC should use a reasonable care standard to protect spectators from the harms of data breaches.[432]

D. Transparency is a Necessity

The current state statutes, as well as prior FTC decisions, require notice and meaningful consent.[433] Two common critiques of the notice component are that consumers do not read the notice, or that the notice is too difficult to locate or comprehend.[434] However, these critiques do not negate the importance of meaningful notice. Progress on regulation will likely halt if people are unaware of what data entities collect. Regulators will not know what to regulate, and consumers cannot provide their input if they do not know that entities collect their data, how the entities use the data, and for how long the data is retained. Stadiums have successfully notified fans of new policies, such as when the NFL changed its bag policy in 2015.[435] The NFL created its new bag policy that only allows small bags or medium-sized clear bags "[t]o provide a safer environment for the public."[436] The NFL disseminated this information through an announcement on its website,[437] updated policies on

---

430 *See* Porter, *supra* note 19.

431 *See* Baraniuk, *supra* note 161.

432 *See, e.g.*, Biometric Information Privacy Act, 2007 Ill. SB 2400 § 15(e)(1) (2008); TEX. BUS. & COM. CODE ANN. § 503.001(c)(2) (West 2019).

433 *See supra* Part III.B. It should be noted that "meaningful consent" does not have a uniform definition. Sometimes consent is only satisfied by writing, whereas other times it can be satisfied verbally or by actions, such as walking in front of a sign with a notice that it uses biometric data. *See id.*

434 *See* Wagner & Sloan, *supra* note 275, at 7–8.

435 *See NFL Stadium Bag Policy*, NFL (last updated Nov. 14, 2015, 3:28 PM), http://www.nfl.com/news/story/0ap3000000579441/article/nfl-stadium-bag-policy [https://perma.cc/FRB4-XSK5].

436 *Id.*

437 *See id.*

team websites,[438] and articles published by independent news sources.[439] Venues should disclose biometric policies through similar communications.

The FTC has already demonstrated that it considers notice of biometric information policies important. In its 2019 settlement with Facebook, the FTC required "clear and conspicuous notice."[440] If the FTC continues to apply this standard to uses of biometric data, as it should, sports venues have many methods by which they can provide spectators with clear and conspicuous notice. For example, venue staff can provide notice by briefing spectators on an applicable fingerprinting policy before they scan their fingerprints.[441] Tickets should also contain notice of such policies.[442] Further, venues should post policies on their websites along with their other procedures, such as bag policies.[443]

Determining what constitutes meaningful consent is a more challenging task. For example, current state statutes disagree about whether written consent is required.[444] To explain the consent prong, the FTC's Best Practice Guidelines used the example of digital signs that recognize demographic characteristics.[445] This directly applies to signage in sports venues such as Madison Square Garden.[446] The FTC used this case study to articulate a sliding scale approach to

---

438 *See, e.g.*, *Guest Policies*, METLIFE STADIUM, https://www.metlifestadium.com/guest-services/guest-policies [https://perma.cc/FK8A-J267].

439 *See, e.g.*, Alex Lockie, *The NFL Is Tightening Security and Asking Patrons Not to Bring Bags to Games After the Attacks on Paris*, BUS. INSIDER (Nov. 14, 2015, 3:35 PM), https://www.businessinsider.com/the-nfl-tightens-security-after-attacks-on-paris-2015-11 [https://perma.cc/G84P-PZEW].

440 FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, *supra* note 291.

441 *See, e.g.*, *Legal Privacy Policy*, CLEAR (last updated Jan. 1, 2020), https://www.clearme.com/privacy_policy [https://perma.cc/4L22-SZK7].

442 Many tickets already do contain notice of biometric policies. *See* Golden & Chemi, *supra* note 9.

443 *See, e.g.*, *Guest Policies*, *supra* note 438. Yet it is critical that these policies are accurate in order to avoid a situation like Nomi where the FTC charged the technology company with misrepresenting its privacy policy. *See* FTC Press Release 2015, *supra* note 93.

444 *See supra* Part III.B.2.d.

445 See FTC, BEST PRACTICES, *supra* note 30, at 13.

446 *See* Draper, *supra* note 5.

notice and consent.[447] The more private the data collected, the higher the standard of consent.[448] For example, walking in front of a sign that a spectator knows detects demographics such as age is consent, whereas more affirmative consent may be required for a sign that can identify a particular individual.[449] This approach seems to balance the customer experience and innovative benefits of collecting biometric information with the aforementioned privacy concerns.

In its recent settlement with Facebook, the FTC required Facebook to obtain "affirmative express user consent prior to any use that materially exceeds its prior disclosures to users."[450] It seems that Facebook interpreted this to mean opt-in, yet it is not clear that was necessarily the FTC's intent.[451] Sports venues could request affirmative express consent in multiple ways. For example, if a vendor disclosed to a spectator, either verbally or with a sign next to the register, that by scanning his fingerprint to purchase a beer, his credit card would be charged and his age would be verified, consent by action should be enough. However, if the machine also recorded that specific spectator's purchases as information to be distributed to third parties, that should require more explicit, affirmative, and express consent such as a signed consent form.

E. Security is No Exception

This Note posits that in the optimal regulatory solution, i.e., a federal scheme administered by the FTC, the Commission should not follow the lead of statutes that except security uses of biometric technology from transparency regulations.[452] If anything, recent evidence of inaccuracies should put venues on notice that the benefits of this technology might not be as sure as they were once thought to be. Security forces can include both government officials stationed at venues and private stadium security. Sporting events'

---

447 *See supra* Part III.B.2.b.

448 *See supra* Part III.B.2.b.

449 For example, running facial recognition data against a database of mugshots. *See* Grossman, *supra* note 56.

450 FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, *supra* note 291.

451 *See supra* Part III.B.2.b.

452 *See, e.g.*, WASH. REV. CODE § 19.375.020(7) (2017).

susceptibility to criminal breaches and terrorist-scale attacks necessitates heightened security.[453] Yet, biometric security technology is not necessarily the means to that end. Perhaps it could be in the future; however, at this point in the development of facial recognition, the technology is too flawed to be effective. Thus, while biometric technology conjures a perception of model security, venues must consider the empirical evidence of inaccuracies with facial recognition technology.[454] The repercussions of inaccurate facial recognition bolster the need for expeditious regulation of such technology.[455] Accordingly, regulators should evaluate not only how to regulate facial recognition's use, but also if venues should use it at all. The FTC should apply the same approach to regulating security uses of biometrics as it does for commercial uses. For example, evidence supports the accuracy of fingerprinting, thus the same notice and consent may be sufficient.[456] However, studies on facial recognition technology reveal its imprecisions, which indicates that this technology may not be ready for stadium use.[457]

Many state and local governments already question the use of facial recognition for security purposes. Cities such as Oakland have banned its local government from using facial recognition,[458] and California's governor recently signed a bill that became effective in 2020, which bans police from using facial recognition on body cameras for three years.[459] Stadiums and arenas are distinct from cities

---

453 *See* WOODWARD, *supra* note 117, at 3.

454 *See* Natasha Singer, *Amazon Is Pushing Facial Technology That a Study Says Could Be Biased*, N.Y. TIMES (Jan. 24, 2019), https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html [https://perma.cc/J6EM-TWP2].

455 *See supra* Part II.B.

456 *See NIST Study Shows Computerized Fingerprint Matching Is Highly Accurate*, NAT'L INST. STANDARDS & TECH. (July 6, 2004), https://www.nist.gov/news-events/news/2004/07/nist-study-shows-computerized-fingerprint-matching-highly-accurate [https://perma.cc/8NG6-EQ27].

457 *See supra* Part II.B.2.

458 *See* Sara Merken, *Berkeley Bans Government Face Recognition Use, Joining Other Cities*, BLOOMBERG L. (Oct. 16, 2019, 2:22 PM) https://news.bloomberglaw.com/privacy-and-data-security/hold-berkeley-bans-government-face-recognition-use-joining-other-cities (subscription paywall).

459 *See* Bryan Anderson, *New Law Bans California Cops from Using Facial Recognition Tech on Body Cameras*, SACRAMENTO BEE (Oct. 8, 2019, 7:38 PM), https://www.sacbee.com/news/politics-government/capitol-alert/article235940507.html.

and states because they are private venues where obtaining and regulating notice and consent is plausible. This gives spectators more autonomy over their data than a person walking on a public street.

Yet the FTC must still consider the unavoidable harms of flawed biometric security technology. When entities inaccurately collect information for commercial or trade purposes, the potential harm is an improperly targeted advertisement; when entities inaccurately collect information for security purposes, the potential harm is an undetected criminal or an innocent person falsely accused of a crime. This potential for substantial, grave ramifications seems to fit directly into the FTC's description of an unfair trade practice—"likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[460] Thus, until facial recognition technology is improved, an FTC-enforced moratorium on its use for security at sports venues is justified and should be implemented as soon as possible to avoid injury to spectators.

CONCLUSION

Determining how to regulate new technologies and their corresponding data mining is a formidable feat, particularly when the technology is so new that it is still developing and its implications are still being discovered. Though not a flawless remedy, looking to existing biometric regulations and regulations of similar technologies and data can help guide that determination. To promote unity, there should be a single, national regulation. While a federal statute would achieve this, the uncertainty surrounding this new biometric technology calls for instant regulation. Thus, the FTC is best positioned to develop and enforce immediate regulation of biometric data. While state statutes govern portions of the country, the FTC is able to uniformly regulate the entire country. Additionally, the FTC has an extensive history in regulating new technologies that

---

[460] *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, *supra* note 195.

could pose privacy concerns.[461] Therefore, the FTC should extend the notice-and-consent regime it already applies to technologies similar to biometric technology. Further, the FTC should require entities to take utmost care to prevent breaches of spectator data. In doing so, the FTC is positioned to uncover deceptive and unfair practices and enforce policy breaches while still allowing the convenience and security benefits that biometric technology strives to provide.

461 *See supra* Part IV.A.