# Regulating Facial Recognition Technology in the Private Sector

Elizabeth A. Rowe*

24 STAN. TECH. L. REV. 1 (2020)

ABSTRACT

*As Congress considers possible federal regulation of facial recognition technology in the US, it is important to understand the way in which this technology is utilized, especially in the private sector, as well as the benefits to and concerns of the various stakeholders. The absence of federal regulation in this space has created much uncertainty for companies and consumers alike. Accordingly, as we stand at the crossroads of this highly significant decision, to regulate or not to regulate, this Article endeavors to identify common interests and common areas of concern among the various stakeholders, including developers of the technologies, business users, and consumers (broadly conceptualized as private*

* Irving Cypen Professor of Law, Distinguished Teaching Scholar, and Director, Program in Intellectual Property Law, University of Florida Levin College of Law. I express my appreciation to Victoria Cundiff, Tait Graves, Camilla Hrdy, Sonia Katyal, David Levine, Andrea Matwyshyn, Sharon Sandeen, and Deepa Varadarajan for insights, comments, or conversations about the ideas expressed in earlier versions of this work. Thank you to Nyja Brown and Laura Kanouse for excellent research assistance.

*individuals, business to business, and government users). With those in mind, it poses certain guided questions to outline the contours of any regulation. Finally, it recommends three concrete and tailored steps toward crafting regulation of facial recognition technology. These include applying a differentiated approach to regulating in this area, providing precise and practical guidance for companies to navigate storage, use, collection, and sharing of biometric data, and considering trade secrecy as one potential reference point from which to address the standards necessary to tackling each of the key areas of concern.*

TABLE OF CONTENTS

## I. INTRODUCTION

The regulation of biometric data is a problem as complex as it is controversial. As with all new technologies that are met with apprehension, they are not all bad or all good. However, the camps for and against regulation start to form quickly. It is therefore important to better understand the nuances of the issues and the various stakeholders' interests and concerns. While the larger question involves biometric data generally, one subset of that group, facial recognition technology, provides the basis for this Article because of its current prevalence and use, as well as the controversy surrounding its various applications.

While much has been written about the use of facial recognition generally or in the criminal justice context,[1] this Article is the first to focus on regulation in the civil and commercial sector. That focus, however, in order to be comprehensive, cannot ignore uses by the government, primarily because the private sector generally develops and provides the technology to government agencies. Thus, for the purposes of this Article, the government potentially falls into the "consumer" category of relevant stakeholders, much like private individuals do. This symbiotic relationship raises interconnected concerns and considerations, and any regulations imposed on the private sector will necessarily implicate the government and its uses of facial recognition technology. The story of one company's groundbreaking facial recognition technology app serves as

1. *See, e.g.*, Katelyn Ringrose & Divya Ramjee, *Watch Where You Walk: Law Enforcement Surveillance and Protester Privacy*, 11 CAL. L. REV. ONLINE 349 (2020); Elizabeth McClellan, Note, *Facial Recognition Technology: Balancing the Benefits and Concerns*, 15 J. BUS. & TECH. L. 363 (2020); Katelyn Ringrose, Essay, *Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns*, 105 VA. L. REV. ONLINE 57 (2019); Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591 (2017); Joseph Clarke Celentino, Note, *Face-to-Face With Facial Recognition Technology Evidence: Admissibility Under the Post-*Crawford *Confrontation Clause*, 114 MICH. L. REV. 1317 (2016).

an illustrative introduction to the significant void which motivates this Article: the absence of federal regulation for biometric data in the US.

Clearview AI is a small company with a large footprint in the facial recognition technology space. The company "scraped" more than three billion images from Facebook, YouTube, Venmo and other websites to create a facial recognition database that is being used by a range of law enforcement offices from local police departments in college towns to the FBI.[2] While Clearview offers its service as a crime-solving tool, it has the capability and potential to be used for much more. Its algorithm is especially powerful because it runs against a massive database that contains almost any image posted online, thus accessing a much wider and more expansive dataset than traditional government databases (or those of its larger Silicon Valley competitors).[3] In practice, this allows the police to identify suspects who do not have a government-issued ID or who have never been arrested. Another advantage of Clearview's algorithm is that it does not require photos of people looking directly at the camera and can identify who they are even when they may be in the background.[4]

Privacy advocates have raised concerns about the accuracy of Clearview's algorithm, because it apparently has not been tested by an independent organization such as the National Institute of Standards and Technology ("NIST"), a federal agency that, among other things, rates the performance of facial recognition algorithms.[5] Thus, some critics have

---

2. *See* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://perma.cc/F2PG-JE7H.

3. *See id.*

4. *Id.* Note that the accuracy of facial recognition technology decreases when there is no standardized photo for comparison or when the comparison comes from a photo from an uncontrolled environment.

5. *See About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II: Hearing Before the H. Comm. On Homeland Sec.*, 116th Cong. (2020) (statement of Charles H. Romine, Dir., Nat'l Inst. Standards and Tech.) (noting that NIST collaborates with federal agencies, law enforcement, industry, and academics to "respond to government

called for a complete ban of the technology.[6] Nevertheless, the program appears to have become very successful and popular in the marketplace, both to government and corporate clients. According to the software's creator, more than 600 law enforcement agencies have started using Clearview's technology in the past year.[7] Clearview has also licensed the app to many private companies for security purposes.[8] Reports from a data breach investigation also indicate that Clearview provided access to its algorithm to other major corporate clients including Macy's,[9] Kohl's, Walmart, and the NBA.[10]

One point of contention is that Clearview keeps all the images it has scraped, even if they are later deleted or taken down. For that reason, Facebook, Google, Twitter, YouTube, LinkedIn, and Venmo have accused it of violating their terms of service and they have each sent cease and desist letters to the company.[11] Clearview contends that it has a right to scrape and keep this information, which it suggests is in the public

---

and market requirements for biometric standards."); *see also* PATRICK GROTHER ET AL., NAT'L INST. STANDARDS AND TECH., ONGOING FACE RECOGNITION VENDOR TEST (PART 1: VERIFICATION) 42-47 (2020), https://perma.cc/BA8J-HE7Z (detailing the ongoing efforts of the NIST to verify the accuracy of voluntarily submitted algorithms, with metrics, datasets).

6. *See* Henry Kenyon, *Privacy Groups Urge White House to Ban Use of Facial Recognition Tech*, CQ ROLL CALL (Jan. 28, 2020), https://perma.cc/C9ZT-FJ55.

7. *See* Donie O'Sullivan, *This Man Says He's Stockpiling Billions of Our Photos*, CNN (Feb. 10, 2020), https://perma.cc/9JHM-BQHX.

8. *See Clearview Is Not a Consumer Application*, CLEARVIEW AI (Jan. 23, 2020), https://perma.cc/XWF4-JVWH.

9. *See* Madeline Mitchel, *Macy's Faces Class Action Lawsuit for Use of Facial Recognition Software Clearview AI*, CINCINNATI ENQUIRER (Aug. 7, 2020), https://perma.cc/6ZLP-MUEA.

10. *See* Ben Gilbert, *Clearview AI Scraped Billions of Photos from Social Media to Build a Facial Recognition App That Can ID Anyone — Here's Everything You Need to Know About the Mysterious Company*, BUS. INSIDER (Mar. 6, 2020), https://perma.cc/5ZF9-SMA4; *see also* Ryan Mac et al., *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA*, BUZZFEED NEWS (Feb. 27, 2020), https://perma.cc/2D6D-YXYY.

11. *See* Gilbert, *supra* note 10.

domain, but it is reportedly working on a tool that would let people request that images be removed if they had been taken down from the website of origin.[12]

Clearview's practices have been challenged in the few states that have enacted biometric protections, including California, Vermont, and Illinois.[13] For instance, the ACLU filed a class action in Illinois.[14] According to one source, the concern is that

> by building a mass database of billions of faceprints without knowledge or consent, Clearview has created the nightmare scenario that we've long feared and has crossed the ethical bounds that many companies have refused to even attempt. Neither the United States government nor any American company is known to have ever compiled such a massive trove of biometrics.[15]

As a result of the Illinois litigation, filed pursuant to the state's Biometric Information Protection Act ("BIPA"), Clearview has promised to no longer collect data from Illinois-based IP addresses.[16]

Outside of the US, Clearview is also receiving scrutiny. Regulators in the UK and Australia are investigating privacy issues related to its data

---

12. *See* Hill, *supra* note 2.

13. *See* Leah Hodgson, *Controversial Facial Recognition Startup Clearview AI Faces International Probe*, PITCHBOOK (July 9, 2020), https://perma.cc/ZGX8-8BEA. *See e.g.*, Complaint, Burke v. Clearview AI, Inc., No. 3:20-cv-00370-BAS-MSB (S.D. Cal. Feb 27, 2020), https://perma.cc/598B-W4N3 (this class action was filed in California, but has since been transferred to New York); Complaint, Mutnick v. Clearview AI, Inc., No. 20 C 512 (N.D. Ill. May 28, 2020); Ryan Kriger, *Attorney General Wins Significant Victory in Clearview AI Lawsuit*, VT. O.A.G. (Sept. 11, 2020), https://perma.cc/6CUK-GZXS (discussing Vermont's ability to move forward with its lawsuit against Clearview).

14 Complaint, ACLU v. Clearview AI, No. 2020CH04353, (Ill. Cir. Ct. Sept. 25, 2020), https://perma.cc/DF3Q-KD3K.

15. *See* Nick Statt, *ACLU Sues Facial Recognition Firm Clearview AI, Calling It a 'Nightmare Scenario' for Privacy*, VERGE (May 28, 2020), https://perma.cc/2DPL-9PZZ.

16. *Id.*

scraping practices.[17] The Royal Canadian Mounted Police recently discontinued their contract with the company.[18] Furthermore, the European Data Protection Board has suggested that Clearview's technology may violate EU regulations.[19]

Clearview's story introduces the kinds of consequences (both intended and unintended) that can arise from the absence of federal oversight and the limitations of a piecemeal approach, if the status quo of only state-by-state regulation continues. This void has created uncertainty for companies, especially because there are wide-ranging business applications for this technology, the expansion of which may be impeded as a result of the legal uncertainty. For instance, the use of facial recognition technology alone for making payments, without a mobile device, is already being used in China,[20] but has not yet taken hold in the US.[21]

This Article is timely because there has been strong congressional interest in this area. However, there are divergent views on the content of any regulation. On March 14, 2019, the US Senate introduced the Commercial Facial Recognition Privacy Act, which would, among other things, require companies to first obtain explicit user consent before collecting any facial recognition data.[22] Interestingly, even some companies that are themselves developers of facial recognition software are encouraging regulation. Most notable among these is Amazon, which has proposed and drafted a bill that it has lobbied Congress to adopt.[23] Other

17. *See* Hodgson, *supra* note 13.

18. *See id.*

19. *Id.*

20. *See infra* Part II.B.

21. *See* Quentin Fottrell, *Silicon Valley's Final Frontier for Payments: 'The Neoliberal Takeover of the Human Body'*, MARKETWATCH (Oct. 23, 2019), https://perma.cc/446E-8SP7.

22. *See* Mark S. Nelson, *Amazon Must Allow Proposals on Facial Recognition Technology and Hate Speech*, WALTERS KLUWER: SEC. REG. DAILY, (Apr. 5, 2019), https://perma.cc/WN7M-23QQ.

23. *See* Kori Hale, *Amazon Pitches Shady Facial Recognition Laws*, FORBES (Oct. 1, 2019), https://perma.cc/S33R-MS4K.

organizations, including the ACLU, oppose the very use of facial recognition technology because of what they believe to be inherent biases.[24]

Accordingly, as we stand at the crossroads of this highly significant decision, to regulate or not to regulate, this Article aims to offer an objective, analytical approach by which to evaluate the critical issues and concerns that may lead to the most efficacious regulatory regime. The Article's main contribution lies not only in its novel analytical approach to the regulation of new technology generally, but in the resulting carefully tailored framework that it proposes for regulating facial recognition technology in the private sector.

Part I begins by providing background information about the use of facial recognition technology in the US by businesses, consumers, and the government. China is also discussed as a point of comparison, since it illustrates a business and regulatory regime that combines widespread adoption of facial recognition technology in everyday life, effectively without regulation.[25] Consideration of the Chinese approach is also relevant to the extent that their programs are exported to and sold in the US market. Part II categorizes and analyzes the concerns that have been raised in the US regarding facial recognition technology, including those related to privacy, accuracy, race and gender biases, religious objections, storage and data privacy, and misuse of the data.[26] The existing regulatory landscape is discussed in Part III, noting the states that have responded to the federal void with their own regulations, and corporate involvement in the debate over national regulation.[27]

Finally, Part IV introduces an analytical framework by which to consider federal regulation in this space, one based on a compromise approach. It suggests a new paradigm for regulating facial recognition technology, offers guidance to legislators and stakeholders based on tailored

---

24. *See ACLU Comment on Bill Stopping Face Recognition Surveillance,* ACLU (June 25, 2020), https://perma.cc/WS7E-372R..

25. *See infra* Part II.B.

26. *See infra* Part III.

27. *See infra* Part IV.

considerations, and recommends three concrete steps toward crafting regulation on this highly consequential and controversial topic.[28] In particular, it recommends a differentiated approach similar to that of the EU. Second, it calls for providing precise and practical rules to companies regarding storage, use, collection, and sharing ("SUCS") of the biometric data. Finally, it suggests the possible consideration of a trade secret framework as one path for organizing and addressing some of the standards that may be needed to address the SUCS problem.

## II. BACKGROUND OF USE

This Part will provide background on the current use of facial recognition technology in order to provide context and a backdrop against which to identify the stakeholders. First, this section sets the stage with examples of how the technology has been implemented in the US. Next, it presents a comparative view to China.

### *A. In the United States*

The use of facial recognition technology in the US has been slowly emerging and creeping into business applications and consumer preferences. While the commercial sphere is the focus of this Article, government uses of the technology are also noted. Indeed, government agencies are "consumers" of the technology in much the same way, yet on a larger scale, as the individual consumers in the marketplace.

#### *1. Business & Consumer Uses*

Facial recognition technology is being used by businesses for a wide range of purposes from internal operations, such as keeping track of employees' time and attendance, to consumer products and services. For instance, in one case, Uber deactivated a driver's account because of a facial recognition software error that registered the employee, who is Black, as

28. *See infra* Part V.

using someone else's photo for verification purposes.[29] In the marketplace, companies are attempting to incorporate the technology to make more effective marketing choices and better business decisions. Some companies are selling their products to consumers to connect to the Internet of Things and create consumer conveniences such as smart homes and child monitoring.[30] How companies are collecting data from employees or consumers to create or implement these products and services (whether anonymously or otherwise) has raised concerns and could implicate privacy issues.[31] Nevertheless, there are beneficial uses to businesses and consumers alike.

*a. Shopping*

While some companies use facial recognition technology to identify customers, some use it to identify shoppers' patterns.[32] Some shopping centers have started to use facial recognition to track paths of travel anonymously. Artificial intelligence is then used to mine that data to determine such things as traffic patterns, worker performance, and consumer reaction to displays and marketing.[33] Commercial landlords could mine

29. Fambrough v. Uber Techs., Inc., No. 4:19-cv-0398-DGK, 2019 U.S. Dist. LEXIS 95926 (W.D. Mo. June 7, 2019) (denying the plaintiff's motion for emergency injunctive relief, reasoning that damages would have been an adequate remedy).

30. *See, e.g.*, Amy Gamerman, *Home Is Where They Know Your Name (and Face, Hands and Fingerprints)*, WALL ST. J. (June 20, 2019), https://perma.cc/A3AW-W8FL (discussing the integration of biometric technology, such as fingerprint scans and facial recognition software, to allow residents to access their homes and amenities); Julie Jargon, *Facial Recognition Tech Comes to Schools and Summer Camps*, WALL ST. J. (July 30, 2019), https://perma.cc/J7U4-AZ5C (describing facial recognition technology that allows photos to quickly review group photos including their child instead of requiring parents to sort through all photos).

31. *See infra* Part III.

32. *See* Esther Fung, *Shopping Centers Exploring Facial Recognition in Brave New World of Retail*, WALL ST. J. (July 2, 2019), https://perma.cc/J35Y-MXJW.

33. *See id.*

this data on consumer behavior to demonstrate and increase the value of brick-and-mortar stores.[34] Aside from marketing patterns, shopping centers also use this technology for security and to identify shoplifters. As I discuss later,[35] there is currently no federal legislation regarding companies' disclosure to consumers about their use of facial-recognition technology or how to obtain consent from individuals in commercial spaces. Three states—Illinois, Texas and Washington—have passed bills to protect biometric information such as faces and other physical attributes.[36]

*b. Photo Sharing*

Consumers, for their part, are enjoying the conveniences that this technology offers. For instance, parents can opt in to receive updates about their children at camp.[37] Camps either pay for the software themselves and offer it to parents or ask parents to pay directly at a daily price.[38] Parents who sign up must submit a reference photo of their child so that the program's artificial intelligence can detect a match between the reference photo and photos taken while at camp, which then automatically sends matched photos to the parents.[39] This allows them to receive photos of their camper without having to sift through hundreds of group shots of other children. The images are stored until a parent asks for them to be deleted.

---

34. *See id.*

35. *See infra* Part IV.

36. *See infra* Part IV.B.

37. *See* Julie Jargon, *supra* note 30.

38. *See, e.g.*, *id.*

39. *See* Melissa Kay, *Waldo, a Facial Recognition Tool, Wants to Track Your Kids This Summer*, GEAR BRAIN (July 30, 2018), https://perma.cc/BD5X-UVQ5 (detailing Waldo's facial recognition software used in camps in which parents submit a photo that is used as a baseline reference to notify parents of when a new photo containing their children's image is uploaded).

People like to post photos on social media, seemingly without thinking about where those photos might end up or how they may be used.[40] In addition to ubiquitous sites like Facebook and Instagram where people share photos with their friends, there is, for instance, a Russian app called FaceApp that encourages the uploading of selfies so people can see what they might look like when they are older.[41] The almost immediate widespread popularity of FaceApp implicates privacy concerns, especially because it is unclear how much data employees have access to, but to date, there does not appear to be any indication of data misuse.[42] FaceApp's terms of service require access to all of the app user's photos.[43] The user must also consent to FaceApp's ability to collect and transfer data about the user to any country in which FaceApp conducts business.[44]

---

40. In 2014, internet users uploaded an average of 1.8 billion images per day across all platforms. In 2020, there are significantly more platforms and 3.8 billion people of Earth's 7.75 billion population are social media users, which suggests that daily upload image counts will continue to rise. *See generally* Jim Edwards, *Planet Selfie: We're Now Posting A Staggering 1.8 Billion Photos Every Day*, BUS. INSIDER (May 28, 2014), https://perma.cc/LW73-UU3M;

Simon Kemp, *Digital 2020: 3.8 Billion People Use Social Media*, WE ARE SOCIAL (Jan. 30, 2020), https://perma.cc/HAP6-4QHQ.

41. *See* Mansoor Iqbal, *FaceApp Revenue and Usage Statistics*, BUS. OF APPS (Oct. 15, 2020), https://perma.cc/VL6J-8FTT (estimating that as of July 2019, between 80 and 86 million FaceApp users uploaded photos to FaceApp).

42. *See* Thomas Brewster, *FaceApp: Is the Russian Face-Aging App a Danger to Your Privacy?*, FORBES (July 17, 2019,), https://perma.cc/MF6X-YEN5.

43. *See* Christopher Brito, *All Your Friends Are Posting Aging Selfies with FaceApp – A Russian App That's Raising Privacy Concerns*, CBS NEWS (July 17, 2019, 4:51 PM), https://perma.cc/M87G-N9GE. *But see* Natasha Lomas, *FaceApp Responds to Privacy Concerns,* TECH CRUNCH (July 17, 2019), https://perma.cc/RMD7-B6V2 (detailing FaceApp founder Yaroslav Goncharov's statement that FaceApp does not sell user data or transmit such data to Russia and that FaceApp allows users to determine when their data is deleted).

44. *See* Brito, *supra* note 43. *But see* Lomas, *supra* note 43.

*c. Schools*

Aside from convenience and fun, safety-conscious individuals and entities are also receiving value from facial recognition technology. Some schools, for example, are able to maintain a database of adults who are restricted from the campus. If an adult is matched to those on the list, administrators receive an alert.[45] In an effort to increase security measures, schools across the country spent an estimated $2.7 billon on security in 2017, including equipment and services.[46] One facial recognition software manufacturer has proposed installing its technology to help identify and track potential shooters on campus.[47] The Lockport City School District in upstate New York became one of the first school systems in the nation to purchase facial recognition software.[48] The Canadian company's AEGIS software used by the school district creates a database containing photos of students and adults to be trespassed from campus, which is then integrated into school cameras to scan for a match.[49] If one is detected, school administrators receive an alert.

This type of integration inherently raises a host of issues because of the collection of biometric data belonging to minors.[50] Among them is the

---

45. *See* Jargon, *supra* note 30.

46. Emily Tate, *With Safety in Mind, Schools Turn to Facial Recognition Technology. But at What Cost?*, EDSURGE (Jan. 31, 2019), https://perma.cc/9LA4-YDWR.

47. *See AEGIS To Shield and Protect from Danger*, SN TECHNOLOGIES, https://perma.cc/K9XW-XYAX (last visited Aug. 6, 2020); Zak Doffman, *New York School District First in U.S. to Adopt Controversial Facial Recognition*, FORBES (May 30, 2019), https://perma.cc/QV2M-SQ4B (including statement of President of SN Technologies, KC Flynn: "[AEGIS] compares all faces seen throughout the building against a school-built and controlled database that includes only individuals that are not allowed on school premises or that are a known threat to the School District. Students are not included in any database nor are any faces seen by the software stored in the system").

48. *See* Doffman, *supra* note 47.

49. *See* Jargon, *supra* note 30.

50. *See* Nila Bala, *The Danger of Facial Recognition in our Children's Classrooms*, 18 DUKE L. & TECH. REV. 249 (2020).

question of whether minors' biometric data should be regulated differently, even when there is parental consent. In 2019, the Federal Trade Commission ("FTC") launched a review under the Children's Online Privacy Protection Act ("COPPA"), a 1998 law that requires websites to obtain parental consent before collecting, using, or disclosing a child's personal information.[51] As defined, this covers information such as name, address, online user name, phone and social security number, geolocation information, and "photograph, video, or audio file, where such file contains a child's image or voice."[52] As of July 2020, the issue of allowing companies to use facial recognition technology with children is unresolved because COPPA's definition of "personal information" has not been amended to specifically include facial recognition data (not just photographs or images).[53] Thus, an open question is whether the definition of "personal information" should be expanded to include biometric data. More recently, in light of the COVID-19 pandemic and the nationwide shift to online learning, the FTC has allowed schools to consent to collection of students' personal data, as long as the data is education-related and not intended for other commercial purposes.[54]

*d. Homes*

Facial recognition technology has also entered private homes and is being implemented in "smart homes."[55] High end listings now mention "biometric" features as amenities to attract tenants and buyers.[56] These

51. 15 U.S.C. §§ 6501-6505 (2018).

52. 16 C.F.R. § 312.5 (2005).

53. *See id.*; *see also Complying with COPPA: Frequently Asked Questions*, FEDERAL TRADE COMMISSION (July 2020), https://perma.cc/JTJ5-GFYJ.

54. *See* Lisa Weintraub Schifferle, *COPPA Guidance for Ed Tech Companies and Schools During the Coronavirus*, FEDERAL TRADE COMMISSION (Apr. 9, 2020), https://perma.cc/KM7W-56Y6.

55. *See* Gamerman, *supra* note 30.

56. Antonio Pacheco, *High-end Homes Are Going Biometric*, ARCHINECT (June 24, 2019), https://perma.cc/DX5C-TNW2.

smart homes can recognize the resident when he or she enters, and certain preferences or access can be enabled.[57] For example, at 15 Hudson Yards, an 88-story Manhattan luxury building, residents can touch a fingerprint scanner to get access to the private spa, golf simulator and screening room.[58] Down in Miami, 2000 Ocean, a luxury tower projected to be completed in 2021, will use digital video cameras with facial recognition technology to screen and welcome residents home.[59] Even owners of older homes are able to retrofit their properties to add biometric features. From fingerprint scanners on wine rooms and even dressing rooms, to security features for securing guns and rifles, biometric technology has entered our homes. Many users and potential users are concerned about who else may get access to the personal information used for biometric systems, including their faceprints and fingerprints. To address this concern, companies generally protect the information with a combination of encryption and storage on secured devices, networks, and servers.[60]

*2. Government Use*

The government is probably the largest consumer of facial recognition technology in the US today. The use of facial recognition technology by government agencies, especially in the criminal justice and law enforcement context, has received extensive treatment in the literature[61] and is largely outside the scope of this Article. However, to provide context for the reader, a brief survey of some of the more common uses by the government will be provided here. Moreover, there is also the issue

57. *See* Gamerman, *supra* note 30.

58. *See id.*; *see also* FIFTEEN HUDSON YARDS, https://perma.cc/EW7K-THBC (last visited Sept. 23, 2020).

59. *See* Gamerman, *supra* note 30; *see also* 2000 OCEAN, https://perma.cc/VH9T-9Z7Q.

60. *See* Gamerman, *supra* note 30.

61. *See supra* note 1.

of private-government partnerships in the provision and use of this technology. Thus, to the extent that private companies are providing and creating the technology to be used by the government, the relevant issues are intertwined and the discussion in this Article is applicable to the considerations of the government's collection, storage, use, and sharing of facial recognition technology.

*a. Airports*

Facial recognition technology has been used in over three million instances by Customs and Border Protection since June 2017.[62] At about a dozen US airports, customs officers collect photos of travelers' faces when they land in the United States.[63] It is optional for US citizens but mandatory for non-US citizens.[64] At fifteen airports, including the international airports in Atlanta, Chicago, Los Angeles, Miami, and Orlando, cameras take facial scans of travelers before they leave the country.[65] It is unclear whether US citizens realize they can refuse to participate.[66] By 2021, facial recognition will be expanded to the top twenty US airports

62. *See* Lori Aratani, *Facial-Recognition Scanners at Airports Raise Privacy Concerns*, WASH. POST (Sept. 15, 2018), https://perma.cc/Y2ME-ZZE3.

63. *See* Aaron Sankin, *Can I Opt Out of Facial Scans at the Airport?*, MARKUP (Mar. 2, 2020), https://perma.cc/8FW4-TMZN (explaining that matched facial recognition photos are retained for twelve hours for US citizens travelling domestically. Records for international travel by US citizens are maintained for fifteen years, while travel records involving non-immigrant aliens are stored for seventy-five years).

64. *See* Aratani, *supra* note 62.

65. *See* Kate O'Flaherty, *Facial Recognition at U.S. Airports. Should You Be Concerned?*, FORBES (Mar. 11, 2019), https://perma.cc/SB9S-4Q9R.

66. *See* Sankin, *supra* note 63 (noting that airlines utilizing facial recognition services include JetBlue, Delta, American Airlines, British Airways, and Lufthansa, all of which allow voluntary opt-out, but refusal may be more difficult depending on individual circumstances when International travel is involved).

for 100% of international passengers, including US citizens.[67] Airports and airlines have also been trying different versions of the biometric programs. At some airports, travelers have their pictures taken with iPads installed at departure gates. The image is then compared with a "gallery" of images pulled from Department of Homeland Security records, including passport or visa photos of all travelers on the flight. If the images match, the screen flashes green, and the person is allowed to board. If there is a mismatch, the screen flashes red, and the person may be pulled aside for additional screening.[68]

*b. Law Enforcement*

Police use facial recognition technology for a wide range of functions, from monitoring protests and demonstrations to identifying suspects in security footage. Facial recognition was used by Baltimore Police to monitor protesters during the unrest and rioting after the death of Freddie Gray, leading to the apprehension and arrest of protestors who had outstanding warrants.[69] More recently, the Department of Homeland Security recorded more than 270 hours of surveillance footage from fifteen

67. Exec. Order No. 13,780 § 8, 82 Fed. Reg. 13,209 (Mar. 6, 2017); O'Flaherty, *supra* note 65.

68. *See* Aratani, *supra* note 62.

69. *See* Malkia Devich-Cyril, *Defund Facial Recognition*, ATLANTIC (July 5, 2020), https://perma.cc/HJ89-WS4Q; Kevin Rector & Alison Knezevich, *Maryland's Use of Facial Recognition Software Questioned by Researchers, Civil Liberties Advocates*, BALT. SUN (Oct. 18, 2016), https://perma.cc/HK2X-HJ8C. Some courts have determined that law enforcement's use of photography at public demonstrations does not violate the First Amendment right to freedom of association. *See* Laird v. Tatum, 408 U.S. 1 (1972); Phila. Yearly Meeting of Religious Soc'y of Friends v. Tate, 519 F.2d 1335, 1337–38 (3d Cir. 1975); Donohoe v. Duling, 465 F.2d 196, 202 (4th Cir. 1972). Under the *Katz* test, an individual would not have an automatic expectation of privacy with respect to his or her face because it is exposed to the public. *See* United States v. Dionisio, 410 U.S. 1, 14 (1973). And although *Kyllo* addressed a technology that could reach into someone's home,

cities involving the protests against George Floyd's killing.[70] Customs and Border Protection have made the footage available to other federal and local law enforcement agencies for future investigations.[71]

Ultimately, it is expected that law enforcement will seek to use facial recognition technology for retroactive and real-time analysis of faces for immediate identification. For example, in the first publicized case of faulty facial recognition, Robert Julian-Borchak Williams, a black male, was arrested as a result of misidentification based on a grainy surveillance photo.[72] Police relied on facial recognition software which, according to the company's general manager, did not conduct accuracy testing and resulted in Williams spending a night in jail.[73]

It soon may be possible for an officer's body-worn camera to use facial recognition technology to identify a person he or she observes on the street. Major police departments are exploring real-time face recognition on live surveillance camera video. Real-time face recognition also lets police continuously scan the faces of pedestrians walking by a street surveillance camera. Whether an individual's public movements captured by facial recognition technology implicate the Fourth Amendment may depend on the timeframe of the surveillance and what it could reveal

---

which (unlike facial recognition technology) is clearly a private area, some commentators have considered the application of *Kyllo* in terms of the limited availability of the technology to facial recognition technology. *See, e.g.*, Michele M. Jochner, *Privacy Versus Cyber-Age Police Investigation – The Fourth Amendment in Flux,* 90 ILL. BAR J. 70, 75 (2002).

70. *See* Tal Axelrod, *Trump Admin Used Drones, Helicopters to Surveil George Floyd Protests in 15 Cities*, HILL (June 19, 2020), https://perma.cc/EQR9-D5PU; Zolan Kanno-Youngs, *U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance*, N.Y. TIMES (June 19, 2020), https://perma.cc/DJX2-UZ5H (noting that the US government surveilled cities including Dayton, OH, Minneapolis, MN, Philadelphia, PA, Washington, D.C., New York City, NY, Detroit, MI, and Buffalo, NY).

71. See Kanno-Youngs, *supra* note 70.

72. *See* Hill, *supra* note 2.

73. *See id.*

about the individual's personal life, such that it could be considered a Fourth Amendment search.[74]

*c. From the DMV to Public Housing*

The technology is also being implemented by government agencies, like state departments of motor vehicles (DMVs), as part of their internal operations. For instance, New York has identified over 10,000 people with more than one driver's license with the help of this technology.[75] Similarly, the New Jersey Motor Vehicle Commission has identified and referred about 2,500 fraud cases to law enforcement since 2011.[76]

Some public housing projects also use facial recognition technology to aid law enforcement. Earlier this year, two public housing units in Detroit were fitted with security cameras to provide round-the-clock video footage that could be made available to the Detroit Police Department.[77] Senator Corey Booker has introduced legislation to ban the use of facial recognition technology in public housing.[78]

*B. In China*

China has been at the forefront of developing facial-recognition technology, which is now used everywhere from government and corporate

74. *See* Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. (forthcoming 2020) (discussing Fourth Amendment concerns where facial recognition is concerned).

75. *See* Clare Garvie & Jonathan Frankle, *Facial-Recognition Software Might Have a Racial Bias Problem*, ATLANTIC (Apr. 7, 2016), https://perma.cc/AB7W-Y3BR; Justin Lee, *NY DMV Use of Facial Recognition Resulted in More than 4,000 Arrests Since 2010*, BIOMETRIC UPDATE (Aug. 22, 2017), https://perma.cc/435B-2NLM.

76. *See* Garvie & Frankel, *supra* note 75.

77. *See* Lola Fadulu, *Facial Recognition Technology in Public Housing Prompts Backlash*, N.Y. TIMES (Sept. 24, 2019), https://perma.cc/V75L-GKLM.

78. *Booker Introduces Bill Banning Facial Recognition Technology in Public Housing*, CORY BOOKER (Nov. 1, 2019), https://perma.cc/5S6J-XMR4.

surveillance of citizens and employees, to toilet-paper dispensers in public bathrooms.[79] The technology has become fully integrated into Chinese society for both business and government use.

China serves as an interesting point of comparison concerning the facial recognition technology debate in the US. That is because it has implemented very advanced uses of the technology with effectively no regulation. Biometric data collected from facial-recognition-enabled surveillance systems in China may be protected by the Personal Information Security Specifications.[80] This regulation, China's first major data privacy rule, provides that collection of personal information should be for "legal, justified, necessary, and specific purposes."[81] It often requires consent, and the information must be kept secure.[82] Commentators have noted, however, that there is little enforcement and biometric data is frequently collected without consent or sufficient data security protections, particularly now during the COVID-19 pandemic.[83]

Another reason why China is important to this background and analysis, is because China's rapid development of its artificial-intelligence-driven facial recognition technology does not remain within its borders and is exported around the world, including to the US. The Carnegie Endowment for International Peace has found that Chinese companies supply these surveillance technologies to sixty-three countries.[84] As a member of the Federal Communications Commission has cautioned, "If governments, organizations, and companies that value civil liberties

79. *See* Travis M. Andrews, *China Uses Facial Recognition Software to Crack Down on Toilet Paper Theft*, WASH. POST (Mar. 21, 2017), https://perma.cc/LAY5-BTQ2.

80. *See* Lauren Dudley, *China's Ubiquitous Facial Recognition Tech Sparks Privacy Backlash*, DIPLOMAT (Mar. 7, 2020), https://perma.cc/PLP5-5URB.

81. *See* Mingli Shi et al., *Translation: China's Personal Information Security Specification*, NEW AM. (Feb. 8, 2019), https://perma.cc/2W6V-LALE.

82. *See id.*

83. *See* Dudley, *supra* note 80.

84. *See* Steven Feldstein, *The Global Expansion of AI Surveillance*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Sept. 17, 2019), https://perma.cc/L7VK-NVNB.

don't get in the game, we may soon find ourselves living in a world that authoritarians have shaped for us."[85]

*a. Business Use*

Chinese companies across many sectors are implementing facial recognition technology to enhance their decision making.[86] For instance, one company uses facial recognition software to assess not only the health of potential clients, but people's level of honesty.[87] Apparently at least one insurance company uses face scans to determine whether a person is a smoker.[88] Another company, SenseTime, developed facial recognition software to detect jaywalkers and issue instantaneous fines via text messages.[89] Financial companies also use the facial recognition technology to shorten loan approval time by scanning an applicant's face to obtain an instantaneous credit score.[90] In addition, from an approximately 15-minute online video interview, loan applicants' facial expressions are analyzed for "eye-shifting or other suspicious behavior."[91]

---

85. Henry Kenyon, *U.S. Must Lead in Setting Global AI Tech Standards, FCC's Starks Says*, CQ ROLL CALL (Jan. 10, 2020), https://perma.cc/8R4J-FTQF.

86. *See* Zhou Wei, *What Your Face May Tell Lenders About Whether You're Creditworthy*, WALL ST. J. (June 10, 2019), https://perma.cc/N3AF-2N8W.

87. *See id.*

88. *See* Wei, *supra* note 86.

89. *See* Claudia Geib, *If You Jaywalk in China, Facial Recognition Means You'll Walk Away with a Fine*, FUTURISM (Mar. 30, 2018), https://perma.cc/2ZJT-ARUR; Christina Zhao, *Jaywalking in China: Facial Recognition Surveillance Will Soon Fine Citizens via Text Message*, NEWSWEEK (Mar. 27, 2018, 9:34 AM), https://perma.cc/7YNZ-F2SB.

90. *See* Wei, *supra* note 86. Chinese credit scoring system uses scores ranging from 350 to 950 and is dependent upon a thousand variables from five data sets. When an individual has negative credit history or incidents, facial recognition (e.g., from a pedestrian surveillance camera) scans may result in the individual's face being broadcasted on nearby billboards. *See, e.g.*, Charlie Campbell, *How China Is Using "Social Credit Scores" to Reward and Punish Its Citizens*, TIME (2019), https://perma.cc/4LS5-FLDU.

91. *See* Wei, *supra* note 86.

Chinese companies have far surpassed American companies in their use of facial recognition technology for mobile payments.[92] Chinese citizens have moved beyond using their phones to make payments; they simply need to look into tablet-sized screens, which quickly scan for facial width, height, and depth measurements.[93] Beyond a wallet with credit cards or cash, even the smartphone has been replaced with variations of "smile to pay" features at the checkout.[94]

Facial recognition machines for payment are everywhere from vending machines, grocery stores, bakeries, subway systems, and hospitals, where three dimensional cameras verify consumers' identities.[95] In some stores, facial-identifying payment machines have completely replaced cashiers.[96] A 2018 survey found that 85% of mobile-payment users in China were willing to make payments using biometric methods such as facial and fingerprint identification, but over 70% noted their biggest concern to be the safety of their personal data.[97] Respondents were particularly concerned about biometric data hacking and data leaks.[98] Unfortunately, Chinese citizens may not have much of a choice given that Chinese government officials are already mandating facial scans as a condition for internet use.[99]

---

92. *See* Stella Yifan Xie, *Using Smartphones to Pay? That's So Yesterday in China*, WALL ST. J. (June 10, 2019), https://perma.cc/4HRA-G8NT.

93. *See* Agence France-Presse, *Smile-to-Pay: Chinese Shoppers Turn to Facial Payment Technology*, GUARDIAN (Sept. 4, 2019), https://perma.cc/YBY7-KQER.

94. Fottrell, *supra*, note 21 (describing "smile to pay" at KFC).

95. *See* Shannon Liao, *A Chinese Subway Is Experimenting with Facial Recognition to Pay for Fares*, VERGE (Mar. 13, 2019), https://perma.cc/7DFZ-NMLF; France-Presse, *supra* 93; Chris Burt, *Chinese Companies Collaborate on Facial Recognition Vending Refrigerator*, BIOMETRIC UPDATE (May 15, 2019), https://perma.cc/AJ7H-6E3H.

96. *See* Xie, *supra* note 92.

97. *Id.*

98. Sam Shead, *Chinese Residents Worry About Rise of Facial Recognition*, BBC NEWS (Dec. 5, 2019), https://perma.cc/VP4T-3TS6.

99. *See* Rosie Perper, *Chinese Government Forces People to Scan Their Face*

In light of COVID-19, SenseTime has also developed new technology to allow for facial recognition even when individuals are wearing face masks.[100] The algorithm will also incorporate thermal imaging cameras and mask recognition to detect when people are not wearing masks in public.[101]

*b. Government Uses*

Chinese scientists have developed a cloud camera system which uses artificial intelligence and can detect thousands of faces at a time and "generate their facial data for the cloud[,] while locating a particular target in an instant."[102] Seemingly unconstrained by regulations, Chinese authorities could conceivably use facial recognition technology everywhere: streets, subway stations, airports, and border check points.[103]

At an even more advanced (and potentially alarming) application, Chinese citizens' DNA samples are being collected as part of a 2017 project designed to use DNA samples to produce facial images.[104] This project has raised many ethical concerns.[105] Among them is a suspicion that the government is collecting DNA of the Uighurs without informed consent, under the facade of the government's mandatory health check program, Physicals for All.[106] If individuals refuse, their families may be

*Before They Can Use Internet as Surveillance Efforts Mount*, BUS. INSIDER (Dec. 2, 2019), https://perma.cc/2H8C-3KUL.

100. Jane Li, *China's Facial-Recognition Giant Says It Can Crack Masked Faces During the Coronavirus*, QUARTZ (Feb. 18, 2020), https://perma.cc/TEV2-EFMY.

101. *Id*.

102. *Id.*

103. *Id.*

104. *See* Sui-Lee Wee & Paul Mozur, *China Uses DNA to Map Faces, with Help from the West*, N.Y. TIMES (Dec. 3, 2019), https://perma.cc/CEB3-B4BX.

105. *Id.*

106. *Id*.

black-listed and subsequently unable to travel or go to a hospital.[107] Thus, questions have been raised about whether this program is being used for racial profiling and other discriminatory purposes against the Uighurs,[108] who were previously sent to concentration camps in large numbers in 2014 and encounter DNA checkpoints more often than other groups.[109] As this controversy unfolded, it was discovered that a Massachusetts company, Thermo Fisher Scientific, provided the software used to analyze the DNA fragments.[110] The company announced in early 2020 that it would suspend sales to the program,[111] but Thermo Fisher has apparently continued to sell its DNA testing kits to Chinese authorities and defended its business.[112]

## III. CONCERNS

The debate surrounding facial recognition technology stems from concerns about how we collect, store, share, and use the technology. In an effort to better understand the stakeholders, their concerns, and the extent to which they may influence how or whether we choose to regulate in this space, this Part categorizes and presents these concerns. The sections below will address collection and privacy, accuracy, race and gender biases, religious objections, storage and data privacy, as well as misuse of the data.

---

107. Jennifer Pak, *Inside China's "Social Credit" System, Which Blacklists Citizens*, MARKETPLACE (Feb. 13, 2018), https://perma.cc/H7EG-467H.

108. *See* Wee & Mozur, *supra* note 105.

109. Ross Andersen, *The Panopticon Is Already Here*, ATLANTIC (Sept. 2020), https://perma.cc/N35T-WRE6.

110. *See* Wee & Mozur, *supra* note 105.

111. *Id.*

112. *Id.*; *see also* Jim Nash, *U.S. DNA Firm Thermo Fisher Reportedly Still Helping China Tamp Unrest, Crime*, BIOMETRIC UPDATE (June 19, 2020), https://perma.cc/PQ9N-ZT3A.

*A. Collection & Privacy*

One of the biggest areas of concern for consumers relates to the collection of the photos and biometric data used to create the various databases and algorithms used with facial recognition technology. Many worry that without privacy regulations, companies are free to collect photos and create large databases that can be shared with other companies. One program that has received attention is MegaFace, a facial recognition software program that collected millions of faces from Flickr to develop and train its algorithm.[113] Flickr users were not aware that their photos were being used or that many of the photos used were of minors.[114] "MegaFace's creation was financed in part by Samsung, Google's Faculty Research Award, and by the National Science Foundation/Intel."[115] MegaFace is not anonymized; but while it does not contain names, each photo includes a numerical identifier that links back to the original Flickr photographer's account.[116] This program was created by researchers at the University of Washington, but it has since been decommissioned and is reportedly no longer distributing data.[117]

About 100 million photos and videos from Flickr have also been released by Yahoo (its parent company).[118] The images were apparently all licensed under Creative Commons licenses.[119] While notice was not provided to users that their photos and videos were released, there was a

113. *See* Kashmir Hill & Aaron Krolik, *How Photos of Your Kids Are Powering Surveillance Technology*, N.Y. TIMES (Oct. 11, 2019), https://perma.cc/Q29X-ZYU3.

114. *See* Mary Meisenzahl, *If You Uploaded Photos of Your Kids to Flickr They Might Have Been Used to Train AI*, BUS. INSIDER (Oct. 17, 2019, 12:37 PM), https://perma.cc/5TAP-JBTS.

115. *See* Hill & Krolik, *supra* note 113.

116. *Id.*

117. *MegaFace and MF2: Million-Scale Face Recognition*, MEGAFACE (2015), https://perma.cc/3JQ8-ANMV.

118. *See* Hill & Krolik, *supra* note 113.

119. *MF2 Training Dataset*, MEGAFACE (2015), https://perma.cc/62FH-YDTE.

safeguard built in such that only links to the photos, and not the photos themselves, were distributed.[120] That way, if a user deleted the images or made them private, they would no longer be accessible through the database.

Some blame permissive privacy laws in the United States for allowing companies to use millions of people's faces without their knowledge in order to promulgate facial recognition technology.[121] Currently, most Americans have limited recourse for such use of their photos, unless they are from Illinois and are protected by the Biometric Information Privacy Act (BIPA).[122] Indeed, it is questionable whether photos themselves, as opposed to scans of the photos, are covered by the Biometric Information Privacy Act.

Facial recognition technology involving minors pose special concerns. For example, the lower accuracy with which the technology can detect rapidly-changing young faces is especially concerning. As a result, face-recognition systems tend to perform poorly on young people. This is partly why researchers saw some promise in the Flickr database which contained millions of photos of children (probably from all the parents who love posting photos of their kids online).[123] Professor Stacey Steinberg has noted that over 90% of two-year-olds have an online presence, thanks to their parents.[124] Furthermore, there is also the question of whether there ought to be different rules for consent or regulations tailored to minors. Moreover, this issue is particularly salient when the concept of children's right to privacy or consent arises elsewhere in the technology landscape. A recent class action lawsuit, for example, alleged that

120. *See* Hill, *supra* note 2.

121. *Id.*

122. *Id.*; 740 ILL. COMP. STAT. ANN. § 14/15 (2008).

123. *See* Stacey B. Steinberg, *Sharenting: Children's Privacy in the Age of Social Media*, 66 EMORY L.J. 839, 842, 846 (2017) (noting that even the most well-intentioned parents may not consider the full implications of sharing their children's photos online, which children have no control over).

124. *Id.* at 849.

TikTok illegally collected location data and images of young people's faces to share with China.[125]

### *B. Accuracy*

Unlike DNA or fingerprints, faces change over time. This simple fact can trigger incorrect results with facial recognition technology when an individual's hairstyle, facial hair, facial jewelry, or body weight changes.[126] Some research indicates that facial recognition algorithms may not be as accurate at reading the faces of certain demographics, in particular African Americans.[127]

Despite these concerns about accuracy, law enforcement relies heavily on facial recognition technology.[128] At least twenty-one states allow law enforcement to run or request searches against their driver's license databases.[129] About half of all American adults have their photos searched in this manner, and, curiously, the FBI has built a biometric network that primarily includes Americans with no prior criminal backgrounds.[130]

Even though many concerns have been raised about the accuracy of facial recognition technology, one report reveals that the only police de-

---

125. *See* Bobby Allyn, *Class-Action Lawsuit Claims TikTok Steals Kids' Data and Sends It to China*, NPR (Aug. 4, 2020, 1:39 PM), https://perma.cc/W5ZG-UZ2E.

126. *See, e.g.*, Umar Toseeb et al., *The Significance of Hair for Face Recognition*, 7 PLOS ONE e34144 (2012).

127. *See* Garvie & Frankel, *supra* note 75.

128. *Id.*

129. *See* Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, WASH. POST (July 7, 2019, 3:54 PM), https://perma.cc/7GSJ-7ANW.

130. David Cuthbertson, *Privacy Impact Assessment Integrated Automated Fingerprint Identification System National Security Enhancements*, FBI (Oct. 15, 2020), https://perma.cc/BW7K-KTA9; *see also* 28 U.S.C. § 534 (2011) (providing the FBI with statutory authority to collect, preserve, and exchange individual information for governmental purposes).

partment still using the technology that conditions its purchase on accuracy tests is Seattle region's South Sound 911.[131] For their part, the providers of the technology have an interest in ensuring its accuracy, but may also disclaim liability if errors occur.[132]

### *C. Race & Gender Disparities*

The failures of this kind of artificial intelligence to adequately address gender and race issues have made headlines. A recently published story of an innocent black man whose arrest was based on a flawed match from a facial recognition algorithm evidenced the concern that the technology does not perform as well when identifying minorities.[133] CNN has also reported that some "algorithms were up to 100 times more likely to confuse two different non-white people" than two white people, and that Asians, Blacks, and Native Americans were particularly likely to be misidentified.[134] In another test, black women were more likely than other race and gender groups to be falsely identified in a large database of mugshots maintained by the FBI.[135] Similarly, the Washington Post reported a few months ago that, according to the NIST, the accuracy of facial recognition technology's algorithms may worsen based on age, gender, or race.[136]

---

131. *See* Garvie & Frankel, *supra* note 75 (while the report also notes that the San Francisco Police Department had also set an accuracy criterion, San Francisco has since banned the use of facial recognition technology); *see infra*, notes 221-226.

132. *See, e.g.*, FACEFIRST (Oct. 15, 2020), https://perma.cc/F6PK-L9V4.

133. Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (June 25, 2020), https://perma.cc/F7UB-RFDW.

134. *See* Brian Fung, *Facial Recognition Systems Show Rampant Racial Bias, Government Study Finds*, CNN (Dec. 19, 2019, 6:37 PM), https://perma.cc/36QY-J9G5.

135. *Id.*

136. *See* Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial Recognition Systems, Casts Doubt on Their Expanding Use*, WASH. POST (Dec. 19, 2019, 6:43 PM), https://perma.cc/ZF94-B439.

Moreover, Amazon discovered that its algorithm for job applicants excluded women because it flagged qualified applicants based on historical trends that favored men.[137] A 2018 study by the ACLU using Amazon's facial recognition software scanned the face of each member of Congress against mugshots and revealed no less than twenty-eight false positive matches.[138] Amazon is not alone in the face of this criticism. IBM's facial recognition software was found to have misidentified gender in up to 7% of lighter-skinned females, up to 12% of darker-skinned males, and up to 35% of darker-skinned females.[139]

Additionally, because some law enforcement systems have disproportionately collected the biometric information of Blacks and Latinos, the facial recognition technology used by the FBI and other agencies may be more likely to misidentify Blacks and Latinos than other groups of people.[140] As a result, law-abiding citizens have been mistakenly identified as terrorism suspects by government biometric identification programs.[141]

Beyond the law enforcement context, there are additional concerns about possible threats to safety and civil rights by the continued use of facial recognition technology. In a letter to Housing and Urban Development Secretary Ben Carson in December 2019, several Democratic senators asked the department to review policies for the use of facial recognition systems, claiming that the systems threatened marginalized

---

137. *See* Kenyon, *supra* note 85.

138. Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (July 26, 2018, 8:00 AM), https://perma.cc/XUQ9-TTWF.

139. *See* Hale, *supra* note 23.

140. *See* Pope, *supra* note 24, at 779.

141. *Id.* at 780 (an attorney, Brandon Mayfield, was mistakenly identified as a suspect in the aftermath of the 2004 Madrid bombings by a false positive match to his fingerprints).

communities and opened the door to unchecked government surveillance.[142] The FCC has also recognized that low-income communities may be negatively affected by the proliferation of facial recognition technology, due to the lower reliability of these algorithms when applied to minorities.[143] A Commerce Department's NIST study found, for example, that many facial recognition algorithms are more likely to misidentify Asians, African Americans and Native Americans relative to Caucasians.[144] The NIST research found the rate of false positives were up to a hundred times more likely for Asian and African American faces compared to white faces.[145] When compared against a database of other people's pictures (as would be used in the criminal justice context), black women had the highest rate of false positives.[146]

The Department of Homeland Security faced similar criticism after publication of a report which showed that the facial recognition technology it used misidentifies women and people of color at a higher rate than men and White individuals.[147] Custom and Border Patrol officials defended the use of the technology at ports and airports, but at least one member of Congress questioned whether promising applications for facial recognition technology outweigh the risks of "automated discrimination."[148]

---

142. See Tyler Sonnemaker, *Kamala Harris and Other Prominent Democrats Are Demanding an Investigation into How Facial Recognition Tech Is Being Used on People Who Live in Public Housing*, BUS. INSIDER (Dec. 18, 2019, 6:44 PM), https://perma.cc/2N5A-KBLU.

143. *See* Kenyon, *supra* note 6.

144. *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, NIST (Dec. 19, 2019), https://perma.cc/2ECA-HERX.

145. *Id.*

146. *Id.*

147. *See* Camila DeChalus, *DHS Facial Recognition Misidentifies Women, Minorities, Democrats Say*, CQ ROLL CALL (Feb. 7, 2020).

148. *Id.*

*D. Religious Objections*

The use of biometric technology can also conflict with religious freedoms. In *EEOC v. Consol Energy, Inc*., for example, an employee refused to use a biometric hand scanner for religious reasons.[149] The defendant company had started using a biometric hand scanner to keep track of its employees.[150] The plaintiff informed his supervisors that his religious convictions prevented him from using the biometric system, but he was denied a religious accommodation.[151] The employee was a devout evangelical Christian and believed the technology was related to the Antichrist. The Fourth Circuit affirmed the jury verdict in the employee's favor. [152] Evangelical Christians have been among the most vocal opponents of finger and palm scanning.[153]

*E. Storage and Data Security*

The storage of consumers' biometric data is of real concern, especially when the data collection occurs in homes and among household brands. Most access systems encrypt users' data and store it on their own data centers, on secured networks, or on the devices themselves. However, many potential users are concerned about who else could get access to the personal information used for biometric systems, including their faceprints and fingerprints, as biometric use expands globally with few regulations.[154] Another concern is hacking, which is not without merit. For example, a security company in charge of ensuring building security maintained a database that was unprotected and unencrypted, thereby

149. EEOC v. Consol Energy, Inc., 860 F.3d 131 (4th Cir. 2017).

150. *Id.*

151. *Id.*

152. *Id.*

153. *Biometric Technology is Here . . . So Are the Legal Challenges*, 36 NO. 2 TERMINATION. EMP. BULL. (Feb. 2020).

154. *See* Jayshree Pandya, *Hacking Our Identity: The Emerging Threats From Biometric Technology*, FORBES (Mar. 9, 2019), https://perma.cc/9X86-VW3Q.

making 23 gigabytes of data—or 27.8 million records—publicly available.[155] The database contained fingerprints and facial recognition information for over one million people and was accessed by UK Metropolitan Police, contractors, and banks.[156]

Most people with Apple devices, for instance, use their fingerprints or faces for access.[157] Apple represents that biometrics are never stored on its servers or in iCloud and are only stored directly on the user's device.[158] However, with the release of the iPhone X, Apple appears to have moved away from its promise to users when it began sharing facial data with third party applications through the phone's new "TrueDepth" camera.[159] Facial recognition is expanding beyond Apple as well, with estimates suggesting that in 2020 alone, over one billion smartphones will be shipped with facial recognition capabilities.[160] The company that presumably has the largest collection of its users' biometric data is Facebook.[161] Facebook claims that it has a "practically infinite" amount of facial data and that its database could allow its system to "recognize the entire population of earth."[162] Facebook's data collection policies have not been without controversy, however, as Facebook recently agreed to pay

155. *See* Josh Taylor, *Major Breach Found in Biometrics System Used by Banks, UK Police and Defence Firms*, GUARDIAN (Aug. 14, 2019), https://perma.cc/4VTN-EYCZ.

156. *Id.*

157. *See* Heather Kelly, *Fingerprints and Face Scans Are the Future of Smartphones. These Holdouts Refuse to Use Them*, WASH. POST (Nov. 15, 2019), https://perma.cc/D7EB-4B54 (noting that there are no exact statistics on the number of iPhone users who only use a passcode, but that as of 2016, Apple reported that 89% of compatible iPhone owners were using fingerprints to unlock their devices).

158. *See* Pope, supra note 24, at 782.

159. *Id.*

160. Chris Burt, *Counterpoint Estimates More than 1 Billion Smartphones to Be Shipped with Facial Recognition in 2020*, BIOMETRIC UPDATE (Feb. 9, 2018), https://perma.cc/2W43-CRVN.

161. *See* Pope, *supra* note 24, at 785.

162. *Id.* at 798.

$550 million to settle a facial recognition suit in which Facebook collected personal data without consent.[163]

An issue involving the storage of data by government agencies relates to requests by the public to produce the data. In one case, a Minnesota resident requested his biometric data from the local government, and because the government was not able to fully and quickly provide the data to the plaintiff, the government was found to have violated the state's Data Practices Act.[164] Minnesota's Data Practices Act governs the storage of government data and public access to that data.[165]

### *F. Misuse*

Ultimately, one concern that goes hand in hand with accuracy and potentially discriminatory use of facial recognition technology is misuse. Especially in the context of government or law enforcement use, the potential for abuse exists. It would therefore be important that certain safeguards be in place to help monitor that searches are not being conducted for illegitimate reasons. Such safeguards could include the police limiting access to those within the department who may use the software, and tracking searches that are conducted to help monitor that they are not being conducted for illegitimate reasons.[166] As Professor Eric Goldman has observed, "[i]magine a rogue law enforcement officer who wants to stalk potential romantic partners, or a foreign government using this to

163. Natasha Singer & Mike Isaac, *Facebook to Pay $550 Million to Settle Facial Recognition Suit*, N.Y. TIMES (Jan. 29, 2020), https://perma.cc/E5CP-3WG2; *see also In re* Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1171-72 (N.D. Cal. 2016) (denying defendant's motion to dismiss because images derived from photographs could reasonably fall within the scope of the Illinois BIPA's definition for biometric identifiers).

164. *See* Webster v. Hennepin Cnty., 910 N.W.2d 420 (Minn. 2018).

165. *Id.* at 427; Minn. Stat. §§ 13.01-13.90.

166. *See* Cindy Swirko, *Photo Software Brings Scrutiny to GPD*, GAINESVILLE SUN (Jan. 22, 2020), https://perma.cc/5NZS-6RQD.

dig up secrets about people to blackmail them or throw them in jail."[167] It is important that incentives and opportunities for dishonest and unethical uses of such powerful weapons are heavily reduced or controlled.

## IV. REGULATORY LANDSCAPE

There is currently no federal regulation of biometric data in the US.[168] As will be discussed further below, a few states have stepped in with their own regulations. Even the government use is unregulated. For instance, in the criminal context, there are no regulations on what access federal agencies have to state databases, and some states have given federal agencies, such as the Immigration and Customs Enforcement (ICE), access to their databases without notification.[169] Federal law-enforcement requests to state agencies for facial-recognition matches of potential suspects, a frequently used investigative practice, have raised concerns about civil liberties for years.[170]

On the corporate side, the lack of federal regulation has created much uncertainty for companies, and they have become strong voices on the question of regulation. As one concrete illustration, as companies move toward using facial recognition technology for something as relatively simple as payments, the regulatory landscape is difficult to assess other than in a piecemeal fashion.[171] Google Pay now allows payment authentication through biometric confirmation in lieu of a PIN code.[172] Walmart submitted a patent application for a blockchain currency that "may act as a pre-approved biometric (e.g., fingerprint or eye pattern) credit."[173]

---

167. *See* Hill, *supra* note 2.

168. *See* discussion *infra* accompanying notes 176-179.

169. *See* Dustin Volz, *ICE Taps States' Photo Databases to Hunt Criminal Suspects*, WALL ST. J. (July 8, 2019), https://perma.cc/32RT-TMDJ.

170. *Id.*; *see also supra* Part III.

171. *Id.*

172. *Require a Google PIN or Fingerprint to Send Money*, GOOGLE PAY HELP, https://perma.cc/A87E-EKRH (last visited Sept. 23, 2020).

173. U.S. Patent Application No. 62,624,721 (filed Jan. 31, 2018).

Not only do they have to be aware of security and data breach considerations, but relying on immutable biometric information to verify consumers' identities can prove thorny. The Illinois Biometric Information Privacy Act (BIPA), for instance, requires any private entity collecting biometric information to provide notice and obtain a written release from the individual.[174] In addition to the states that have adopted specific biometric regulations, the California Consumer Privacy Act (CCPA), which went into effect on January 1, 2020, is a comprehensive data privacy law that may also cover biometric information.[175]

Adding to the complex web of uncertainty on the payment systems is the possible applicability of the Gramm-Leach-Bliley Act (GLBA) at the federal level.[176] It may apply in lieu of state laws in certain scenarios, but companies should not assume that it will apply in every case. GLBA has limited application as it applies only to financial institutions and protects only information that consumers provide in connection with receiving financial products or services.[177] Thus, it is possible that, in some circumstances, GLBA could capture biometric information that is provided to verify payments.

Another federal law that could potentially cover some aspects of biometric data is the Stored Communication Act.[178] While it is not clear that the statute would apply, an argument can be made that it does cover biometric data because of its "any transfer of . . . data" language.[179] On the other hand, one could argue that the "transfer" is not being made as part of a communication. For example, the data is simply being collected and stored by the company (e.g., Facebook) and is not used for communication between users in the same sense that Facebook Messenger works

174. 740 ILL. COMP. STAT. ANN. § 14/15 (2008); *see infra* Part IV.

175. Cal. CIV. CODE § 1798.100 et seq.

176. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

177. *Gramm-Leach-Bliley Act*, FED. TRADE COMM'N, (last visited Sept. 23, 2020), https://perma.cc/R27N-ZZ7R.

178. 18 U.S.C. § 2510(12).

179. *Id.*

(i.e., a chat room).[180] There are, however, some scenarios where facial features are being used to actually communicate between users. The iPhone has a feature, for example, called Animoji that creates a cartoon animal/figure that mirrors your voice and facial expressions. Further, Snapchat allows users to send photos back and forth to communicate.

Congressional interest in passing biometric regulation has been high. On March 14, 2019, the US Senate introduced the Commercial Facial Recognition Privacy Act, which, if passed, would require companies to first obtain explicit user consent before collecting any facial recognition data.[181] It would also require notice that the technology is being utilized while informing about its capabilities and limits.[182]

The push for regulatory action seems to be coming largely from companies. That is itself telling and reveals an area of shared concern among the various stakeholders with interests in biometric data: the need for regulation. Nonetheless, the views are divergent on what that regulation should look like and the motivations for regulation. Other organizations, such as the ACLU, oppose the use of facial recognition technology because of the threat of racial and gender biases.[183]

For one thing, piecemeal state-by-state regulations for companies that do business nationally are, at the very least, inefficient and burdensome. As a result, leaders of some of America's largest businesses are advocating for federal privacy legislation to govern the collection, use and sharing of personal data across industry sectors in order to preempt state legislation. The proposed Consumer Privacy Legislation Framework, drafted by the Business Roundtable on behalf of the CEO's of some of America's largest companies, would cover:

---

180. *See In re* Search of a Residence of Oakland, 354 F. Supp. 3d 1010 (N.D. Cal. 2019).

181. S. 847, 116th Cong. (2019).

182. *See* Nelson, *supra* note 22.

183. *See* Pope, *supra* note 24, at 798.

> consumer data that is held by the organization and identifies or is identifiable to a natural, individual person. This information may include but is not limited to: name and other identifying information, such as government-issued identification numbers, and personal information derived from a specific device that reasonably could be used to identify a specific individual.[184]

Similar to the California Consumer Privacy Act, the legislation would provide consumers with a right of access, a right to opt out, and a right to deletion over their personal data that is collected and stored by companies.[185] While the definition does not specifically mention biometric data, such data could fall under the "identifies . . . a natural, individual person" language.[186]

### *A. Corporate Involvement*

It is noteworthy that companies that are themselves involved in the development of facial recognition software are pushing Congress to regulate. Most notably among these is Amazon. Amazon's policy team has drafted legislation that it hopes Congress will adopt.[187] Amazon wants to solidify the use of its facial recognition technology, "Rekognition." Amazon's proposals instinctively raise concerns or suspicions because of its self-interest. Amazon calls for "open, honest, and earnest dialogue among all parties involved to ensure that the technology is applied appropriately and is continuously enhanced."[188] According to Rekognition's FAQ page, however, images and videos may be stored and used

---

184. *See* Dominic Dhil Panakal, *What Does a Business Friendly National Privacy Law Look Like?*, NAT'L L. REV. (Oct. 3, 2019), https://perma.cc/ZZU6-S34S.

185. *Id.*

186. *Id.*

187. *See* Hale, *supra* note 23.

188. *See* Michael Punke, *Some Thoughts on Facial Recognition Legislation*, AMAZON WEB SERVICES MACHINE LEARNING BLOG (Feb. 7, 2019), https://perma.cc/C6PE-Y3VD.

for any of Amazon's machine learning or artificial intelligence technologies unless the user affirmatively opts out.[189]

Amazon's proposed legislation focuses on five guidelines: (1) facial recognition should always be used in accordance with the law, including laws that protect civil rights; (2) when facial recognition is used in law enforcement, human review is a necessary component to ensure that the use of a prediction to make a decision does not violate civil rights; (3) when facial recognition is used by law enforcement for identification or in a way that could threaten civil liberties, a 99% confidence threshold score is recommended; (4) law enforcement agencies should be transparent in how they use facial recognition technology; and (5) there should be notice when video surveillance and facial recognition technology are used together in a public or commercial setting.[190] Amazon urges that the fear of new technology should not call for an all-out ban of the technology, and that there are ways to safely and effectively implement and regulate facial recognition technology.[191] "Our communities are safer and better equipped to help in emergencies when we have the latest technology, including facial recognition technology, in our toolkit."[192] Amazon does not appear to support fully automated, final decision making even with its own technology, and it recommends that facial recognition matches be considered in the context of other evidence, rather than as the sole basis for taking action.[193]

The ACLU has criticized multi-jurisdictional police use of Amazon's Rekognition tool as posing a threat to civil liberties.[194] The criticism likely resonates in a particularly personal way with members of Congress, since this is the software that misidentified twenty-eight members of Congress

189. AWS, *Amazon Rekognition FAQs*, AMAZON WEB SERVICES, INC., (last visited Aug. 11, 2020), https://perma.cc/KVS4-EEEQ.

190. *See* Punke, *supra* note 188.

191. *Id.*

192. *Id.*

193. *Id.*

194. *See* Snow, *supra* note 138.

as people who had previously been arrested for crimes.[195] The false matches disproportionately involved members of Congress who are people of color.[196]

Supporters of facial recognition technology have also urged the adoption of regulations for continued use of the technology as an important tool for police departments.[197] Facial recognition can be a powerful means for assisting local and state police departments. In an open letter to Congress thirty-nine groups warned that "bans would keep this important tool out of the hands of law enforcement officers, making it harder for them to do their jobs efficiently, stay safe, and protect our communities."[198]

Other big tech companies have voiced concerns about the lack of regulation. Microsoft has asked governments around the world to step up and regulate facial recognition technology.[199] Facebook, on the other hand, has fought against many state bills seeking to regulate the use of biometric data.[200]

### *B. States*

Because there is no generally applicable federal law regulating the private industry's collection, storage, use, purchasing, and selling of biometric information, a handful of states have enacted state statutes governing biometric data collection. For example, Connecticut, Iowa, Nebraska, North Carolina, Oregon, Wisconsin, and Wyoming have regulated the collection of biometric information by defining "personal

---

195. *Id.*

196. *Id.*

197. *See* Melissa Hellmann, *Tech and Police Groups Urge Lawmakers To not Ban Facial-Recognition Technology*, SEATTLE TIMES (Sept. 27, 2019, 10:24 AM), https://perma.cc/SC7J-7HAD.

198. *Id.*

199. Brad Smith, *Facial Recognition: It's Time for Action*, MICROSOFT (Dec. 6, 2018), https://perma.cc/39NP-QX4S.

200. *See* Pope, *supra* note 24, at 798-99.

information" in data security breach notification laws to include some types of biometric data.[201] Illinois and Texas have implemented even further regulation of biometric data collection by creating statutes focusing solely on biometric data privacy.[202]

In 2008, Illinois became the first state to regulate biometric data.[203] Put simply, BIPA requires companies to give notice when they collect biometrics and to state what they intend to do with the information.[204] BIPA also provides that any private entity in possession of consumers' biometric information should develop and make available to the public a retention schedule and guidelines for destroying that information.[205] It further provides certain standards for storing, transmitting, and protecting the information.

BIPA has inspired other states to follow its lead, and it has also generated its fair share of litigation.[206] Since its enactment, five[207] states have followed suit with some measure of protections ranging from exclusive attorney general enforcement to causes of action only when personal information is at issue.[208] Significantly, the Illinois statute is the only one so

---

201. *See* Jason B. Binimow, *State Statutes Regulating Collection or Disclosure of Consumer Biometric or Genetic Information*, 41 A.L.R.7th Art. 4 (2019).

202. *Id.*

203. Natalie A. Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020*, NAT. L. REV. (Jan. 15, 2020), https://perma.cc/8MG8-ERQQ (noting that Illinois was the first state to regulate the collection and storage of biometric data).

204. Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. IRVINE L. REV. 107, 135 (2019).

205. 740 ILL. COMP. STAT. ANN. 14/5(a) (2008).

206. *See, e.g.*, Biminow, *supra* note 201 (discussing cases).

207. *See* Arkansas A.C.A §4-110-103(7)(E); California CAL. CIV. CODE § 1798.100 et. seq.; New York extended the SHIELD Act in N.Y. GEN. BUS. LAW § 899-bb, and also regulates biometric data in the employment context N.Y. Lab. Law §201-a; Texas TEX. BUS. & COM. CODE §503.001; and Washington WASH. REV. CODE ANN. §19.375.020.

208. Molly K. McGinley et al., *The Biometric Bandwagon Rolls On: Biometric*

far that provides for a civil claim.[209] Thus, litigation in Illinois provides the bulk of the case law currently existing on this issue.[210] There are several states with pending legislation related to facial recognition and other biometric data.

Interestingly, back in 2007 it was not the widespread use of biometric data in Illinois that moved its legislature to action. Rather, a company, Pay By Touch, was going through bankruptcy in 2007 and almost sold consumer fingerprint and financial records as an asset. The threat of such an action spurred the Illinois legislature to take action to protect its residents' personal data.[211] The legislature wished to implement protections for unknown future similar scenarios and were mostly concerned about data security.[212] The "[i]ntent of BIPA is to protect consumers from the unknown ramifications of widely adopting biometric identifiers in business transactions."[213] Technology companies and Silicon Valley lobbyists do not appear to have been involved, and perhaps they may not have even been aware of it or failed to entertain its significance at the time.

Businesses using facial recognition technology have had to be more careful in states with biometric legislation. That has sometimes meant limiting some uses and functions to states with no regulation. Thus, when Google released a feature in 2018 that matched selfies to famous works of art, it was not available in Illinois and Texas. Similarly, Google's Nest

---

*Legislation Proposed Across the United States*, NAT. L. REV. (Mar. 25, 2019), https://perma.cc/5CK5-B8FR.

209. 740 Ill. Comp. Stat. Ann. 14/20 (2008); *see also New Biometric Information Privacy Cases Reveal Breadth of Potential Exposure for Companies*, LEXOLOGY (Mar. 5, 2018), https://perma.cc/QNC6-DRH5.

210. *See*, Binimow, *supra* note 201 (reporting on the important cases interpreting BIPA including statutory requirements, damages, constitutional standing, class certification, and other issues).

211. *See*, Kugler, *supra* note 204, at 130.

212. *See*, Kugler, *supra* note 204, at 131-32.

213. 740 ILL. COMP. STAT. 14/5 (2008).

security cameras do not offer a standard feature for recognizing familiar faces in Illinois.[214]

There is little case law directly discussing facial recognition. Most of the cases that discuss biometric data have been brought under Illinois' BIPA. [215] In these cases, notice seems to be the biggest issue.[216] Courts tend to find that there is constructive notice when a reasonable person would believe that their information is being collected.[217] The courts find a violation when the user does not have notice that their information is being collected and/or shared with third parties.[218] If there is an actual violation, then the plaintiff still must establish standing to bring suit but does not need to plead actual harm under BIPA.[219]

### *C. Bans, Moratoria, & Limits*

Because of the lack of federal action, some state and local governments are implementing their own bans. These have been a particular concern when used for law enforcement. The California legislature passed a temporary ban for state and local law enforcement on the use of facial-recognition software in body cameras.[220] This bill is preemptive because currently no law enforcement agency in California uses facial-

214. *See* Hill & Krolik, *supra* note 113.

215. *See*, Binimow, *supra* note 201 (reporting on the important cases interpreting BIPA including statutory requirements, damages, constitutional standing, class certification, and other issues).

216. *See generally* McGinnis v. U.S. Cold Storage, Inc., 382 F. Supp. 3d 813 (N.D. Ill. 2019); Patel v. Facebook Inc., 290 F. Supp. 3d 948 (N.D. Cal. 2018); McCollough v. Smarte Carte, Inc., No. 16 C 03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016).

217. *See, e.g.*, Howe v. Speedway LLC, No. 17-cv-07303, 2018 WL 2445541, at *6 (N.D. Ill. May 31, 2018); Santana v. Take-Two Interactive Software, Inc., 717 Fed. App'x 12, 16 (2d Cir. 2017).

218. *See, e.g.*, Rosenbach v. Six Flags, 129 N.E.3d 1197, 1206 (Ill. 2019).

219. *See id.* at 1205.

220. *See* Rachel Metz, *California Lawmakers Ban Facial-Recognition Software from Police Body Cams*, CNN (Sept. 13, 2019), https://perma.cc/HXH7-KQT7.

recognition software in body cams. This preemptive type of legislation exemplifies the mistrust some people have with government use of facial recognition within the criminal justice system.

Local governments are going even further by taking matters into their own hands. San Francisco, for example, has banned police use of facial recognition software.[221] San Francisco became the first US city to pass a ban on the use of facial recognition by local agencies.[222] Critics of facial-recognition tools argue that they give government authorities excessive surveillance power and can perpetuate bias in policing.[223] San Diego County law enforcement has suspended the use of facial recognition software as of January 1, 2020 to comply with a new state law, A.B.1215, which creates a three-year moratorium on law enforcement use of facial recognition technology.[224] Similarly, the Seattle Police Department stopped using its facial-recognition software sometime in 2018.[225] In 2020 alone, Oakland and San Francisco, California, as well as Somerville, Massachusetts, all banned the government's use of facial recognition technology as a larger legislative package overseeing police surveillance technology.[226]

Proponents of the technology support a moratorium while the technology is further developed and understood.[227] While there may be

---

221. *Id.*

222. Kate Conger et al., *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES (May 14, 2019), https://perma.cc/KP9P-FQGA.

223. *See* Kenyon, *supra* note 6.

224. Henry Kenyon, *San Diego Country Suspends Police Facial Recognition Program*, CQ ROLL CALL (Dec. 18, 2019), https://perma.cc/R8J9-U2LV.

225. *See* Hellmann, *supra* note 197.

226. Jason Tashea, *As Facial Recognition Software Becomes More Ubiquitous, Some Governments Slam on the Brakes*, A.B.A.J. (Sept. 24, 2019), https://perma.cc/BS5C-8M6X.

227. *See* Conger, *supra* note 222; *see also Coalition Letter Calling for a Federal Moratorium on Face Recognition*, ACLU (June 3, 2019), https://perma.cc/XU6R-XC3G (providing a copy of the letter sent to Congress on behalf of sixty privacy,

agreement on the need for regulation, proponents disagree with outright bans. This view recognizes that there are useful applications of the technology, such as helping to find missing persons, including individuals with dementia who have wandered away.[228]

Accordingly, some agencies have chosen a middle ground route of closer monitoring and better limits. For instance, the Ohio Attorney General required a training program for any law enforcement officer using the state's facial recognition database, which utilizes driver's license photos, and ongoing auditing of the system (which was reviewed by a task force from September 23, 2019 through January 2020).[229] In Vermont, there is a statutory prohibition on DMV implementation of any procedures or processes for identifying applicants that involve the use of biometric identifiers.[230] As a result, in 2017, Vermont disallowed the search of its driver's license databases by facial recognition because the program was illegal under state law.[231] In Michigan, state police have a policy requiring random systems audits, which are made available to researchers.[232] The Seattle Police Department, working with the American Civil Liberties Union of Washington, developed a policy in 2016 that allowed for the technology's use, so long as it was regularly audited and was never used for real-time tracking.[233]

---

civil liberties, and other groups urging Congress to place a federal moratorium on facial recognition software until further explicit laws are developed).

228. *Id.*

229. *Id.*; *see also* OH. ATT'Y. GEN. FACIAL RECOGNITION TASK FORCE, REPORT & RECOMMENDATIONS (Jan. 26, 2020), https://perma.cc/TJ4X-984S.

230. 23 V.S.A. § 634(c) (Vt. 2019) ("The Department of Motor Vehicles shall not implement any procedures or processes for identifying applicants for licenses, learner permits, or nondriver identification cards that involve the use of biometric identifiers").

231. *See* Tashea, *supra* note 226.

232. *Id.*

233. *See* Steve Miletich, *Seattle Police Win Praise for Safeguards with Facial-Recognition Software*, SEATTLE TIMES (Oct. 18, 2016), https://perma.cc/KWV7-9TB3.

Corporate boards and shareholders have also been a source for possible internal action. For instance, Amazon received two shareholder proposals that sought to require it to perform investigations on its Rekognition technology to assess the potential negative impact on civil liberties. After Amazon attempted to exclude the proposals from its proxy materials, the SEC's Division of Corporation Finance ruled that Amazon may not rely on the economic relevance exception to exclude them.[234]

## V. REGULATING FROM THE MIDDLE

As Congress considers federal regulation of facial recognition technology it is important to be aware of and understand the way in which this technology has developed and is used in the US as well as the benefits to and concerns of the various stakeholders. Coming from that perspective, it becomes immediately apparent that a one-size-fits all approach is not likely to be effective and that the considerations ought to be nuanced and tailored. This Article focuses only on the private commercial sector, rather than the public sphere. However, knowledge of the concerns and benefits on the government uses contribute to the overall understanding, as the issues are intertwined, and the private sector supplies the technology to the government sector.

To be clear, regulating for the sake of regulating is not an ideal long-term option. This is complicated by the fact that it is often difficult to get it right. Regulations do not always achieve the desired goals, or they may fall short on doing so effectively and with efficiency.[235] In addition, even those calling for regulation or certain protections are likely to find those protections unsatisfying or even annoying. For instance, do consumers

234. *See* Nelson, *supra* note 22.

235. *See, e.g.*, Abby Jackson, *3 Big Ways No Child Left Behind Failed*, BUS. INSIDER (Mar. 25, 2015), https://perma.cc/EMV2-ABS2 (discussing how the No Child Left Behind Act's purpose of heightened school standards to hold schools accountable through measurable metrics largely failed as a result of high-stakes testing, punitive consequences for students not meeting score requirements, and hard deadlines for all states to have 100% proficiency).

actually read the hard-fought General Data Protection Regulation ("GDPR") privacy updates when they pop up on the screen, or do they simply click "consent" and move on?[236]

Even companies that favor regulation may find that regulations come with increased costs and the inevitable ambiguities in regulations make compliance difficult.[237] Concern about potential fines and litigation may also contribute to business decisions against expanding into certain geographic areas or sectors, resulting in fewer choices for some consumers.[238] Thus, effectiveness, efficiency, costs and burdens are realistic considerations for regulatory tools in this area.

What follows is a proposed framework for approaching the problem. It involves identifying common interests and common areas of concern among the various stakeholders. With those in mind, certain guided questions are suggested as an outline for the contours of any regulation. Finally, I recommend certain concrete steps toward building and approaching the substantive and procedural debate on the regulation of facial recognition technology.

### *A. Identifying Common Ground Among Stakeholders*

Companies receive tremendous benefit from facial recognition technology. Among them are more information, quicker decision making, and increased revenue.[239] The lack of federal regulations, however, raises many concerns such as how to avoid liability (for collection, storage, sharing, use, etc.) and the inefficiency of dealing with a patchwork of state legislation and court rulings.[240] Many businesses are also concerned

---

236. *See generally* Katherine M. Wilcox, Note, *"Hey Alexa, Do Consumers Really Want More Data Privacy?": An Analysis of the Negative Effects of the General Data Protection Regulation*, 85 BROOK. L. REV. 257 (2019).

237. *Id.*

238. *Id.* at 260.

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

240. *See supra* Part III.

about misuse (and potential liability for such) and compliance costs.[241] They value secrecy to protect their algorithms and also the data which is collected and stored.

Whether for allowing easy access into their phones without having to type in passcodes or opening doors in their luxury condos, consumers love and value the convenience that biometric technologies provide.[242] They are very much concerned about privacy, misuse, and civil liberties. They also would benefit from secrecy to protect their privacy, especially since biometric data, much like a social security number (except even more sensitive because it is irreplaceable) should be treated as a trade secret.[243] The patchwork of regulation offering protections in a few states is also not particularly helpful, because in some cases it may mean that certain desirable services are not offered to consumers simply because they live in a certain state.[244] China provides a cautionary tale in a direction where consumers can see expansive utilization of the technology by businesses and its potentially pervasive nature into everyday life (with or without regulations) as we look into the future.[245]

Government uses range widely from local law enforcement to border patrol, to housing.[246] The technology is a very useful tool contributing to the various agencies' effectiveness and efficiency. However, in order to continue to derive those benefits, they must be balanced against potential constitutional violations, potential abuse and misuse, poor decision making, and a need to avoid outright bans as a result of public outcry.

Areas of overlap therefore include (i) a need for regulation; (ii) a need for consistency and uniformity to address expectations, and efficiency; (iii) a need for security and secrecy or privacy; (iv) a need to bal-

241. *See supra* Part III.
242. *See supra* Part II.A.
243. *See infra* Part V.B.3.
244. *See supra* Part IV.
245. *See supra* Part II.B.
246. *See supra* Part II.A.2.

ance civil liberties and privacy concerns; and (v) a need to ensure accuracy and reliability. In light of these areas of common ground, the next section will discuss key considerations and a three-part approach to a regulatory framework for this area.

### *B. Key Considerations & Steps*

A paradigm for regulating facial recognition technology is likely to have certain basic components similar to those that have been attempted for data privacy.[247] However, there are unique concerns in this area that are best addressed with a more carefully tailored approach. Thus, the analysis in this Article raises certain guided questions as an outline for the contours of regulation: (i) should businesses be regulated, and if so, which ones? (ii) who will be the regulating agency or agencies, what will be their powers, and how much discretion and flexibility will they have? (iii) what penalties and sanctions will be imposed for misuse, abuse, and noncompliance? (iv) how will the regulated information be defined? (v) what provisions are necessary for notice and consent? (vi) what transparency about collection and handling of the information will be required? (vii) what exceptions, if any, will be made for certain types of information, certain uses or applications, or certain types groups of people? With those questions in mind, I now recommend three concrete steps toward building and approaching the substantive and procedural debate that is inevitable on this controversial topic.

#### *1. Apply a Differentiated Approach*

As a threshold matter, I do not recommend approaching the regulation of facial recognition technology or more broadly, artificial intelligence, and the regulation of biometric data, as an all-or-nothing or one-size-fits-all endeavor. Rather, each area should at least be considered and

247. *See* Peter Leonard, *Beyond Data Privacy: Data "Ownership" and Regulation of Data-Driven Business*, 16 SCITECH LAWYER 2 (Jan. 17, 2020), https://perma.cc/DKM3-EAV9.

tackled separately in order to craft a better-suited and well-tailored solution. Consider facial recognition technology separate from fingerprint technology, and biometrics separate from all artificial intelligence as a wider subset. Perhaps separate civil issues from criminal justice concerns while noting overlaps and possible "cross contamination." For instance, how does one use facial recognition technology to maintain security at a sporting event?[248] Consider addressing issues related to specific markets (e.g., healthcare[249]), discrete business applications and uses, or categories of people (such as minors) separately.

The EU has taken a similar approach where it has experienced analogous problems in this area. Indeed, the EU is ahead of the US[250] in attempting to implement regulation over facial recognition software. As in the US, there is a sharp divide on views over the technology. There were proposals to curb or ban some uses of automated surveillance tools, including facial recognition software, in order to proactively address risky applications of artificial intelligence. The result was a compromise regulating such algorithms, only in mass surveillance.[251] Thus, one option for the US is to follow the EU's lead and first implement regulations over areas of greatest concern (e.g., mass surveillance or real time identification by government agencies).[252]

---

248. *See* John Wagner Givens & Debra Lam, *Smarter Cities or Big Brother? How the Race for Smart Cities Could Determine the Future of China, Democracy, and Privacy*, 47 FORDHAM URB. L.J. 829, 875-76 (2020) (discussing how in Europe compliance with the GDPR is met when names from a watchlist are entered into a facial recognition system only on game day "and is deleted at the end of the day," the data is isolated from the internet, "and a cross-check is used to avoid false positives").

249. *See* Savannah G. Stewart, Recent Development, *Privacy - When Is an Individual's Biometric Data Protected?*, 43 AM. J. TRIAL ADVOC. 269 (2019).

250. *See* Parmy Olson & Sam Schechner, *AI, Surveillance Tools Scrutinized by European Regulators*, WALL ST. J. (June 26, 2019), https://perma.cc/QU74-X873.

251. *Id.*

252. *Id.*

Reflecting the challenges of coming up with one set of universal rules, there were strong divisions within the EU's panel on the question of how—and whether—to apply government regulations to the development and implementation of artificial intelligence.[253] One camp, including groups and researchers that investigate problems like biases baked into algorithms, argued that the EU should regulate all uses of artificial intelligence because of the fast progress in the field and the potential dangers the technology could pose.[254]

### 2. *Provide Precise and Practical Rules for SUCS*

Regulations should consider and provide specific guidance on each of the key components of facial recognition technology. These areas are storage, use, collection, and sharing ("SUCS"). Ultimately, these four areas underlie the scope of concern for all stakeholders: developers of the technologies, business users, and consumers (including private individuals, business to business, and government users).

As part of the overall scheme, it will be important to reduce or minimize compliance costs for businesses in order to encourage widespread adoption of specified practices. Companies often fear regulation because in practice, the costs may appear to outweigh any benefits.[255] Thus, properly crafted and incentivized, the cost of non-compliance should be higher than the cost of compliance in regulating this technology.[256]

---

253 . *See, e.g.*, OECD, ARTIFICIAL INTELLIGENCE IN SOCIETY (2019), https://perma.cc/KN99-8W3Z; EUROPEAN PARLIAMENTARY RESEARCH SERVICE, THE ETHICS OF ARTIFICIAL INTELLIGENCE: ISSUES AND INITIATIVES (Mar. 2020), https://perma.cc/2M3V-N32T.

254. *See* Olson & Schechner, *supra* note 250.

255. *See, e.g.*, Wilcox, *supra* note 236, at 272-74.

256. *See* PONEMON INSTITUTE LLC, THE TRUE COST OF COMPLIANCE WITH DATA PROTECTION REGULATIONS (Dec. 2017), https://perma.cc/755W-ZYE4 (finding that with respect to some regulations like HIPPA and the GDRP, the cost of noncompliance was about three times higher than the cost of compliance for sampled multinational corporations).

Moreover, to further support compliance, it will be necessary to have clarity on what compliance looks like for day to day interaction with employees, consumers, and business partners. For instance, what written policies should cover the storage, use, and collection of the relevant biometric data? What written notice or consent is required and in what form? What security measures will be necessary and sufficient to protect the data and to prevent disclosure?

Finally, it bears repeating here that effective regulation in this area cannot be divorced from the key concerns that have been identified in this Article.[257] Thus, collection and privacy concerns must be carefully considered. Fears about accuracy of the technology may, for instance, be addressed through an industry standard certification or independent testing and verification. Related to accuracy concerns are the race and gender disparities and to overall issues with algorithmic equity and fairness in the marketplace.[258] Religious objections illustrate the need for a broader mindfulness of constitutional protections even in a non-governmental context and especially in employment settings.[259] The security interests in storage and use, along with the need to be proactive in preventing misuse, are paramount, and one possible approach to addressing those concerns, trade secrecy, is introduced below.

### *3. Consider Trade Secrecy as a Framework to the SUCS Problem*

A point of reference to an existing area of law that could be especially instructive as a security framework for storage, use, collection, and sharing is trade secret law. To begin, all stakeholders share an interest in pro-

257. *See supra* Part III.

258. *See supra* Part III.C.

259. *See supra* Part III.D.

tecting the information (or may be faced with a duty to do so by regulation), and the value of the information to each could be evaluated in terms of the value requirement from trade secrecy.[260]

Moreover, the reasonable efforts requirement[261] in trade secrecy could serve as the standard for determining the level of care required for storage and security. Relatedly, the need for particular care and assurances when sharing confidential information in order to guard against improper disclosure could be applicable to consumers (who should be careful about providing their biometric data without proper assurances of confidentiality) and to developers and businesses alike. Thus, companies that collect and store this data could be required to or may voluntarily assume the responsibility of both using reasonable efforts to secure the data and for any contracts with third parties that provide for sharing or using that information.

Further, to the extent companies (and consumers) utilizing these technologies for private business uses may wish to prevent the information from being provided to the government, trade secrecy also provides an appropriate framework within which to do so.[262] Finally, a possible liability framework for misuse of biometric data could be trade secret misappropriation,[263] where, for instance, the level of knowledge to trigger liability could be borrowed.

To be sure, I am not suggesting that a trade secrecy framework in its entirety may be an ideal fit given all of the articulated concerns and the possible applications of facial recognition technology and other biometric data. In some contexts, especially in the criminal justice system, where

---

260. *See* ELIZABETH A. ROWE & SHARON K. SANDEEN, TRADE SECRET LAW: CASES AND MATERIALS 139-40 (West Acad., 2nd ed. 2017).

261. *Id.* at 187.

262. *See* Elizabeth A. Rowe, *Striking a Balance: When Should Trade-Secret Law Shield Disclosures to the Government?*, 96 IOWA L. REV. 791 (2011).

263. 18 U.S.C. § 1836(b) (providing for civil causes of action for trade secret misappropriation).

transparency and constitutional concerns may be paramount, very careful consideration should be given to balancing concerns and the public interest.[264] Indeed, regulation in this area may merit reconceptualizing who the "public" is and what "they" want.[265] Where, as here, there are different stakeholders with different interests, the public is not monolithic. Perhaps its or their interests ought to be considered in a more nuanced and robust fashion than is traditionally done.

## VI. CONCLUSION

As Congress considers federal regulation of facial recognition technology, it is important to be aware of and better understand the ways in which this technology is used in the US, especially in the private sector, as well as the benefits to and concerns of the various stakeholders. From that perspective, it becomes immediately apparent that a one-size-fits-all approach is not likely to be effective and that the considerations for deciding whether or not to regulate and how to do so ought to be nuanced and tailored. In that vein, this Article endeavored to identify common interests and common areas of concern among the various stakeholders, including developers of the technologies, business users, and consumers (broadly conceptualized as private individuals, business to business, and government users). It identified needs in the following areas of overlap

---

264. *See, e.g.*, Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103, 171 (2018) ("Perhaps most notably and controversially, certain data will be excluded, in spite of its potential predictive value, for a variety of policy reasons. . . . Immutable characteristics such as race and gender are constitutionally problematic; . . . ."); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1359-60 (2018); State v. Loomis, 881 N.W.2d 749, 770-71 (Wis. 2016) (rejecting defendant's challenge for algorithm disclosure and finding no due process violation).

265. *See generally supra* Part III; *see also* Brauneis & Goodman, *supra* note 264, at 109; Cary Coglianese & David Lehr, *Transparency and Algorithmic Governance*, 71 ADMIN. L. REV. 1 (2019).

(i) a need for regulation; (ii) a need for consistency and uniformity to address expectations, and efficiency; (iii) a need for security, secrecy or privacy; (iv) a need to balance civil liberties and privacy concerns; and (v) a need to ensure accuracy and reliability. With those in mind, it posed certain guided questions to outline the contours of any regulation. Finally, it recommended three concrete and carefully tailored steps toward designing regulation of facial recognition technology. They included applying a differentiated approach to regulating in this area, providing precise and practical guidance for companies to navigate storage, use, collection, and sharing of biometric data, and considering trade secrecy as one potential reference point from which to address the standards necessary to addressing each of these key components.