TOWARD A BIOMETRIC PRIVACY ACT TO PROTECT INDIVIDUAL RIGHTS: WHAT THE UNITED STATES CAN LEARN FROM THE EUROPEAN UNION AND CHINA

*Sophia Hilsman**

* Online Editor, Cardozo International & Comparative Law Review; J.D. Candidate 2024, Benjamin N. Cardozo School of Law; B.A. 2014, University of Virginia. I would like to thank professors Alexander A. Reinert and Yuval Shany for their helpful feedback; the editors and especially the executive board of the Cardozo International & Comparative Law Review for their diligence and thoughtful suggestions; and my friends and family for their unending support throughout the writing process.

I. INTRODUCTION

Many of us leave our homes each day to go about our business in public without thinking twice about our privacy, whether it is on our way to school, work, or the grocery store. We may be seen by others walking past us, by CCTV cameras on the street, and we may even appear in the background of people's photos as we pass by. We sit in restaurants and talk about our private lives with our friends, knowing that even if the person next to us overhears, they do not know our identity or background. If someone unfamiliar to you could instantly identify you as you go about your day, however, perhaps to a religious service, a doctor, or a political group meeting, you may lose the comfort of anonymity in public. What if you are not only identified out of a crowd, but also quickly linked to other data, like your address, job, movements, and friends' names, which could be stored, stolen, and misused? Biometric technologies using artificial intelligence ("AI"), especially facial recognition, contain these risks. What was once taboo—deploying technology to identify strangers—is now a reality.

In 2023, there were over 500 biometrics companies in the United States.[1] Biometric AI is becoming increasingly prevalent in our lives,

1 *Biometric Companies*, SEC. INFORMED, https://www.securityinformed.com/companies.html?product_area=biometrics&country=united-states-of-america&type=manufacturers [https://perma.cc/Y7CG-PDZ2] (last visited Feb. 4, 2024, 10:33 AM).

from using our faces to unlock our phones to using our palms to check out at the grocery store. Biometric recognition or "biometrics" is the "automated recognition of individuals based on their biological and behavioral characteristics."[2] Biometric identifiers include retina or iris scans, fingerprints, voiceprints, scans of hand or face geometry,[3] behavioral biometrics such as gait, and genetics, including DNA.[4] Technology that collects and uses biometric data is becoming increasingly sophisticated and widespread. Yet, its use in the United States is mostly regulated by an insufficient patchwork of state and local laws with no comprehensive federal regulation.

This Note examines the current state of biometric AI usage and regulation in the United States, China, and the European Union. It analyzes and compares the United States' legal framework with the approaches employed by China and the European Union to construct an ideal framework for avoiding the destruction of our privacy and erosion of our civil liberties. It will examine all biometric data types and uses, with a focus on facial recognition and similar biometrics that can be used for remote identification.

Part II provides a background on biometrics and the advantages and risks of using biometric data in the private and public sector. It focuses on the dangers of biometric identification through mass surveillance. Part III provides a background on biometric data use in the United States and the current legal landscape at the federal, state, and local levels. Part IV examines China's approach, which engages in widespread biometric collection and surveillance with minimal restraints on the government and only recent regulation of the private sector. Part V explores the European Union, which has enacted and proposed significant regulation. Part VI then argues that remote biometric identification, especially through real-time technology, threatens our privacy, our fundamental rights, and even our democracy. It argues that the United States needs to urgently protect against these threats through federal regulation enacted by Congress, as opposed to state action, executive power, or courts alone. Finally, through lessons from a comparison of the United States', China's, and the European

---

2 SUBCOMM. ON INVESTIGATIONS & OVERSIGHT OF THE U.S. HOUSE OF REPS. COMM. SCI., SPACE, & TECH., 117TH CONG., HEARING CHARTER: PRIVACY IN THE AGE OF BIOMETRICS 2 (2022) [hereinafter 2022 HEARING CHARTER], https://www.congress.gov/117/meeting/house/114964/documents/HHRG-117-SY21-20220629-SD002.pdf [https://perma.cc/E6QK-5ZMU].

3 *Id.*

4 *See* Margaret Hu, *Biometrics and an AI Bill of Rights*, 60 DUQ. L. REV. 283, 286 (2022); 2022 HEARING CHARTER, *supra* note 2, at 2.

Union's current regulatory frameworks, this Note proposes suggestions for such a federal regulation.

II. BACKGROUND

A. The Basics of Biometrics

Biometrics are unique to an individual. Biometric recognition generally involves either verification or identification. Biometric verification (also known as authentication) seeks to confirm whether a person is who they claim to be, which involves one-to-one matching between a scanned biometric trait (e.g., a face scan) and an existing template identifying the individual (e.g., a stored facial image).[5] Alternatively, biometric identification seeks to identify an unknown person, which involves "one-to-many matching" by comparing a scanned trait to an entire database to find a potential match.[6] Biometric data, primarily from facial recognition, can also be used for characterization (also known as "categorization") to use "images to identify broad demographic information . . . [without connecting] the biometric data to a specific identity."[7] Finally, biometrics can be used for detection, where AI uses biometric data to detect if the scanned trait is a human face, or even a face exhibiting a certain emotion.[8] Biometric AI software analyzes data in a database, such as photos, and learns to predict which images show the same person; the more images or data in the database, the better the predictions.[9]

Unlike fingerprinting, facial recognition and certain other new biometric identification systems constitute what scholar Laura Donohue calls "Remote Biometric Identification" ("RBI"), which "give[s] the [user] the ability to ascertain the identity (1) of multiple people; (2) at a distance; (3) in public space; (4) absent notice and consent; and (5) in a continuous and on-going manner."[10] Depending on the jurisdiction, violations of privacy can occur when biometric data (1) is collected, retained, or used without an individual's knowledge or consent; (2) is used or misused for an unauthorized purpose; or (3) is exposed

---

5 Hu, *supra* note 4, at 286.

6 2022 HEARING CHARTER, *supra* note 2, at 2.

7 *Id.*

8 *Id.*

9 *Id.*

10 Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 468 (2012).

to unauthorized third parties.[11] Unlike social security numbers that can be changed if they are compromised, biometric identifiers cannot be changed if a database storing biometric data is compromised, leaving the individual without recourse and at heightened risk for identity theft.[12] Because biometric identifiers are unique to every individual, it is appealing to governments and the private sector to use such data for identification, verification, characterization, and detection.

B. Benefits of Biometric Technology

Biometric technologies are rapidly evolving and impacting the status quo of many sectors. The convenience and efficiency of using biometric verification for consumers is undeniable. Verifying your identity with one's fingerprints, palm, or face, is simple and fast. For example, people can spend less time in airport lines where biometric authentication is offered.[13] Because no two biometric identifiers are the same, biometric authentication offers a tool to combat fraud and identity theft, especially for personal transactions.[14] Using biometrics for account and device logins like Apple's Face ID enhances security over traditional passwords that can be guessed.[15] Biometric AI also offers companies a way to further tailor advertising based on biometric characterization. Biometric emotion detection could also be used to help determine if drivers are alert, if patients are in pain, or if people are sick.[16]

In the public sector, biometric identification has helped law enforcement apprehend criminals, suspected terrorists, and human

---

11 2022 HEARING CHARTER, *supra* note 2, at 2.

12 740 ILL. COMP. STAT. ANN. 14/5(c) (West 2008).

13 Jennifer Bradley Franklin, *How Airports Are Using Biometrics so You Can Spend Less Time Waiting in Lines*, CONDÉ NAST TRAVELER (Nov. 15, 2021), https://www.cntraveler.com/story/how-airports-are-using-biometrics-so-you-can-spend-less-time-waiting-in-lines [https://perma.cc/JQ9R-YM5T].

14 Louis Columbus, *Why Your Biometrics Are Your Best Password*, FORBES (Mar. 8, 2020, 12:38PM), https://www.forbes.com/sites/louiscolumbus/2020/03/08/why-your-biometrics-are-your-best-password/ [https://perma.cc/7BEM-9U66].

15 Kashmir Hill, *Your Face Is Not Your Own*, N.Y. TIMES (Mar. 18, 2021), https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html [https://perma.cc/9H2M-SG5X].

16 *See* Tate Ryan-Mosley, *AI Isn't Great at Decoding Human Emotions. So Why Are Regulators Targeting the Tech?*, MIT TECH. REV. (Aug. 14, 2023), https://www.technologyreview.com/2023/08/14/1077788/ai-decoding-human-emotions-target-for-regulators/ [https://perma.cc/4EWH-A9K7].

traffickers.[17] The Department of Homeland Security has found wanted criminals in child exploitation cases using facial recognition software from Clearview AI, a particularly controversial AI company.[18] Proponents argue that the technology will end human trafficking and make the world safer.[19]

C. Harms of Biometric Technology

1. Harms Related to Both Public and Private Sector Use

There are many possible harms that can result from both private and public sector actors' collection and use of biometric data. Creating unique biometric templates from a person's physical features and transforming them into digital data leads to what some call the "datafication of humans."[20] The "datafication" violates their personal autonomy and dignity by objectifying the human body and allowing others to use this unique data for their own aims.[21]

Relatedly, individuals' privacy is at risk if their data is misused or accessed by unauthorized parties. People cannot change or encrypt their faces, eyes, or other biometrics, certain features are remotely capturable, and all are inexpensive to collect and store.[22] Anyone who has access to databases storing biometric data, can track, surveil, or

---

17 *INTERPOL Unveils New Biometric Screening Tool*, INTERPOL (Nov. 29, 2023), https://www.interpol.int/en/News-and-Events/News/2023/INTERPOL-unveils-new-biometric-screening-tool [https://perma.cc/NWB8-CNF6].

18 Thomas Brewster, *Exclusive: DHS Used Clearview AI Facial Recognition in Thousands of Child Exploitation Cold Cases*, FORBES (Aug. 7, 2023, 3:52 PM), https://www.forbes.com/sites/thomasbrewster/2023/08/07/dhs-ai-facial-recognition-solving-child-exploitation-cold-cases/ [https://perma.cc/BT3Y-2XX5]. Clearview AI scraped, without knowledge or consent, existing photos from the internet, to create its database currently stated to include 20 billion images. 2022 HEARING CHARTER, *supra* note 2, at 6.

19 *See* Joshua Lee, *How Technology Can Help Law Enforcement Fight Human Trafficking*, POLICE1 (May 18, 2023, 6:18 PM), https://www.police1.com/investigations/articles/how-technology-can-help-law-enforcement-fight-human-trafficking-KYJfdLKcQAygFSKD/ [https://perma.cc/95DV-PZCJ]; Brewster, *supra* note 18.

20 CHRISTIANE WENDEHORST & YANNIC DULLER, BIOMETRIC RECOGNITION AND BEHAVIOURAL DETECTION 44 (2021) [hereinafter IPOL Report], https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf [https://perma.cc/R75D-YU8Z].

21 *Id.*

22 Woodrow Hartzog, *Facial Recognition Is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66 [https://perma.cc/9J2L-D5DC].

duplicate the templates to commit identity fraud.[23] This makes biometric data security very important. Other forms of misuse can include facilitating harassment, stalking, and violence.[24] These databases and algorithms that match a biometric identifier like a face print to an existing template are often populated with data (e.g., facial images) taken or "scraped" without consent, intruding on privacy.[25]

Biometric emotion detection is also problematic because the nascent technology has accuracy issues, in part because of the "Hawthorne Effect," where people alter their behavior when they think they are being observed.[26] Emotion detection also raises manipulation fears and has been particularly controversial in employment contexts, policing (where it is used to identify nervousness), and schools.[27]

2. Harms Specific to Public Sector Use

Facial recognition and, more recently, iris and voice recognition, allow for RBI at scale. With increasing governmental biometric surveillance in public spaces, several possible harms to the public arise. A government actor with widespread remote biometric surveillance capabilities can identify individuals in real time and track their movements.[28] This remotely captured biometric data can be aggregated with other biometric, personal, and social media data to create detailed profiles of individuals, impinging on their private lives and allowing actors with this data to monitor and exercise a form of social control.[29] To be used effectively, these surveillance systems collect, process, and retain data on a massive scale.[30] These surveillance capabilities could eliminate the anonymity, and even the practical obscurity or "privacy in public" that one might expect when walking down a crowded street. Unlike complete anonymity or "face in the crowd privacy," obscurity is the idea "that information is safe—at least to some degree—when it is hard to obtain or understand."[31]

---

23 *See* IPOL Report, *supra* note 20, at 45.

24 *See* Hill, *supra* note 15.

25 2022 HEARING CHARTER, *supra* note 2, at 6.

26 *See* Jonathan Turley, *Anonymity, Obscurity, and Technology: Reconsidering Privacy in the Age of Biometrics*, 100 B.U. L. REV. 2179, 2229 (2021)..

27 IPOL Report, *supra* note 20, at 9; Tate Ryan-Mosley, *supra* note 16.

28 IPOL Report, *supra* note 20, at 44.

29 *See id.* at 46; Ryan-Mosley, *supra* note 16.

30 Rep. of the Off. of UN High Comm'r for Hum. Rts., *The Right to Privacy in the Digital Age*, ¶ 44, U.N. Doc. A/HRC/51/17 (Aug. 4, 2022).

31 Evan Selinger & Woodrow Hartzog, *Obscurity and Privacy*, *in* SPACES FOR THE FUTURE: A COMPANION TO PHILOSOPHY OF TECHNOLOGY 119, 119 (Joseph C.

Accuracy is another concern. Automated decisions or predictive analyses based on an inaccurate match from a biased algorithm can harmfully affect individuals. If law enforcement uses facial recognition that inaccurately identifies someone, that person may be wrongfully arrested, stopped, harassed, or even harmed.[32] Biometric emotion detection can also be inaccurate, but could be the basis of further characterization and identification.[33] One federal agency found that many facial-recognition algorithms were less accurate in identifying people of color,[34] and an MIT study found that images of darker-skinned women were misclassified by three commercial algorithms over twenty percent of the time, compared to less than one percent of the time for men with light skin.[35]

On a societal scale, the potential effect of biometric surveillance on democratic participation and on people exercising their constitutional rights is particularly concerning. One study evaluating artificial intelligence regulation argued that the critical issue of mass biometric surveillance is that it interferes with individuals' self-determination.[36] Feeling constantly surveilled can alter how individuals interact with each other in public spaces, affecting freedom of speech, expression, and assembly.[37] One privacy scholar argues that the mere existence of facial recognition is enough to raise people's suspicions that they are being surveilled and it thus harms civil liberties.[38] Biometric

---

Pitt & Ashley Shew eds., 2016). There is an idea of "privacy in public" when people seek to keep some interactions private, despite being in public (e.g., a conversation with a friend or a kiss) which really are about obscurity, rather than about complete secrecy. *Id.* at 119-20.

32 In 2021, police officers jailed the wrong person (all black men) based on an inaccurate match in at least three cases. Hill, *supra* note 15.

33 *See* IPOL Report, *supra* note 20, at 21.

34 *Id.* at 9.

35 Nicol Turner Lee & Caitlin Chin-Rothmann, *Police Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color*, BROOKINGS (Apr. 12, 2022), https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ [https://perma.cc/83EV-M2GD]. One way to combat inaccuracy is to combine multiple biometric identifiers for identification, however that means more biometric data collection, and more opportunities to infringe on people's privacy. IPOL Report, *supra* note 20, at 14.

36 IPOL Report, *supra* note 20, at 48.

37 This is known as the Hawthorne Effect. *See* Turley, *supra* note 26.

38 Hartzog, *supra* note 22.

surveillance could leave "no room for free speech, free thought, dissent, or human rights."[39]

Individuals may fear that their behavior is being scrutinized,[40] which could lead them to fear retribution for their activities, such as making sensitive healthcare visits or participating in protests or religious organizations. The feeling of constant surveillance could seriously threaten individuals' rights to free speech and peaceful assembly, which help ensure participation in a democracy.[41] While the threat of surveillance extends beyond the form of biometric surveillance, it is important for people to be able to peaceably assemble without fear of retribution for democracies and protecting political rights broadly. Biometric identification, characterization, and detection technologies are a powerful tool that governments can use to suppress opposition even preemptively, monitor and profile populations, and exercise a form of control.[42]

III. CURRENT USE AND LEGAL APPROACH IN THE UNITED STATES

A. Current Biometric Use

1. Federal Government Use

This Section will first introduce biometric uses in the United States by the federal, state, and local governments, and by private entities. The federal government has been using biometric systems for security and law enforcement purposes since at least the 1960s.[43] Fingerprint databases were used long before September 11, 2001.[44] September 11 triggered a shift in the U.S. government's effort to use biometrics in federal and state government agencies, initially in the name of border security.[45] After September 11, numerous departments, including the Department of Homeland Security ("DHS"), the Department of Justice ("DOJ"), Department of State ("DOS"), and

39 Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591, 1594 (2017).

40 IPOL Report, *supra* note 20, at 48.

41 *Id.* at 47; U.N. Doc. A/HRC/51/17, *supra* note 30, ¶ 47.

42 U.N. Doc. A/HRC/51/17, *supra* note 30, ¶ 45.

43 2022 HEARING CHARTER, *supra* note 2, at 3.

44 Donohue, *supra* note 10, at 420.

45 *Id.*

Department of Defense ("DOD"), each created new biometric programs.[46] Biometric usage by the federal government has since proliferated.[47]

Under the Trump Administration, DHS was required to complete a biometric entry-exit tracking system.[48] The Office of Biometric Identity Management under DHS currently oversees the IDENT database, which contains an estimated 300 million unique identities and claims to process over 400,000 biometric transactions daily.[49] The U.S. Government Accountability Office found that half of the forty-two federal agencies that employ law enforcement use facial recognition technology, including technology from Clearview AI.[50] Notably, Clearview AI was used to identify individuals involved in the riot at the U.S. Capitol on January 6, 2021.[51] The Transportation Security Administration ("TSA") is running pilot programs at certain airports for biometric identity authentication.[52] More recently, iris biometrics have been expanding, and the iris depository maintained by the Federal Bureau of Investigation ("FBI") has reached 2.5 million individuals.[53]

2. State and Local Use

Thousands of police departments utilize Clearview's facial recognition technology.[54] One study estimated that around 25% of state and

---

46 *Id.* at 425.

47 U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-106100, FACIAL RECOGNITION TECHNOLOGY: FEDERAL AGENCIES' USE AND RELATED PRIVACY PROTECTIONS 8 (2022), https://www.gao.gov/assets/gao-22-106100.pdf [https://perma.cc/9WU8-AWBB].

48 Hu, *supra* note 4, at 289.

49 *Biometrics*, DEP'T HOMELAND SEC., https://www.dhs.gov/biometrics [https://perma.cc/EA6F-D42D] (Mar. 4, 2024).

50 U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-105309, FACIAL RECOGNITION TECHNOLOGY: FEDERAL LAW ENFORCEMENT AGENCIES SHOULD HAVE BETTER AWARENESS OF SYSTEMS USED BY EMPLOYEES (2021), https://www.gao.gov/assets/gao-21-105309.pdf [https://perma.cc/N98N-MW77].

51 Kashmir Hill, *The Facial-Recognition App Clearview Sees a Spike in Use After Capitol Attack*, N.Y. TIMES, https://www.nytimes.com/2021/01/09/technology/facial-recognition-clearview-capitol.html [https://perma.cc/SM64-WXMP] (Jan. 31, 2021).

52 GAO-22-106100, *supra* note 47, at 15.

53 Bianca Gonzalez, *FBI's Iris Biometrics Repository Reaches 2.5 Million with Tech from Iris ID*, BIOMETRIC UPDATE (June 27, 2023, 5:20 PM), https://www.biometricupdate.com/202306/fbis-iris-biometrics-repository-reaches-2-5-million-with-tech-from-iris-id [https://perma.cc/269V-TQYP].

54 2022 HEARING CHARTER, *supra* note 2, at 7.

local law enforcement agencies had access to facial recognition technology.[55] Clearview's founder claimed that, as of March 2021, 3,100 law enforcement agencies had used its facial recognition software.[56] Data show that forty New York Police Department ("NYPD") officers ran over 11,000 searches using Clearview, while the New York State Police ran over 5,100 searches.[57] Multiple local law enforcement agencies used facial recognition technology to identify protesters during Black Lives Matter protests, including police departments in New York City, Philadelphia, and Miami.[58] Department of Motor Vehicle ("DMV") offices and correctional facilities also use biometrics.[59]

3. Private Sector Use

The use of biometric authentication by U.S. companies almost tripled from 2019 to 2022.[60] For example, Amazon One uses machine learning to create "palm signatures" linked to customers' payment information, enabling customers to pay at participating stores by scanning their palm.[61] This palm print biometric payment system is currently being implemented in over 500 Amazon-owned Whole Foods

---

55 Lee & Chin-Rothmann, *supra* note 35.

56 Ryan Mac, Caroline Haskins, Brianna Sacks & Logan McDonald, *Surveillance Nation*, BUZZFEED NEWS (Apr. 9, 2021, 7:52 PM), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition [https://perma.cc/KS8L-LQAH]. Clearview offered free trials to local government and law enforcement agencies. *Id.*

57 *Id.*

58 Kate Cox, *Cops in Miami, NYC Arrest Protestors from Facial Recognition Matches*, ARS TECHNICA (Aug. 19, 2020, 4:45 PM), https://arstechnica.com/tech-policy/2020/08/cops-in-miami-nyc-arrest-protesters-from-facial-recognition-matches/ [https://perma.cc/5RRU-A6PE].

59 *See* Justin Lee, *NY DMV Use of Facial Recognition Resulted in More Than 4000 Arrests Since 2010*, BIOMETRIC UPDATE (Aug. 22, 2017, 2:01 PM), https://www.biometricupdate.com/201708/ny-dmv-use-of-facial-recognition-resulted-in-more-than-4000-arrests-since-2010 [https://perma.cc/UD4D-E9KX]; Simon McCormack, *Inaccurate Facial Recognition in Prisons is Keeping Families Apart*, NYCLU (Mar. 17, 2023), https://www.nyclu.org/commentary/inaccurate-facial-recognition-prisons-keeping-families-apart [https://perma.cc/PFN9-48B6].

60 Alessandro Mascellino, *Biometric Authentication Use in US Businesses Tripled over 3 Years to Tackle Cyber Threats*, BIOMETRIC UPDATE (Sept. 21, 2022, 1:07 PM), https://www.biometricupdate.com/202209/biometric-authentication-use-in-us-businesses-tripled-over-3-years-to-tackle-cyber-threats [https://perma.cc/L6NV-BKEW].

61 Lauren Forristal, *Amazon Expands Palm-Scanning Payment Tech to 65 More Whole Foods Locations*, TECHCRUNCH (Aug. 10, 2022, 12:58 PM), https://techcrunch.com/2022/08/10/amazon-expands-palm-scanning-payment-tech-to-65-more-whole-foods-locations/ [https://perma.cc/R6K4-8T39].

stores, as well as in various sports and entertainment venues.[62] Red Rocks Amphitheatre in Colorado was planning on using the same technology to check people into a concert but this was met with swift backlash over fears that Amazon would share data with law enforcement, in addition to general unease with it storing biometric data.[63] Still, biometric authentication and identification could increasingly be used for access to stadiums, concert venues, and events.[64]

Companies are also testing, developing, and selling their technology and database access to government actors. Retailers are also using facial recognition to prevent shoplifting and provide personalized advertising. For example, Macy's uses facial recognition in certain stores "with high incidences of organized retail theft and repeat offenders."[65]

B. Current Legal Approach

1. Federal

No uniform current federal regulation directly prevents the government or private sector from using biometric technologies to collect and use citizens' data. The Privacy Act of 1974 governs *federal* "collection, use, and disclosure of personally identifiable information," but does not provide "robust protection of the types of technologies that mark the biometrics realm."[66] The Privacy Act of 1974 does not regulate state and local governments, private entities, companies, non-resident aliens, and foreigners.[67] Several exemptions further limit the Act's impact, including an exemption for records maintained by the Central Intelligence Agency ("CIA") or law enforcement, and record systems that concern classified information pursuant to rulemaking by the head of any federal agency.[68] While no general data privacy

62 Sarah Perez, *Amazon's Palm-Scanning Payment Technology Is Coming to All 500+ Whole Foods*, TECHCRUNCH (July 20, 2023, 7:11 AM), https://techcrunch.com/2023/07/20/amazons-palm-scanning-payment-technology-is-coming-to-all-500-whole-foods/ [https://perma.cc/R97V-EDZZ].

63 *Id.*

64 Khari Johnson, *Get Used to Face Recognition in Stadiums*, WIRED (Feb. 2, 2023, 8:00 AM), https://www.wired.com/story/get-used-to-face-recognition-in-stadiums/ [https://perma.cc/3FF3-AL3T].

65 Hannah Towey, *The Retail Stores You Probably Shop at that Use Facial-Recognition Technology*, BUS. INSIDER (July 19, 2021, 1:14 PM), https://www.businessinsider.com/retail-stores-that-use-facial-recognition-technology-macys-2021-7 [https://perma.cc/CVA3-64F4].

66 Donohue, *supra* note 10, at 468.

67 *Id.* at 471.

68 *Id.* at 472-74.

proposals have passed yet, several have been proposed in the past, including the American Data Privacy and Protect Act ("ADPPA") in 2022.[69] Most recently, President Biden's Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence calls on Congress to pass bipartisan legislation.[70]

Citizens could look to the Federal Trade Commission ("FTC") to protect their biometric privacy interests, but its powers are limited. The FTC is empowered to protect consumers in several ways, including through enforcement under section 5 of the Federal Trade Commission Act ("FTCA").[71] Under section 5, the FTC can bring an enforcement action against a commercial entity that engages in an "unfair or deceptive act."[72] However, it can only seek civil monetary penalties after an FTC order is violated.[73]

The FTC has brought "hundreds of privacy and data security cases," but in 2021, the agency signaled its willingness to go further to protect consumers' biometric data. The FTC Commissioner even called facial recognition technology "discriminatory and dangerous."[74] Notably, the FTC investigated and sued Everalbum, Inc. over misrepresentations it made about its mobile photo application's settings. Everalbum used facial recognition technology in its "Friends" feature to sort and tag users' photos.[75] The default setting activated the

---

69 The bill's principles rest on data minimization, a duty of loyalty, privacy by design, and nondiscrimination. Individuals would have rights of access, correction, deletion, and portability. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. §§ 101-103 (2022).

70 Exec. Order No. 14110, 88 Fed. Reg. 75191 (Nov. 1, 2023).

71 *See* 15 U.S.C. § 45(a) (1975).

72 *See id.* § 45(a)(1) (prohibiting "unfair or deceptive acts or practices in or affecting commerce").

73 FED. TRADE COMM'N, FTC REPORT TO CONGRESS ON PRIVACY AND SECURITY 1 (2021), https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf [https://perma.cc/82F2-NXUH]. For Section 5 violations the FTC may require the entity to implement a comprehensive privacy and security program. *Id.*

74 Chris Burt, *FTC Declares Facial Recognition Surveillance Tech Dangerous, Warns Against Federal Privacy Pre-emption*, BIOMETRIC UPDATE (Jan. 12, 2021, 12:41 PM), https://www.biometricupdate.com/202101/ftc-declares-facial-recognition-surveillance-tech-dangerous-warns-against-federal-privacy-pre-emption [https://perma.cc/US9U-5N9B].

75 *See* Nerissa Coyle McGinn, *FTC, Federal and State Lawmakers Signal Focus on Biometric Data*, LOEB & LOEB LLP (Mar. 2021), https://www.loeb.com/en/insights/publications/2021/02/ftc-federal-and-state-lawmakers-signal-focus-on-biometric-data [https://perma.cc/3H4J-5FAD]; Press Release, Fed. Trade Comm'n, FTC Finalizes Settlement with Photo App Developer Related to Misuses of Facial Recognition Technology (May 7, 2021) https://www.ftc.gov/news-

face recognition "Friends" feature, which could not be turned off, except in Illinois, Texas, and Washington (states with biometric data laws), despite representing to customers that it would not do so without their affirmative consent.[76] Everalbum also collected millions of facial images to compile a database to train AI facial recognition technology for commercial clients.[77] The company's settlement with the FTC required the company to obtain consumers' express consent before using the feature, delete photos and videos from users who deactivated their accounts, and for the first time, delete its facial recognition algorithms developed through the use of Everalbum users' photos or videos.[78]

In August 2022, the FTC issued an Advanced Notice of Proposed Rulemaking ("ANPRM") seeking public comment on commercial surveillance and lax data security practices.[79] The FTC sought public comment "on whether new rules are needed to protect people's privacy and information in the commercial surveillance economy," signaling a shift towards regulation.[80] In May 2023, the FTC issued a policy statement about the ways that misused biometric information harms consumers and warned vendors that making false or unsubstantiated claims about accuracy or efficacy of biometric technologies may violate the FTCA.[81] For the first time, the FTC set forth how it will evaluate companies' behavior to determine what is "unfair" or

---

events/news/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse-facial-recognition-technology [https://perma.cc/SGG8-9MHM]; Complaint, In re Everalbum, Inc., FTC File No. 1923172, Dkt. No. C-4743, ¶ 3, 5, (May 7, 2021).

76 McGinn, *supra* note 75. Everalbum further represented that it would delete photos of Ever users who deactivated their accounts but instead retained them indefinitely. *Id.*

77 *Id.*

78 *Id.*

79 Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (Aug. 22, 2022). The ANPRM's focus on commercial surveillance sought comment on biometric surveillance and security practices due to the scale of data collection and the associated harms. *See generally id.*

80 FED. TRADE COMM'N, FACT SHEET ON THE FTC'S COMMERCIAL SURVEILLANCE AND DATA SECURITY RULEMAKING 1 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Commercial%20Surveillance%20and%20Data%20Security%20Rulemaking%20Fact%20Sheet_1.pdf [https://perma.cc/HT4K-9VQM].

81 *See* FED. TRADE COMM'N, POLICY STATEMENT ON BIOMETRIC INFORMATION AND SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT 6 (2023) [FTC POLICY STATEMENT], https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf [https://perma.cc/N66C-NXD3].

"deceptive" in the biometrics realm.[82] Even if certain biometric collection practices could be deemed unfair or deceptive, the FTC's deterrent powers are limited because it cannot seek civil penalties for first-time violations of section 5.

2. States

In the absence of a federal privacy law, Illinois, Washington, and Texas have passed comprehensive biometric-specific privacy laws that regulate private entities. Illinois' law, the Biometric Privacy Information Act ("BIPA") is most notable because it contains a private right of action for any person "aggrieved by a violation of [BIPA]" and individuals can recover damages of $1,000 against a private entity for negligent violations of BIPA or $5,000 for intentional or reckless violations.[83] The legislature enacted BIPA to protect consumers in biometric-facilitated transactions with the aim that "[t]he public welfare, security, and safety [would] be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[84] It is based on a notice and consent framework; entities must not collect such information or subsequently disclose it unless they provide notice and obtain consent from the individual.[85]

Under BIPA, anyone "aggrieved by a violation of [BIPA]" may bring a claim;[86] actual damage is not necessary.[87] In *Rosenbach v. Six Flags Entertainment Corporation*, the plaintiff sued Six Flags, claiming that the theme park violated BIPA for fingerprinting her son during a school field trip.[88] To finish signing up for a season pass, her son was required to scan his thumb.[89] The Illinois Supreme Court held that a person does not need to sustain actual damage, beyond the violation of their statutory rights, to bring a claim under BIPA.[90] Courts have also held that companies are subject to claims each time they violate BIPA by collecting or transmitting a person's biometric identifiers or

---

82 *Id.* at 7.
83 740 ILL. COMP. STAT. 14/20 (2008).
84 *Id.* at 14/5(g).
85 *See id.* at 14/10, 14/15(d)(1).
86 *Id.* at 14/20.
87 Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1207 (Ill. 2019).
88 *Id.* at 1200.
89 *Id.*
90 *Id.* at 1207.

information without informed consent, leading to potentially enormous statutory damages.[91]

In *Patel v. Facebook*, the Ninth Circuit Court of Appeals found that the class-action plaintiffs had both BIPA and Article III standing.[92] The suit against Facebook concerned the "Tag Suggestions" feature, which used facial-recognition technology to identify a match and suggest tagging that person.[93] The Ninth Circuit concluded that BIPA protected the class's concrete privacy interests and that violations of the procedures in BIPA harmed those interests sufficiently to confer Article III standing.[94] The court concluded that developing a face template database to enable the matching without consent invades an individual's "private affairs and concrete interests."[95] Facebook settled the lawsuit for $650 million.[96]

Similarly, the Texas Attorney General sued Google in October 2022 for allegedly collecting and using biometric data on millions of Texans without their consent in connection with Google's Photos app, Assistant, and Nest products.[97] Under Texas's Capture or Use of Biometric Identifier ("CUBI") law, private entities must give notice and obtain consent before collecting biometric information and must follow limitations on retention, destruction, sale, disclosure, and security of the data.[98] Washington's statute, the Washington Biometric Privacy Act ("WBPA"), is also based on notice and consent.[99] However, the

---

91 Cothron v. White Castle Sys., Inc., 216 N.E.3d 918, 928 (Ill. 2023) (defendant argued damages could be over $17 billion for collecting and using employee fingerprint scans without consent). See also *Rogers v. BNSF Railway Co.*, 680 F. Supp. 3d 1027 (N.D. Ill. June 30, 2023), where a jury had previously found that the defendant truck company violated BIPA over 45,000 times, or once per driver, when requiring truck drivers to scan fingerprint before entering defendant employer's railyard. *Id.* at 1032. The district court subsequently vacated the jury's damages award of $228 million, however, citing dicta in *Cothron* that BIPA's Section 20 suggests damages are subject to the fact finder's discretion. *Id. at 1040-41.*

92 Patel v. Facebook, Inc., 932 F.3d 1264, 1275 (9th Cir. 2019).

93 *Id.* at 1268.

94 *Id.* at 1275.

95 *Id.* at 1273.

96 *Judge Approves $650M Facebook Privacy Lawsuit Settlement*, AP (Feb. 26, 2021, 11:29 PM), https://apnews.com/article/technology-business-san-francisco-chicago-lawsuitsaf6b42212e43be1b63b5c290eb5bfd85 [https://perma.cc/5GS8-GA9P].

97 Lauren Ban, *Texas AG Sues Google over Collection of Facial and Vocal Recognition Data*, JURIST (Oct. 20, 2022, 7:45 PM), https://www.jurist.org/news/2022/10/texas-ag-sues-google-over-collection-of-facial-and-vocal-recognition-data/ [https://perma.cc/JSB9-7WX8].

98 *See* TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017).

99 *See* WASH. REV. CODE ANN. § 19.375.020 (West 2017).

WBPA focuses on *enrollment* of biometric identifiers into a database for a commercial purpose, rather than *initial collection.*[100]

Other types of state laws that explicitly mention biometrics are data security breach notification and general data privacy laws that often include biometrics in the definition of "personal information." More states now have such comprehensive data privacy laws, including California, Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, New Jersey, Oregon, Tennessee, Texas, Utah, and Virginia, many of which were enacted in 2023.[101] However, the scope of consumer protection can vary widely depending on how biometrics are defined. For example, California's Privacy Rights Act ("CPRA") is notable for its expansive definition of "biometric information," which includes characteristics intended to be used singly or with other data to "establish individual identity," imagery from which an identifier template can be extracted (rather than the facial geometry itself), and keystroke and gait patterns, leading to a wider set of technologies that fall under its scope.[102] In contrast, Virginia's definition of "biometric data" explicitly excludes data generated from photo, video, or audio recordings, which is how facial geometry is measured.[103]

Finally, some state laws ban biometrics in certain situations (e.g., employment and law enforcement).[104] For example, California banned facial recognition technology on police body cameras, but the law expired at the end of 2022.[105] Notably, Virginia, Colorado, Montana, Massachusetts, and Maine restrict or ban facial recognition

---

100 *Id.*

101 *See, e.g.*, California Privacy Rights Act, CAL. CIV. CODE § 1798.140, et seq. (West 2024); Virginia Data Protection Act, VA. CODE ANN. § 59.1-575–59.1-585 (2023); Colorado Privacy Act, COLO. REV. STAT. ANN. § 6-1-1302 (West 2023).

102 CAL. CIV. CODE § 1798.140(c) (West 2024). "Sensitive Personal Information" is subject to additional restrictions and includes processing biometric information for the purpose of identifying a consumer. *Id.*

103 VA. CODE ANN. § 59.1-575 (2022).

104 *See* MD. CODE ANN. LAB. & EMPL. § 3-717 (prohibiting employers from using facial recognition without consent in certain hiring processes); N.Y. LAB. LAW § 201-a (banning requiring fingerprints as a condition of employment).

105 Rachel Metz, *First, They Banned Facial Recognition. Now They're Not So Sure*, CNN BUS. (Aug. 5, 2022, 8:20 AM), https://www.cnn.com/2022/08/05/tech/facial-recognition-bans-reversed/index.html [https://perma.cc/GX9Y-99LM]. Virginia had completely banned local police and campus law enforcement from using facial recognition technology, but in March 2022, amended the bill to allow its use in certain situations. *Id.*

surveillance and identification with limited exceptions.[106] If law enforcement in these states wants to use facial recognition systems in connection with a crime, the laws vary on whether the crime must be "serious," and whether there must be probable cause, a warrant, or a court order.[107] For example, Montana requires a warrant before performing the search except for certain emergencies, while Virginia only requires a "reasonable suspicion the individual has committed a crime."[108] Interestingly, Colorado explicitly prohibits using facial recognition technology based on protected characteristics, or at participation in lawful events and organizations, including when one exercises their First Amendment rights.[109]

Finally, in 2023, several states proposed biometric regulations like BIPA, while other proposals were more tailored to regulating certain uses, such as for advertising, retail activity, or law enforcement and surveillance. Interestingly, the New York State Senate proposed a bill prohibiting the use of a "biometric surveillance system" by law enforcement or in places of public accommodation and the New Jersey Senate similarly proposed a bill banning facial recognition technology in places of public accommodation.[110]

3. Cities

Several cities and municipalities have passed biometric regulations, either regulating private entities or law enforcement. New York City's biometric law regulates how the private sector, not the public sector, can collect, use, store, and retain biometric information.[111] The law permits a private right of action, but with an opportunity for the

---

106 *See* MONT. CODE ANN. § 44-15-104 (West 2023); ME. REV. STAT. ANN. tit. 25 § 6001 (West 2021); COLO. REV. STAT. ANN. § 24-18-307 (West 2022); VA. CODE ANN. § 15.2-1723.2 (West 2022).

107 Maine requires probable cause that an unidentified individual in an image committed a serious crime. ME. REV. STAT. ANN. tit. 25 § 6001 (West 2021). Montana requires a court order that the information be relevant to an ongoing criminal investigation. MONT. CODE ANN. § 44-15-106 (West 2023). Virginia's law sets out fourteen lawful purposes where facial recognition technology can be used, requires any facial recognition algorithm to receive a 98% accuracy rating from NIST, and it bans live real-time use of FRT. VA. CODE ANN. § 15.2-1723.2 (West 2022).

108 *See* VA. CODE ANN. § 15.2-1723.2 (West 2022); MONT. CODE ANN. § 44-15-105 (West 2023).

109 *See* COLO. REV. STAT. ANN. § 24-18-307 (West 2023).

110 *See* S.B. 1609, 2023 Reg. Sess. § 2 (N.Y. 2023); S.B. 7135, 2023 Reg. Sess. § 2 (N.Y. 2023); S.B. 968, 229th Leg. (N.J. 2024).

111 N.Y.C. ADMIN. CODE §§ 22.1201–1205.

business or entity to cure first.[112] Portland, Oregon went further and now prohibits the use of facial recognition technology by private entities in places of public accommodation.[113] Yet another approach targets law enforcement's use of facial recognition technology, generally in response to the harms of inaccuracy, discrimination, and misuse. In 2019, San Francisco was the first U.S. city to ban facial recognition technology by any local government agency.[114] Around twenty cities and municipalities have enacted similar bans.[115] However, in 2022, amid perceived rising crime rates, cities have increasingly reversed bans and increased access to facial recognition technologies.[116]

4. The U.S. Supreme Court's Position on Constitutionally Protected Privacy

The right to privacy is not explicitly enumerated in the U.S. Constitution, though one has been implied in the "penumbras" of other amendments' protections.[117] Topics that implicate privacy or the "right to be let alone" are generally matters of state law pursuant to the states' reserved power under the Tenth Amendment.[118] The most relevant constitutional provision protecting privacy is the Fourth Amendment, which states that "[t]he right of the people to be secure in their persons, house, papers, and effects, against unreasonable searches and seizures, shall not be violated."[119] Historically, the Fourth Amendment only protected against searches that constituted physical intrusions.[120]

---

112 *Id.*

113 PORTLAND, OR. CITY CODE, Ch. 34 §§ 10.010–34.10-050.

114 Johana Bhuiyan, *Surveillance Shift: San Francisco Pilots Program Allowing Police to Live Monitor Private Security Cameras*, THE GUARDIAN (Oct. 4, 2022, 6:00 AM), https://www.theguardian.com/us-news/2022/oct/04/san-francisco-police-video-surveillance [https://perma.cc/5PLR-R8BM]. San Francisco is now piloting a program that allows police to monitor live footage from consenting businesses and civilians' surveillance cameras without a warrant. *Id.*

115 BAN FACIAL RECOGNITION, https://www.banfacialrecognition.com/map [https://perma.cc/5SY5-9KG7] (last visited Feb. 9, 2024).

116 *See* Caroline Sinders, *Why New Orleans' Facial Recognition Ban Reversal Is Devastating News for All of Us*, MEDIUM (Aug. 9, 2022), https://medium.com/@carolinesinders/why-new-orleans-facial-recognition-ban-reversal-is-devastating-news-for-all-of-us-64065852fd81 [https://perma.cc/RM5D-PKC5]. In 2020, New Orleans banned law enforcement from using facial recognition technology, but the city council rolled it back in 2021, allowing police offers to request access for use for "crimes of violence." *Id.*

117 *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

118 *See* U.S. CONST. amend. X.

119 U.S. CONST. amend. IV.

120 Katz v. United States, 389 U.S. 347, 353 (1967).

An improper search violated the Fourth Amendment if it satisfied a trespassory test which was grounded in property and tort law, until the Supreme Court in *United States v. Katz* introduced the "reasonable expectation of privacy test" and held that the trespass doctrine was not controlling.[121] In *Katz*, the Court held that the government, in wiretapping a public phone booth and recording the conversation, violated the privacy that Katz justifiably relied on while using the phone booth, thus violating his Fourth Amendment rights, because "what he [sought] to preserve as private, even in an area accessible to the public, may be constitutionally protected."[122] Justice John Marshall Harlan's two-part test in his *Katz* concurrence asked: (1) whether the individual exhibited an actual (i.e., subjective) expectation of privacy, and (2) whether that expectation was one that society was prepared to recognize as "reasonable."[123] The Court in *Katz* recognized for the first time that modern surveillance did not require a physical intrusion to violate the Fourth Amendment.[124]

However, what society considers "a reasonable expectation of privacy" is limited by the "third-party doctrine," which says that individuals have no legitimate expectation of privacy in information voluntarily divulged.[125] For example, under the *Katz* test, the Supreme Court in *Smith v. Maryland* held that the police's installation and use of a pen register that allowed law enforcement to see the numbers dialed from plaintiff Smith's home (which led to his warrant and arrest), was not a violation of the Fourth Amendment because there was no expectation of privacy in phone numbers voluntarily dialed.[126]

In *United States v. Jones*, a police officer installed a GPS tracking device on Jones's vehicle.[127] Here, the Court rested its decision on the trespassory test, but clarified that either the *Katz* test or the trespassory test can be used to determine whether there was an unlawful search.[128] Justice Sonia Sotomayor in concurrence recognized an individual has

---

121 *Id.*

122 *Id.* at 351.

123 *Id.* at 361 (Harlan, J., concurring).

124 Margaret Hu, *Orwell's* 1984 *and a Fourth Amendment Cybersurveillance Nonintrusion Test*, 92 WASH. L. REV. 1819, 1840 (2017). However, the Supreme Court reserved the question of how its decision related to national security concerns. *Id.*

125 Smith v. Maryland, 442 U.S. 735, 744 (1979).

126 *Id.*

127 United States v. Jones, 565 U.S. 400, 402 (2012).

128 *Id.* at 404, 409; *see also* United States v. Karo, 468 U.S. 705, 713 (1984) (holding that an actual trespass was neither necessary nor sufficient in finding a Fourth Amendment violation).

an expectation of privacy in one's movements.[129] She posited that societal awareness that the government may be watching may chill associational and expressive freedoms and consequently alter the relationship between citizens and the government.[130] In fact, George Orwell's *1984* was referenced at least six times during the *Jones* oral argument.[131] Professor Margaret Hu argues that the Orwellian rhetoric allowed the Court to restrain government surveillance where Fourth Amendment precedent may otherwise have allowed it.[132]

The Supreme Court has yet to hear a Fourth Amendment case concerning RBI, but technological advances have increased surveillance capabilities for location tracking, which the Court addressed in *United States v. Carpenter*.[133] In *Carpenter*, police obtained several months' worth of Carpenter's detailed cellphone location data without a warrant.[134] The Court held that the government must obtain a warrant before accessing a person's sensitive cellphone location data and that traditional rules like the third-party doctrine do not automatically apply in the digital age.[135] The Court recognized that technological advances provide access "to a category of information otherwise unknowable" and called the tracking method "near perfect surveillance."[136] Importantly, *Carpenter* held that, despite the third-party doctrine, individuals do not lose Fourth Amendment protection merely because they store information on a third-party server.[137] This case was monumental because the Court affirmed that it had a role to ensure the viability of privacy protections in the digital age.[138]

Having examined biometrics regulation in the United States, this Note next examines China's biometrics uses and regulatory framework—a country with even more widespread biometrics usage.

---

129 *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).
130 *Id.*
131 Hu, *supra* note 124, at 1825-26.
132 *Id.* at 1825.
133 *See* Carpenter v. United States, 585 U.S. 296 (2018).
134 *Id.* at 302.
135 *Id.* at 313-14.
136 *Id.* at 311-12.
137 *Id.* at 315.
138 *Id.* at 320.

IV. CURRENT BIOMETRIC USE AND LEGAL APPROACH IN CHINA

A. Public Sector Use

In China, biometric technology use—and facial recognition in particular—is widespread, which "touches upon almost every aspect of an individual's life."[139] China is estimated to have half of the world's nearly one billion surveillance cameras.[140] Police place the cameras with facial recognition technology at strategic locations to maximize data collection and then run it through analytical software, aggregate the data, and store it.[141] Under project "Sharp Eyes," government bodies are implementing facial recognition systems that aim to provide complete surveillance in public spaces, even in common areas of residential buildings.[142] The police stated that their surveillance strategy under this program was to ultimately control and manage people, as well as to encourage citizens to surveil and report each other.[143] The Chinese government aims to maintain its authoritarian rule by creating a system to "maximize what the state can find out about a person's identity, activities and social connections."[144] This strategy seems to go hand in hand with China's credit scoring system, a system whose aim is build trust in society by assessing citizens' conduct , both in terms of "financial creditworthiness" and "social creditworthiness."[145]

In addition to facial geometry, the Chinese government collects other types of biometric data that expand its ability to collect more

---

139 Yan Luo & Rui Guo, *Facial Recognition in China: Current Status, Comparative Approach and the Road Ahead*, 25 U. PENN. J.L. & SOC. CHANGE 153, 155 (2021).

140 Isabelle Qian, Muyi Xiao, Paul Mozur & Alexander Cardia, *Four Takeaways from a Times Investigation into China's Expanding Surveillance State*, N.Y. TIMES, https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html [https://perma.cc/E2PB-STSU] (July 26, 2022).

141 *Id.*

142 Xiao Qiang, *The Road to Digital Unfreedom: President Xi's Surveillance State*, 30 J. DEMOCRACY 53, 57 (2019).

143 Qian et al., *supra* note 140.

144 *Id.*

145 *See* Zeyi Yang, *China Just Announced a New Social Credit Law. Here's What It Means*, MIT TECH. REV. (Nov. 22, 2022), https://www.technologyreview.com/2022/11/22/1063605/china-announced-a-new-social-credit-law-what-does-it-mean/ [https://perma.cc/A43E-2FMM]. The Chinese government thinks this will help build trust in society, though there has been little guidance from the central government. *Id.* Thus far local governments, as opposed to the central government, have been piloting such a system. *Id.*; *see also* Qiang, *supra* note 142, at 59-61.

details on its residents. In some locations, police attach sound recorders to facial recognition cameras to collect voice prints, which enable faster identification when analyzed with facial data.[146] Chinese police are also building iris-scan databases.[147] Most controversially, the Chinese government has been surveilling, imprisoning, and collecting DNA from certain ethnic minorities, political dissidents, and others deemed a danger to social stability through compulsion.[148] At Chinese police checkpoints established where Uyghurs, an ethnic minority, live, police require them to have their facial geometry and irises scanned and DNA collected.[149] Government bidding documents show that the Chinese government was seeking products to improve data consolidation on such populations, and a New York Times investigation found that the Chinese police were already able to create a "personal dossier" on each person from the collected data.[150]

In sum, vast amounts of biometric data are collected in public spaces, airports, train stations, and stores in China. Data have been used for many reasons, including tracking and pursuing suspected criminals, tracking Covid health risks, surveillance, and administrative identity verification.[151] Facial recognition is also prevalent in state-owned enterprises across many sectors.[152]

B. Private Sector Use

The Chinese private sector also engages in widespread collection and use of biometrics, especially facial recognition. For example, shoppers can use their facial geometry and phone number to pay at stores equipped with Alipay, an Alibaba product, and other Chinese e-

---

146 Qian et al., *supra* note 140. This is an example of multimodal biometric AI.

147 *Id.*

148 Qiang, *supra* note 142, at 58; Qian et al., *supra* note 140.

149 ALINA POLYAKOVA & CHRIS MESEROLE, EXPORTING DIGITAL AUTHORITARIANISM: THE RUSSIAN AND CHINESE MODELS 5 (2019), https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf [https://perma.cc/UK9D-2SVM].

150 Qian et al., *supra* note 140.

151 Luo & Guo, *supra* note 139, at 159-60. Some provinces photograph and identify jaywalkers and post the photo and home address of the person in public to force the individual to pay a fine or help a traffic officer. Paul Mozur, *Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras*, N.Y. TIMES (July 8, 2018), https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html [https://perma.cc/S3T5-J2D8].

152 *See* Luo & Guo, *supra* note 139, at 161 (saying that FRT is used in bank account verification and some public housing projects).

commerce platforms were even selling facial data.[153] Besides receiving financial assistance from and being used by government actors, Chinese biometric AI companies are also prominent exporters of such technology abroad.[154] China is currently the biggest exporter of face recognition technology.[155] However, Chinese society has become increasingly concerned with the lack of transparency around biometric collection, data leakage, and consent.[156]

C. Current Legal Approach

Widespread biometric collection and use took place for a long time with little limitations on the government and only sector-specific regulation for consumer privacy, if any.[157] However, in 2021, for the first time, Chinese lawmakers passed China's first comprehensive data privacy law, the Personal Information Protection Law ("PIPL"), that uses many data privacy principles found in EU law.[158] Some of the commonalities between the PIPL and the European Union's General Data Privacy Regulation ("GDPR") are principles of lawfulness, necessity, data minimization, transparency, accuracy, security, and limited data retention.[159] While not a biometric-specific law, the PIPL's definition of "sensitive personal information" includes biometric data collection and usage.[160] Article 26 contains a broad exception for

---

153 Agence France-Presse, *Smile-to-Pay: Chinese Shoppers Turn to Facial Payment Technology*, THE GUARDIAN (Sept. 4, 2019, 1:08 AM), https://www.theguardian.com/world/2019/sep/04/smile-to-pay-chinese-shoppers-turn-to-facial-payment-technology [https://perma.cc/ZF2N-BWSA]; *see* Mark Jia, *Authoritarian Policy*, 91 U. CHI. L. REV. 733, 771 (2024).

154 *See, e.g.*, Arthur Kaufman, *Interview: Josh Chin on China's Surveillance State*, CHINA DIGIT. TIMES (Sept. 23, 2022), https://chinadigitaltimes.net/2022/09/interview-josh-chin-on-chinas-surveillance-state/ [https://perma.cc/A6N9-A37R] (showing that the Chinese ambassador helped Huawei sell a $127 million "safe city" surveillance system in Uganda by arranging for local police to travel to Beijing).

155 Will Knight, *China Is the World's Biggest Face Recognition Dealer*, WIRED (Jan. 24, 2023, 7:00 AM), https://www.wired.com/story/china-is-the-worlds-biggest-face-recognition-dealer/. The United States is the second largest importer of such technology. *Id.*

156 Luo & Guo, *supra* note 139, at 155.

157 *Id.* at 156-58.

158 *See generally China's New National Privacy Law: The PIPL*, COOLEY (Nov. 30, 2021), https://www.cooley.com/news/insight/2021/2021-11-30-china-new-national-privacy-law [https://perma.cc/YQ8E-6VXY].

159 *Id.*

160 Zhongguo Renmin Gongheguo Geren Xinxi Baogu Fa (中华人民共和国个人信息保护法) [Personal Information Protection Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021,

image collection and facial recognition technology in public venues for the purpose of safeguarding public security.[161] In 2023, China's internet regulator, Cyberspace Administration of China ("CAC"), released draft provisions to regulate private sector use of facial recognition, proposing purpose, necessity, and consent principles, except where regulations otherwise permit collection.[162]

Under the PIPL and other data breach laws, the CAC imposed a $1.2 billion fine, the largest yet for data collection and breach violations, on Chinese ride-hailing app, Didi.[163] The CAC accused Didi of "malicious evasion of supervision" and deemed its infractions a national security risk.[164]

While the PIPL does technically apply to government bodies handling personal information, there are broad exemptions from its requirements such that it is unclear whether the PIPL applies in practice to government agencies or state-owned enterprises providing utilities or services using biometrics.[165] Overall, the Chinese government's biometric surveillance activities appear largely unrestrained.[166] Thus, some scholars argue that China has a dual approach to privacy, increasing data privacy protections for consumers and appearing to protect privacy rights, while maintaining government control over citizens' privacy.[167] Authorities encourage citizens to have awareness of and concern for privacy issues, provided such concern is focused on

---

effective Nov. 1, 2021) 2021 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. 1117, art. 28 (China).

161 *Id.* art. 26. The European GDPR also has exceptions, though the interpretation of safeguarding public security differs.

162 *See Provisions on Security Management in the Application of Facial Recognition Technology (Trial) (Draft for Comment)*, CHINA L. TRANSLATE (Aug. 8, 2023), www.chinalawtranslate.com/en/facial-recognition-draft/ [https://perma.cc/SJX3-UDS6].

163 Paul Mozur & John Liu, *China Fines Didi $1.2 Billion as Tech Sector Pressures Persist*, N.Y. TIMES (July 21, 2022), https://www.nytimes.com/2022/07/21/business/china-fines-didi.html [https://perma.cc/SPH7-CSZ7]. Didi was accused of illegally collecting an excessive amount of data and mishandling personal data. *Id.*

164 *Id.*

165 *See* Luo & Guo, *supra* note 139, at 156; PERSONAL INFORMATION PROTECTION LAW OF THE PEOPLE'S REPUBLIC OF CHINA, *supra* note 160, arts. 35, 45.

166 China's Counterterrorism Law authorizes public security bodies to collect and retain biometric data. *See* Zhongguo Renmin Gongheguo Fan Kongbu Zhuyi Fa (中华人民共和国反恐怖主义法) [Counterterrorism Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 27, 2015, effective Jan. 1, 2016), arts. 45, 50 (China).

167 *See, e.g.*, Luo & Guo, *supra* note 139, at 157.

companies' collection and usage of their data.[168] By enacting these protections, the Chinese Government can both appear responsive to its citizens' concerns against private actors and portray itself as a protector of privacy rights to increase its legitimacy while distracting from its own biometric surveillance and collection practices.[169] Worryingly, some Chinese government databases containing biometric data have had little security protection and have been breached.[170] Researchers say public awareness of privacy concerns has risen, but few people openly criticize the government's collection of their data.[171]

This Note next examines the European Union, which operates a stronger regulatory framework than either the United States or China.

V. CURRENT BIOMETRIC USE AND LEGAL APPROACH IN THE EUROPEAN UNION

In the European Union, facial recognition technology has been used by law enforcement, commercial venues (including sports stadiums, shopping centers, hotels, airports), and some employers, who use it to record working hours.[172] Behavioral biometrics are used by law enforcement in some member states and by border control authorities.[173] The European Union adopted a regulation in 2017 to establish "smart" borders, now called the "Entry-Exit System," which will begin registering and verifying third-party nationals with fingerprints and facial biometrics in October 2024.[174] These borders may also include emotion detection systems in the future.[175] One member state that is embracing biometrics is France. In 2023, French lawmakers passed a three-year pilot program that allows facial recognition

---

168 Kaufman, *supra* note 154.

169 *See* Jia, *supra* note 153, at 800, 804.

170 Amy Qin, John Liu & Amy Chang Chien, *China's Surveillance State Hits Rare Resistance from Its Own Subjects*, N.Y. TIMES, https://www.nytimes.com/2022/07/14/business/china-data-privacy.html [https://perma.cc/7GEX-CS34] (July 15, 2022).

171 *Id.*

172 *See* Matt Burgess, *Europe Makes the Case to Ban Biometric Surveillance*, WIRED (July 7, 2021, 1:00AM), https://www.wired.co.uk/article/europe-ai-biometrics [https://perma.cc/YA9B-VFQG]; IPOL Report, *supra* note 20, at 15.

173 IPOL Report, *supra* note 20, at 14.

174 *See id.* at 16-17; Angela Symons, *Post-Brexit Border Checks: Facial Scan EES System to Be in Place by Late 2024*, EURONEWS.TRAVEL (Dec. 19, 2023), https://www.euronews.com/travel/2023/10/20/eu-confirms-timeline-for-new-border-controls-everything-you-need-to-know-about-ees-and-eti [https://perma.cc/6MVA-5CQY].

175 *See* IPOL Report, *supra* note 20, at 16-17.

technology in public spaces to be accessed in real time for purposes of preventing terrorism, child abduction, and serious crimes.[176]

A. Foundational EU Law

The European Convention on Human Rights ("ECHR"), the Charter of Fundamental Rights of the European Union ("CFR"), and the Treaty on the Functioning of the European Union ("TFEU") set forth the relevant fundamental rights of EU citizens. In particular, ECHR Article 8 protects "respect for private and family life," including the right to privacy; Article 10 protects freedom of expression; and Article 11 protects freedom of assembly and association.[177] However, these rights are not absolute and may be impinged upon if the interference is (1) in accordance with the law, (2) in furtherance of the government's legitimate aim, (3) necessary in a democratic society, and (4) proportionate to the aim.[178] The CFR protects fundamental rights for European Union citizens, including the rights to privacy, human dignity, integrity, freedom, and equality.[179] Finally, both the CFR and the TFEU explicitly grant individuals the right to protection of their personal data.[180] Thus, where European Union law is applicable, the CFR must be followed, including the rights of respect for and protection of human dignity and private and family life, as well as protection of personal data.[181] Any abridgment of these protected rights must be "provided for by law, proportionate and [must] meet objectives of general interest or the need to protect the rights and freedom of others."[182] These are the foundational charters, but several other highly relevant privacy regulations are discussed next.

---

176 Masha Borak, *French Senate Votes in Favor of Public Facial Recognition Pilot*, BIOMETRIC UPDATE (June 14, 2023, 8:27 PM), https://www.biometricupdate.com/202306/french-senate-votes-in-favor-of-public-facial-recognition-pilot [https://perma.cc/ENU8-YARD].

177 Convention for the Protection of Human Rights and Fundamental Freedoms arts. 8, 10, 11, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter ECHR].

178 *See* IPOL Report, *supra* note 20, at 25-26.

179 *See* Charter of Fundamental Rights of the European Union arts. 1-26, 2000 O.J. (C 364) 1, 9-14 [hereinafter CFR].

180 *See* Consolidated Version of the Treaty on the Functioning of the European Union art. 16, 2012 O.J. (C 326) 47, 55 [hereinafter TFEU]; *see also* CFR, *supra* note 179, art. 8 (stipulating that personal data must be processed legitimately by consent or another lawful basis and be processed fairly for specified purposes).

181 *See* CFR, *supra* note, 179, arts. 1, 7, 8.

182 IPOL Report, *supra* note 20, at 25.

B. Public Sector Regulations

The European Union's Law Enforcement Directive ("LED") applies when law enforcement agencies process personal data for "prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties."[183] Article 10 of the LED limits law enforcement's ability to process biometric data for the purpose of identification and if infringed, the subjects of the data can request data erasure.[184] To process biometric data for identification, law enforcement's purpose must be strictly necessary; satisfy safeguards for the data subject's rights; and "either (i) be authorised by Union or Member State law, (ii) protect the vital interests of the data subject or of another natural person, or (iii) relate to data which has manifestly been made public by the data subject."[185] The European Union also regulates the collection, storage, and use of biometrics in certain situations. For example, EU Member States are required to include a facial image and two fingerprints on any passports and travel documents they issue, and they must be highly secured per Council Regulation (EC) No 2252/2004.[186] This regulation is intended to protect against fraudulent use of travel documents and the biometric identifiers are only used for identity verification.[187]

---

183 *Id.* at 27.

184 Directive 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, art. 10, 2016 O.J. (L 119) 89, 109 (EU) [hereinafter LED].

185 IPOL Report, *supra* note 20, at 27. The LED also provides for certain safeguards related to automated decision-making and data security. LED, *supra* note 184, arts. 10, 11.

186 Council Regulation (EC) No 2252/2004 of 13 December 2004 on Standards for Security Features and Biometrics in Passports and Travel Documents Issued by Member States, art. 1, 2004 O.J. (L 385) 1, 2.

187 The Entry-Exit System Regulation, part of the Smart Border Package, also allows for collection and use of biometric data. Regulation (EU) 2017/2226, of the European Parliament and of the Council of 30 November 2017 Establishing an Entry/Exit System (EES) to Register Entry and Exit Data and Refusal of Entry Data of Third-Country Nationals Crossing the External Borders of the Member States and Determining the Conditions for Access to the EES for Law Enforcement Purposes, and Amending the Convention Implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, art. 6, 2017 O.J. (L 327) 20, 33.

C. Private Sector Regulations

The European Union's one major data privacy regulation in effect is the General Data Privacy Regulation ("GDPR").[188] The GDPR harmonizes data privacy laws across the European Unions because as a regulation it is automatically binding on member states, thus setting the floor for data privacy. Importantly, the GDPR states that controlling one's personal data is a fundamental right, though not an absolute right.[189] The structure of the GDPR is based on the idea of "privacy by design and by default" which means "taking data protection risks into account throughout the process of designing a new process, product or service."[190] This can be done by implementing measures that comply with GDPR at the outset, such as automatically deleting biometric data after searching for a match.[191] "Data protection by default" requires implementing procedures to ensure that "only the minimum amount of personal data is collected and processed for a specific purpose; the extent of processing is limited to that necessary for each purpose; the data is stored no longer than necessary and access is restricted to that necessary for each purpose."[192]

Biometric data is "sensitive personal data" under the GDPR.[193] Additionally, biometric data is defined broadly to recognize that the data points collected and the method in which biometric data is collected could change as technology develops.[194] The Regulation requires that sensitive personal data is subject to impact assessments, consent, erasure, access requests and more.[195] Because of the risks that

---

188 Regulation (EU) 2016/679, of the European Parliament and of the Council, 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, 2016 O.J. (L 119) 1 [hereinafter GDPR].

189 GDPR, *supra* note 188, art. 1.

190 Michael Monajemi, *Privacy Regulation in the Age of Biometrics that Deal with a New World Order of Information*, 25 U. MIAMI INT'L & COMPAR. L. REV. 371, 388 (2017).

191 For example, "[p]seudonymisation is when the processing of personal data is done in such a way that it can no longer be tied to a specific data subject without more information." *Id.* at 389; *see also* GDPR, *supra* note 188, art. 4(5).

192 Monajemi, *supra* note 190, at 389.

193 *See* GDPR, *supra* note 188, art. 4(14) (defining biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data").

194 Monajemi, *supra* note 190, at 382-83.

195 *See id.* at 383-89.

biometric data processing poses to individuals' fundamental rights, Article 9(1) generally prohibits such processing for biometric identification purposes unless an exception is met.[196] Even if an individual is identified under Article 9(1), Article 22 gives individuals the right to not be subject to a decision "based solely on automated processing, including profiling, which produces legal effects concerning them," such as an arrest.[197]

GDPR violations incur steep fines. Clearview AI has been fined the maximum penalty, €20 million, for its unlawful processing of biometric data, failure to cooperate with the French data protection authority, and for violating individuals' rights under the GDPR's protection of transparency, the right to access, and the right to erasure.[198] While the EU authority can order Clearview to delete EU citizens' data, it cannot order the destruction of the underlying algorithms.[199] This is a significant limitation because Clearview can still reap the benefits of training its algorithms on unlawfully obtained data by selling the valuable algorithms themselves, not the database.

1. Artificial Intelligence Act

In April 2021, the European Commission proposed a regulatory framework for artificial intelligence called the Artificial Intelligence Act ("AI Act").[200] The AI Act emphasizes societal needs "so that people can trust that the technology is used in a way that is safe and compliant with the law, including the respect of fundamental rights."[201] The Act's objectives are to give businesses legal certainty to facilitate innovation, enhance enforcement of existing law applicable to AI systems, avoid market fragmentation, and "facilitate the development of a single market for lawful, safe and trustworthy AI applications."[202] The EU digital internal market strategy is a key driver of the proposal

---

196 GDPR, *supra* note 188, art. 9.

197 *Id.* art. 22.

198 Natasha Lomas, *France Fines Clearview AI Maximum Possible for GDPR Breaches*, TECHCRUNCH (Oct. 20, 2022, 2:04 PM), https://techcrunch.com/2022/10/20/clearview-ai-fined-in-france/ [https://perma.cc/YC9M-JNX8].

199 *See* GPDR, *supra* note 188, art 58.

200 *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts*, COM (2021) 206 final (Apr. 21, 2021) [hereinafter AI Act].

201 *Id.* at 1.

202 *Id.* at 3.

because leaders fear market fragmentation and the related legal uncertainty it can cause for providers and users of AI systems in EU member states.[203]

To effectuate their purpose, the EU policymakers chose a uniform regulation which would bind all member states and would follow a risk-based approach.[204] AI systems deemed to have an "unacceptable risk" would be banned, while those deemed "high-risk," "limited," or "minimal to no risk," would be subject to varying degrees of ex-ante and ex-post requirements.[205] Once AI systems enter the EU market, they would be subject to continuous monitoring, transparency obligations, and human oversight requirements.[206]

To become law, the three legislative bodies representing different interests, the European Commission, European Parliament, and European Council, had to agree on the final text of the AI Act. The European Parliament and Council came to a provisional agreement on the final AI Act's key points in December 2023, a draft passed the European Parliament in March 2024, and the final text is going through a final lawyer-linguist check.[207] This agreement came after rounds of fierce debate, as legislators attempted to strike a balance between fostering AI innovation and protecting fundamental human rights.[208]

Classifying biometric AI systems used for "real time" remote identification was one of the primary points of contention.[209] The

---

203 *Id.* at 6. The EU digital internal market strategy seeks to "ensure the proper functioning of the internal market by setting harmonised rules in particular on the development, placing on the Union market and the use of products and services making use of AI technologies or provided as stand-alone AI systems." *Id.*

204 *Id.* at 9-10.

205 *Id.* at 12-13.

206 MAURITZ KOP, EU ARTIFICIAL INTELLIGENCE ACT: THE EUROPEAN APPROACH TO AI 4-5 (2021), https://law.stanford.edu/wp-content/uploads/2021/09/2021-09-28-EU-Artificial-Intelligence-Act-The-European-Approach-to-AI.pdf [https://perma.cc/8JZD-MHNA].

207 *See* European Parliament Press Release 20231206IPR15699, Artificial Intelligence Act: Deal Comprehensive Rules for Trustworthy AI (Dec. 9, 2023); European Parliament Press Release 20240308IPR19015, Artificial Intelligence Act: MEPs Adopt Landmark Law (Mar. 13, 2024).

208 *See* Foo Yun Chee, Supantha Mukherjee & Martin Coulter, *Talks on EU's AI Act to Resume Friday After Marathon Debate*, REUTERS (Dec. 7, 2023), https://www.reuters.com/technology/eu-still-hammering-out-landmark-ai-rules-marathon-overnight-talks-2023-12-07/; European Parliament Press Release 20240308IPR19015, *supra* note 207.

209 Elizabeth M. Renieris, *Europe at a Crossroads over Planned Use of Biometrics*, CTR. FOR INT'L GOVERNANCE INNOVATION (Nov. 2, 2022), https://www.cigionline.org/articles/europe-at-a-crossroads-over-planned-use-of-biometrics/ [https://perma.cc/9WLN-GWFK].

European Commission, supported by the European Council, proposed prohibiting real-time or near real-time RBI (e.g., facial recognition) in public spaces, specifically for law enforcement purposes, with certain law enforcement and national security carveouts where the use "is strictly necessary to achieve a substantial public interest."[210] However, the European Parliament wanted to ban all real-time RBI systems, without carveouts for law enforcement, but allow some uses of systems where identification occurs after a significant delay or "post" RBI.[211] The European Data Protection Board argued that "[d]eploying remote biometric identification in publicly accessible spaces means the end of anonymity in those places," and called for a ban on using such technology in public spaces for "facial recognition, gait recognition, fingerprints, DNA, voice, keystrokes and other types of biometrics."[212] Advocates for more stringent protections argued against having exceptions and encouraged including "clear safeguards that will protect against mass surveillance and AI systems such as facial recognition that can harm privacy and entrench discrimination."[213] Some leaders fear that exceptions for law enforcement could lead to mass surveillance permitted under the guise of security.[214]

The final agreed-upon text does include exemptions for RBI in public spaces for law enforcement and national security, as the European Council wanted, but with stricter conditions than originally proposed.[215] RBI is subject to prior judicial authorization and limited to use for a defined lists of serious crimes.[216] Real-time RBI is only permitted for targeted searches of victims, prevention of a specific and present terrorist threat, or identifying a suspect of a serious crime.[217] The exact wording of these safeguards and exemptions is likely one of

---

210 AI Act, *supra* note 200, at 22-23. The Council also supported these qualifications in its common negotiating position. *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, No. 14954/22 of 25 Nov. 2022, at 21-22.

211 European Parliament Press Release 20230505IPR84904, AI Act: A Step Closer to the First Rules on Artificial Intelligence (May 11, 2023).

212 Burgess, *supra* note 172.

213 Ayang Macdonald, *US and EU AI Regulatory Proposals Under the Microscope*, BIOMETRIC UPDATE (Oct. 17, 2022, 2:40 PM), https://www.biometricupdate.com/202210/us-and-eu-ai-regulatory-proposals-under-the-microscope [https://perma.cc/W22Q-P8JS].

214 *Id.*

215 European Parliament Press Release 20231206IPR15699, *supra* note 207.

216 European Parliament Press Release 20230505IPR84904, *supra* note 211.

217 *Id.*

the primary issues needed to agree on a final text of the AI Act. The bodies also agreed that the prohibited systems that pose an "unacceptable risk" of grossly violating fundamental rights include those involving remote biometric categorization using sensitive characteristics, emotion recognition in the workplace and education, social scoring, individualized predictive policing, certain AI systems that manipulate behavior, and indiscriminate biometric data scraping to create facial recognition databases.[218] Companies that violate the regulation could be fined up to 7% of their annual global turnover (i.e., net sales) or €35 million.[219]

D. Case Law

The European Court of Human Rights ("ECtHR") has heard cases concerning biometric data collection and retention, mainly about fingerprints and DNA samples stored in databases. In July 2023, however, the ECtHR heard a case about a peaceful demonstrator who was arrested by Russian authorities after being identified through facial recognition technologies and held that Russia violated Article 10 (freedom of expression) and Article 8 (private life) of the ECHR because, in part, it found Russia's use of live facial recognition could not be regarded as necessary in a democratic society.[220] Earlier cases mostly concerned data retention. In *S. and Marper v. the United Kingdom*, the ECtHR concluded that indefinite DNA sample retention for convicted and accused persons interfered with the "right to private life" and violated Article 8 because data was held indefinitely, even for acquitted persons.[221] It also held that fingerprint retention requires duration, storage, usage, and destruction safeguards.[222] The ECtHR has also noted "the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for

---

218 European Parliament Press Release 20240308IPR19015, *supra* note 207. These agreements reflect a broader usage than the European Parliament's version. European Parliament Press Release 20231206IPR15699, *supra* note 207.

219 European Parliament Press Release 20231206IPR15699, *supra* note 207.

220 *See* Glukhin v. Russ., App. No. 11519/20, ¶¶ 86-90 (Oct. 4, 2023), https://hudoc.echr.coe.int/eng?i=001-225655 [https://perma.cc/QVK2-MGBG] (concluding that "use of highly intrusive facial recognition technology in the context of the applicant exercising his Convention right to freedom of expression is incompatible with the ideals and values of a democratic society governed by the rule of law").

221 S. & Marper v. U.K., App. Nos. 30562/04 and 30566/04, ¶¶ 113-26 (Dec. 4, 2008), https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-90051%22]} [https://perma.cc/H4AY-BKSU].

222 *Id.* ¶ 125.

private and family life"[223] and safeguards are particularly needed when the data is subject to automatic processing and used by police.[224] According to the ECtHR, storing fingerprints and DNA profiles indefinitely without the data subject being able to request its deletion is an unwarranted interference with the respect for private life and "cannot be regarded as necessary in a democratic society."[225] The importance of protecting personal data in the European Union and its relation to the fundamental right of respect for private life is not found in the United States.

VI. CONGRESS SHOULD REGULATE BIOMETRIC DATA THROUGH FEDERAL LEGISLATION

A. Comparative Analysis

Biometric technologies have become increasingly sophisticated and widespread. They are being used across the world by governmental and private actors. Even seemingly mundane uses in the name of efficiency can be used for harmful ends. On one end of the spectrum is China's dual-system approach, which imposes few, if any, limits on the government and new regulations on private entities (though data may be turned over to the government).[226] As one protestor described the privacy landscape: "There is no privacy in China."[227] Biometric data collection has become so pervasive both within the Chinese government and private sector, that, despite some concerns, many harmful data collection practices have become expected or accepted as a tradeoff for security and convenience.[228] Though China enacted the PIPL in 2021, its AI-powered biometric technology is already advanced, its government is bent on using all of its surveillance capabilities, and its society has already had to adapt to the existing

---

223 M.K. v. France, App. No. 19522/09, ¶ 35 (July 18, 2013), https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-119075%22]} [https://perma.cc/58M5-RLSE].

224 *Id.*

225 *Id.* ¶ 46.

226 *See supra* Part IV.

227 Qin et al., *supra* note 170. A study of over 20,000 Chinese people found that over 60% of participants felt that facial recognition technology has been abused. *Id.*

228 *Id.* Due to the Chinese government framing itself as protecting privacy through the PIPL, citizens "may see state surveillance, even in its harshest forms, as another manifestation of the party-state's protective policies." Jia, *supra* note 153, at 800.

surveillance system and burgeoning social credit score program.[229] The massive biometric surveillance system in China and widespread commercial use of biometrics exemplify technology's ability to skyrocket when it far outpaces the privacy laws, practices, and values that seek to curb their potential misuse.

On the other end of the spectrum is the European Union, which has a different conception of data privacy, in part because of its legal framework that explicitly frames protecting personal data as a fundamental right in addition to protecting private and family life, human dignity, and freedom of expression.[230] The European Union currently regulates private sector uses of biometrics as "sensitive data" under the GDPR and will further regulate biometrics under the forthcoming AI Act. The GDPR's conception that personal data is part of you and that you own it is distinctively European.[231] Importantly, in the European Union, biometric identification (e.g., who is this person?) is viewed as uniquely harmful to fundamental rights of its citizens as compared to authentication (e.g. is this person who they say they are?).[232] The AI Act debate over which biometric systems would be considered an "unacceptable risk," including whether and how to draft any exceptions for real-time RBI, shows the tension between, on one hand, perceived beneficial uses for law enforcement and public safety-type interests and, on the other hand, the interference with privacy and fundamental rights. Any regulation in the United States must also grapple with this tension.

In the United States, as in the European Union, there is a tension between protecting individual rights and harnessing technological innovation. The perceived threat to fundamental rights has led some states to regulate or even ban certain uses of biometrics, such as facial recognition in policing.[233] However, a complete ban in the current technological landscape is unrealistic. After all, the United States' technology sector and government are heavily invested in biometric-related AI.[234] The United States' patchwork approach of sector or state-specific data privacy laws falls short of protecting the rights of vast swaths of the population. If the United States wants to avoid both

229 *See supra* Part IV, Section C.

230 *See supra* Part V, Section A.

231 *See supra* Part V, Section C.

232 *See id.*

233 *See supra* Part III, Section B.1.

234 *See* Knight, *supra* note 155; *see also supra* Part III, Section A.1.

China's dual-system approach and its impact on society, it must meaningfully regulate the private *and* the public sector.

B. Limitations of the United States' Current Approach

Rather than local bans on certain biometric uses, Congress should pass a regulation harmonizing biometric data practices across the states and focus on limiting harms from RBI, which poses a unique threat to democracy due to its potential to chill speech and expression in public spaces if people feel they are being remotely identified. The United States' patchwork approach to privacy is insufficient to protect Americans' biometric data from the harms associated with both private and public sector use discussed in Part I. The current U.S. regulatory landscape consists of sector-specific federal data privacy laws that do not thoroughly address biometrics, if at all, and state and local laws.[235] As a result of uneven federal regulation, state and federal practices sometimes conflict, causing both potential uncertainty among individuals over their expectation of privacy and risks to their privacy from breaches.[236] For example, ICE officials, without approval from Maryland state officials or a court, ran facial-recognition searches on millions of Maryland drivers' license photos.[237]

Only three states have passed comprehensive biometric privacy laws that regulate companies. At least thirteen states have passed general data privacy laws.[238] Illinois's BIPA has admirable qualities—e.g., its notice-and-consent regime, private right of action, and provision (as interpreted by the courts) that a BIPA violation is sufficient to qualify as an injury.[239] BIPA, however, is limited to private actors and its scope protects Illinois residents. While this forces companies doing business in Illinois to consider BIPA, they may decide it is necessary to only establish protections for Illinois residents, as Everalbum did for states with biometrics laws.[240] It is much more common for states to pass data breach notification laws that require disclosure if electronically stored personal information is disclosed.[241] However, these laws generally do not protect against the initial biometric collection or provide parameters for lawful use of such data like BIPA. Similarly, the

---

235 *See supra* Part III, Section B.

236 GAO-22-106100, *supra* note 47, at 13-14.

237 Turley, *supra* note 26 at 2256.

238 *See supra* note 101 and accompanying text.

239 *See supra* Part III, Section B.2.

240 *See supra* Part III, Section B.1.

241 *See supra* Part III, Section B.2.

FTC's powers are useful to protect consumers, but are currently limited, as discussed in Part III. The FTCA may motivate companies to not misrepresent how they collect and use biometric data, or how accurate their technology is, but it does not restrict their practices so long as they are not "unfair or deceptive."[242] Also, any sweeping rule the FTC may consider promulgating on commercial data surveillance is likely to be challenged as exceeding its regulatory authority. Finally, the Biden Administration's executive order is an important step forward for transparency and oversight in the development of AI, but it rightly urges Congress to take action.

Thus, the private sector largely operates in a "notice-and-choice" framework, relying on consumers to understand the risks of biometric data collection and decide for themselves whether to use a product or service. The potential for abuse with facial recognition and other biometric identification technologies in this system is high.[243] Some companies have exercised restraint in deploying advanced biometric technologies, though Clearview AI has crossed that line. How long will it be before we see effects typically associated with an Orwellian dystopic state? The sports and entertainment company Madison Square Garden, for example, used facial recognition to identify attorneys litigating against it and expelled them from its venues under the guise of security.[244]

Congress, not states, should set the floor for biometric regulation. States-rights proponents would argue that leaving biometric regulation to the states allows them the freedom to experiment and balance interests. Those in favor of federal regulation may argue that one uniform federal law is necessary to set expectations for all affected parties, which would preempt contrary state laws.[245] Alternatively, a federal law could set the floor for regulation, but allow states to enact stricter measures. This is the European Union's approach and the approach this Note supports.[246]

Setting a floor for all states is important for both private and public sector use of biometrics as well as protecting against the worst

---

242 *See generally* FTC POLICY STATEMENT, supra note 81, at 5-12.

243 *See supra* Part II, Section C.

244 Kashmir Hill & Corey Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies*, N.Y. TIMES, https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html [https://perma.cc/5UCM-ACYY] (Jan. 3, 2023).

245 Turley, *supra* note 26, at 2257.

246 The benefit of the European Union's LED, GDPR, and AI Act is that they set the floor for all member states. *See supra* Part V.

harms that flow from remote biometric identification, categorization, and detection at scale. A government assessment that analyzed biometric AI systems' possible harms concluded that systems capable of RBI particularly threaten individual rights, especially when combined with mass surveillance, or when used as a basis for further targeting or automated decisions about a person.[247] As AI develops with more data, "the greatest danger of [facial recognition technology] is not its inaccuracy, but its accuracy" which "threatens to expose all citizens to continual monitoring of moves and associations in public."[248]

Biometric surveillance has potential for abuse and can chill speech and association.[249] This chilling effect can be clearly seen in China, where the accuracy of its biometric identification surveillance apparatus has enabled it to identify and track its citizens, including protestors, journalists, and dissidents, thus raising the risks for public activity.[250] As discussed in Part II, in the context of the Hawthorne Effect, if people expect that they are being monitored and evaluated they may alter their behavior, thus restricting their freedom of speech and expression, ultimately weakening democratic foundations and giving greater control to the government and other actors.

Unfortunately, public sector use of facial recognition and other remotely capturable biometrics fall within a "blind spot" of existing privacy protections.[251] Some jurisdictions ban law enforcement from using facial recognition technology for biometric identification while others actively use technology like Clearview AI.[252] For constitutional protections, as discussed, Fourth Amendment jurisprudence heavily relies on either a trespassory test or the *Katz* test (reasonable expectation of privacy).[253] Biometrics that are remotely captured, like most used for biometric identification, evade the trespass test. Therefore, any Fourth Amendment protection must stem from the *Katz* test, where the question would be whether an individual has a reasonable expectation that they will not be remotely identified in public by

---

247 IPOL Report, *supra* note 20, at 46-50.

248 Turley, *supra* note 26, at 2212.

249 In China, protestors marching against the government's strict "Zero Covid" policy were often identified and tracked by police to get the protestors to pledge not to do so again. Paul Mozur, Claire Fu & Amy Chiang Chien, *How China's Police Used Phones and Faces to Track Protestors*, N.Y. TIMES, https://www.nytimes.com/2022/12/02/business/china-protests-surveillance.html [https://perma.cc/72B4-A69K] (Dec. 4, 2022).

250 *See supra* Part IV.

251 Turley, *supra* note 26, at 2213.

252 *See supra* notes 101-106 and accompanying text.

253 *See supra* Part III, Section B.4.

biometric technologies capable of knowing who they are, what they do, or with whom they are friends. On the one hand, people's expectation of privacy is likely decreasing, even in crowded public spaces. Rather than living in anonymity, as the privacy scholar Jonathan Turley says, we live in an increasingly "nonymous world where people are known by face and name on the Internet and social media."[254] This could give government actors more leeway to use RBI without infringing Fourth Amendment protections, which could in turn lower expectations of privacy further.[255] However, five Supreme Court justices in *Jones* recognized a reasonable expectation of privacy in one's physical movements and the majority in *Carpenter* cautioned that cell-site location information gave police retrospective "access to a category of information otherwise unknowable."[256] Just as cell-site location was considered "detailed, encyclopedic, and effortlessly compiled" in *Carpenter*,[257] RBI when combined with other data on an individual can create the same privacy-invading encyclopedic knowledge of a person's movements and behaviors. Courts should therefore consider a government actor's unrestrained use of these technologies as invading an individual's reasonable expectation of privacy.

C. Suggestions

1. Public Sector

Congress should regulate the public sector use of biometric AI rather than impose a total ban on certain technologies like facial recognition. Advocates for a total ban on facial recognition argue that the "harm to benefit ratio" is so imbalanced that a categorical ban is needed, claiming that "[t]he mere existence of facial recognition systems . . . harms civil liberties[] because people will act differently."[258] While biometric harms can interfere with individual rights, perpetuate discrimination, and erode anonymity, it is unrealistic to ban technology that can also further compelling legitimate governmental interests like national security. Similarly, businesses and consumers have

254 Turley, *supra* note 26, at 2241. Jonathan Turley describes a "nonymous" society as one where "where our movements and associations will be made increasingly transparent." *Id.* at 2179.

255 *Id.* at 2214.

256 Carpenter v. United States, 585 U.S. 296, 312 (2018).

257 *Id.* at 309.

258 Hartzog, *supra* note 22.

adopted biometrics uses, particularly for authentication, and are unlikely to stop.

To avoid the worst harms to society—the harms to civil rights and democracy—those that which stem from remote biometric identification, categorization, and detection, the government should strive to foster obscurity.[259] Focusing on obscurity rather than unrealistic anonymity can protect against the chilling effect on democratic activities.[260]

The United States should use the "privacy by design" principle found in the GDPR and PIPL.[261] The design should be based on codifying obscurity by limiting access and use of facial recognition and other technology capable of RBI,[262] building in safeguards for real-time and post RBI like those contemplated in the European Union's AI Act.[263] This way, even if individuals can technically be identified, their identity and movement would be obscured in many instances. This principle can be implemented through the courts and by statute. The Supreme Court should extend the Fourth Amendment's warrant requirements to searches using biometric identification, but Congress should also enact statutes holding biometric identification to those standards as some states do. The technology is undoubtedly useful to law enforcement, but Congress should require probable cause to access facial recognition livestreams (on public systems or private-owned systems such as video doorbells) or recorded data. Changes to the law or its interpretation will help to reinforce privacy expectations that people are not always being identified and tracked, while still allowing law enforcement to access facial recognition and similar technologies when warranted. Federal legislation should also limit access to databases and safeguard data transfers, as is common in the European Union. Using the European Union's framework of "privacy by design," these controls should be part of the design of any government-controlled biometric technology. Additionally, biometrics should be defined broadly, as in the GDPR, or the CPRA, to account for developing technologies and capabilities.

---

259 *See supra* Part II (discussing obscurity).

260 *See, e.g.*, Turley, *supra* note 26, at 2257.

261 *See supra* Part IV and Part V, Section C.

262 *See* Turley, *supra* note 26, at 2254-59.

263 *See supra* Part V.C.

2. Private sector

It is not enough to address only the government's use of biometric technology. It would be meaningless if there were only regulations on a public square, but not on every business that could install facial recognition technology. Jonathan Turley argues that it is important to reinforce privacy expectations uniformly.[264] For the private sector, such a regulation should be based on many of the GDPR's foundation principles, including notice, consent, proportionality, data minimization, and transparency. Without having regulation in the private and public sector, society may trend toward China's dual system, one set of rules for the private sector and one for the public sector, where data from the private sector may be turned over to the public sector.[265] Congress should also expand the United States' conception of privacy, as the European Union did in the TFEU. Finally, to address accuracy harms associated with both biometric identification and authentication, Congress should empower the National Institute of Standards and Technology, which is involved in evaluating algorithms, to require any company that sells biometric technologies to use a certain industry standard algorithm to reduce problems of bias.

VII. CONCLUSION

This century, tension between harnessing technology and protecting individual rights will continually recur. Americans should have the same minimum expectation of privacy whether they live in Illinois or New York, or whether they are walking down the street or in a store. Individuals should be able to attend a protest, event, or other lawful activity, without fear of being remotely identified and having that data aggregated with other personal data—a fear so strong that they may decide to stay home instead. They should feel comfortable that a level of obscurity will be built into technology used by companies or governments and that government officials will need probable cause before they can access this wealth of information. Congress should pass legislation built around protecting obscurity to avoid the possible chill on civil rights and the other myriad harms of biometric authentication, identification, characterization, and detection.

---

264 Turley, *supra* note 26, at 2257-58.

265 *See supra* Part IV, Sections C, D.