# FACE VALUE: A PROPOSAL FOR FEDERAL REGULATION OF FACIAL RECOGNITION TECHNOLOGY COMPANIES

Hope Corbit*

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and . . . to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is.[1]

## *I. INTRODUCTION*

The COVID-19 pandemic drastically changed the American way of life when a nationwide shutdown in 2020 forced businesses to close and left millions of Americans jobless.[2] State unemployment claims skyrocketed and caused unemployment agencies to scramble to manage the influx of claims.[3] Many agencies implemented facial recognition technology ("FRT") to assist in verifying citizens' identities, a decision that may have deprived thousands of Americans of timely benefits due to issues with the technology's performance.[4] And for the individuals who

 J.D. Candidate, Stetson University College of Law, May 2023; B.S. in Music, cum laude, University of Colorado Denver, 2008. Local Government Editor, *Stetson Law Review*, 2022–23. Thank you to my writing advisor, Professor Roy Balleste, and my Notes & Comments Editor, Sasha Ledney, for their feedback throughout the writing of this Article. Many thanks as well to Articles & Symposia Editor, Elizabeth Alderson, and to all the Editors and Associates of *Stetson Law Review*, for their hard work in preparing this Article for publication. Finally, a special thanks to my husband, Kris, and my son, Tyler, for their unending support and encouragement of this Article—and all of my endeavors.

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195–97 (1890).

2. Sean M. Smith, Roxanna Edwards & Hao C. Duong, *Unemployment Rises in 2020, as the Country Battles the COVID-19 Pandemic*, MONTHLY LAB. REV., U.S. BUREAU OF LAB. STATS. (June 2021), https://doi.org/10.21916/mlr.2021.12.

3. Shawn Donnan & Dina Bass, *Cybersecurity Company ID.me Is Becoming Government's Digital Gatekeeper*, BLOOMBERG BUSINESSWEEK (Jan. 28, 2022, 1:03 PM), https://www.bloomberg.com/news/features/2022-01-20/cybersecurity-company-id-me-is-becoming-government-s-digital-gatekeeper.

4. *Id.*

successfully accessed the system, their unique biometric information—accompanied by personal government documents—is now stored at the mercy of a largely unregulated company at the requirement of a government agency.[5]

Certainly, many Americans benefit daily from FRT when using the technology to unlock mobile phones and laptops, approve payments through smartphone apps, or gain access to systems through a multifactor authentication process.[6] Indeed, FRT use is undoubtedly a valuable tool for most Americans.[7] So why should anyone question the need to upload a selfie to access government benefits? What could go wrong? The government touts fraud prevention, national security, and enforcing immigration to support its use of FRT.[8] But allowing third-party companies to collect biometric data on behalf of the government poses a great risk to American citizens if a company's collection and storage practices are not properly regulated.[9]

Americans should not have to worry that their biometric data has been collected without their knowledge and placed in danger of third-party exploitation, but because Congress' efforts have failed in passing a federal biometrics protection act, the protection of an individual's biometric data is only as good as the laws of the state in which they live.[10] To be sure, large-scale data breaches are increasingly common and have left Americans asking when—not

5. *See Consent for ID.me to Collect Biometric Data*, HELP CENTER, ID.ME https://www.id.me/biometric#:~:text=How%20Long%20Does%20ID.me,retained%20in%20line%20with%20ID (last visited Feb. 9, 2023) [hereinafter *ID.me Biometric Retention*].

6. *See Mobile Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/; Nguyen et al., *Master Face Attacks on Face Recognition Systems*, 4 IEEE TRANSACTIONS ON BIOMETRICS, BEHAV., & IDENTITY SCI. 398, 398 (2022).

7. Nguyen et al., *supra* note 6.

8. Paresh Dave & Jeffrey Dastin, *Spending to Fight U.S. Unemployment Fraud Brings Boost, Scrutiny to Alphabet-Funded ID.me*, REUTERS (July 22, 2021, 6:00 PM), https://www.reuters.com/world/the-great-reboot/spending-fight-us-unemployment-fraud-brings-boost-scrutiny-alphabet-funded-idme-2021-07-22/; U.S. GOV'T ACCOUNTABILITY OFF., GAO-21–526, FACIAL RECOGNITION TECHNOLOGY: CURRENT AND PLANNED USES BY FEDERAL AGENCIES (2021) [hereinafter AUGUST 2021 GAO REPORT].

9. Jake Laperruque, *Preserving the Right to Obscurity in the Age of Facial Recognition*, THE CENTURY FOUND. (Oct. 20, 2017), https://tcf.org/content/report/preserving-right-obscurity-age-facial-recognition/?agreed=1.

10. James A. Lewis & William Crumpler, *Report: Facial Recognition Technology Responsible Use Principles and the Legislative Landscape*, CTR. FOR STRATEGIC & INT'L STUD. (Sept. 29, 2021), https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape.

if—our biometric data will be exposed.[11] Thus, a solution requires a restructuring of the role federal agencies play concerning biometric information.

FRT, including a form of biometric information known as "face mapping," and the methods commercial FRT companies like Clearview AI ("Clearview"), ID.me, and the former Facebook—Meta Platforms, Inc. ("Meta")—employ to handle biometric data, have evaded federal regulation due to Congress' inability to agree on legislation.[12] Meanwhile, within the last year Canada, the United Kingdom, Australia, and France have all found Clearview in breach of various privacy and data collection laws, and have issued fines and/or ordered the FRT company to terminate its image collection practices.[13] Despite the international denunciation, in the United States, federal and state agencies, local law enforcement, and the military continue to use Clearview's services.[14]

Likewise, many government agencies continue to require citizens to use ID.me, though recent public outcry has led to some rejection of the federal government's use of the identity verification platform.[15] Still, the lack of federal regulation has left the crucial protection of citizens' most sensitive data to the states.[16] Commercial FRT companies can store, mishandle, or sell someone's biometric data, and the individual's recourse is limited to their state privacy laws.[17] Further, when a government agency

11. Bree Fowler, *Data Breaches Break Record in 2021*, CNET (Jan. 24, 2022, 8:47 AM), https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/.

12. Palash Basu & Jenny Holmes, *Facial Recognition Systems Regulation: Outlook for 2022*, BLOOMBERG L. (Dec. 23, 2021, 4:00 AM), https://www.bloomberglaw.com/product/privacy/bloomberglawnews/privacy-and-data-security/BNA%200000017dc401d949affdfe6fa7d00000? (detailing multiple proposals regulating FRT technology).

13. *Id.*

14. AUGUST 2021 GAO REPORT, *supra* note 8, at 20.

15. Alan Rappeport & Kashmir Hill, *I.R.S. to End Use of Facial Recognition for Identity Verification*, N.Y. TIMES (Feb. 7, 2022), https://www.nytimes.com/2022/02/07/us/politics/irs-idme-facial-recognition.html. Many ID.me users for other governmental services were frustrated by technical issues with the platform that resulted in an inability to access services. *Id.* Additionally, lawmakers and citizens were concerned about the company's handling and storage of biometric data. *Id.*

16. Matthew R. Lowe, *All Eyes on U.S.: Regulating the Use & Development of Facial Recognition Technology*, 48 RUTGERS COMPUT. & TECH. L.J. 1, 14 (2021).

17. Thorin Klosowski, *The State of Consumer Data Privacy Laws in the U.S. (And Why It Matters)*, N.Y. TIMES: WIRECUTTER (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

requires an individual in need of governmental services to submit biometric data to a third-party commercial company for authentication purposes, it essentially creates a "forced consent" to the third party's biometric handling policies.[18] Nonetheless, the use of biometric data is vital to the world in which we operate.[19] Without federal regulation, the litany of litigation in various state courts could result in massive setbacks for companies on which we rely to further technology.[20]

FRT has a place in our modern technological society. However, a line must be drawn to define acceptable circumstances and the amount of control various parties have over such sensitive personal information. Part II of this Article examines the benefits of FRT use in the United States as well as the potential frightening consequences for American citizens that could result from the mishandling of FRT. Part III of the Article focuses on United States commercial FRT companies Clearview AI and ID.me and the increased governmental use of the commercial FRT companies. Part IV explains the current state and federal laws and regulations on biometric data, including state biometric protection and privacy laws and the Federal Trade Commission's ("FTC's") role in enforcing federal privacy regulations. Finally, Part V recommends a detailed draft of federal legislation that creates a national biometric safety board to ensure the handling and security of an individual's biometric information so Americans may continue to benefit from technological advances, particularly in the field of biometric technology.

## *II. REASONS TO LOVE AND FEAR FACIAL RECOGNITION TECHNOLOGY USE IN THE UNITED STATES*

American society unquestionably benefits from the multitude of conveniences and protections that FRT affords. Indeed, Americans have embraced the use of FRT, and the boundless opportunities presented by the technology. Nevertheless, ramifications of potential misuse or mishandling of FRT could

18. Donnan & Bass, *supra* note 3.

19. Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. IRVINE L. REV. 107, 114–15 (2019).

20. Taylor Hatmaker, *Facebook Will Pay $650 Million to Settle Class Action Suit Centered on Illinois Privacy Law*, TECHCRUNCH (Mar. 1, 2021, 4:36 PM), https://techcrunch.com/2021/03/01/facebook-illinois-class-action-bipa/.

result in dire consequences for Americans—both individually and societally.

### A. The Benefits of Facial Recognition Technology

As technology and the internet have grown, so have the societal expectations of an elevated level of convenience—particularly in the United States.[21] Modern technological advances have certainly provided many Americans luxuries that previously would have seemed impossible.[22] Yet, some of these modern comforts have left citizens vulnerable to dangers ranging from fraud to geo-political attacks, and numerous businesses in both the public and private sectors have turned to FRT to combat these dangers.[23]

#### *1. Fraud Protection and Physical Security*

The pervasiveness of identity theft in the United States has resulted in the desensitization of many Americans to the common need for fraud avoidance.[24] Identity theft may result when bad actors employ innovative methods to trick unknowing victims into granting the actor digital access to the victim's sensitive personal information in hopes that it will result in a big payday.[25] One way businesses combat such theft is through multi-factor authentication ("MFA") which utilizes FRT to secure a user's personal information.[26] MFA requires a user to complete multiple steps to access their account and bars entry to the account if one

21. *Mobile Fact Sheet*, *supra* note 6 (stating that when polled on Feb. 8, 2021, 77% of adults polled owned a laptop and 53% of adults polled owned a tablet).

22. *Id.* (pointing out that 15% of adults polled only access the internet through a smartphone, even though 96% polled between ages 18 and 29 and 95% in the age group of 40 through 59 owned a smartphone).

23. Jason C. Gavejian et al., *Jump in Facial and Voice Recognition Raises Privacy, Cybersecurity, Civil Liberty Concerns*, NAT'L L. REV., Feb. 3, 2022, https://www.natlawreview.com/article/jump-facial-and-voice-recognition-raises-privacy-cybersecurity-civil-liberty#:~:text=The%20majority%20of%20states%20are%20using%20facial%20recognition,persons%20eligible%20for%20government%20benefits%20to%20prevent%20fraud.

24. Shanice Jones, *2022 Identity Theft Statistics*, CONSUMER AFFS. (May 6, 2022), https://www.consumeraffairs.com/finance/identity-theft-statistics.html.

25. *Scams and Frauds*, USA.GOV, https://www.usa.gov/scams-and-frauds (last visited Feb. 9, 2023).

26. *Multi-Factor Authentication*, CISA (Jan. 2022), https://www.cisa.gov/sites/default/files/publications/MFA-Fact-Sheet-Jan22-508.pdf.

step of the process fails—even if the correct login information is presented.[27]

Still, fraud prevention through FRT is not limited to digital access security.[28] Companies also use FRT in physical locations to authorize entry into classified areas, monitor visitors, verify employees, and identify customers to ensure the physical security of establishments.[29] Clearly, utilizing FRT to aid in fraud prevention plays an essential role in modern society that must not be overlooked in the attempt to regulate FRT use.

### *2. National Defense and Travel Protections*

On a broader scale, FRT also assists federal agencies and the United States military in strengthening national defense.[30] For example, federal agencies use FRT to identify terrorists attempting to enter the country by comparing photos on travel documents against a searchable database containing pictures of known or suspected terrorists.[31] Further, the United States Army recently sought to deploy an FRT program that would be installed at army base security checkpoints.[32] The camera-based technology would recognize a driver upon approach of the checkpoint, analyze a database of authorized base visitors, and notify the checkpoint guard to grant or deny the driver access to the base.[33] The real-time analysis of the system is particularly beneficial because it would allow heightened security without slowing down the efficiency of entrance to the base.[34]

United States airports provide another advantageous area for FRT usage—particularly with the recent emergence of two new

27. *Id.*

28. *Facial Recognition: Potential and Risk*, SENATE RPC (Nov. 20, 2019), https://www.rpc.senate.gov/policy-papers/facial-recognition-potential-and-risk.

29. *Id.*

30. AUGUST 2021 GAO REPORT, *supra* note 8, at 14. The report noted that the Department of Homeland Security, Department of Defense, Department of Justice, and the Department of State all utilize FRT as a matter of national defense. *Id.* For example, FRT searches performed compare visa and passport photos against terrorism watchlist photos. *Id.*

31. *Id.*

32. Stephen Silver, *U.S. Army Seeks Facial Recognition Technology for Bases*, NAT'L INT. (Apr. 5, 2021), https://nationalinterest.org/blog/buzz/us-army-seeks-facial-recognition-technology-bases-182041.

33. *Id.*

34. Aaron Boyd, *U.S. Army Wants Face Recognition at Base Gates*, DEF. ONE (Apr. 5, 2021), https://www.defenseone.com/technology/2021/04/army-wants-automate-base-access-facial-recognition-drive-thru-checkpoints/173122/.

FRT programs aimed to ensure safe and efficient travel in the United States.[35] The Transportation Security Administration ("TSA") recently piloted a passenger verification program that employs FRT to identify travelers at security checkpoints throughout the airport.[36] The program allows a traveler to insert their government-issued photo ID into a kiosk that first snaps the traveler's photo and then compares it to the traveler's ID.[37] Potentially, the program has the ability to make travel more efficient while granting TSA agents the freedom to focus on more intensive passenger verification.[38]

Similarly, the Miami International Airport announced the implementation of a new face biometric boarding program that is slated to be fully operational in 2023.[39] Upon arrival at the passenger's gate, the boarding program technology takes a picture of the passenger that is then analyzed with FRT to verify the passenger's identification, and upon verification, the passenger is allowed to board the airplane.[40] The program aims to increase a traveler's speed and convenience of navigating the airport.[41] Airports' increased use of FRT undoubtedly benefits travelers tremendously and should continue to enhance the commercial air travel experience in the coming years.[42]

### B. Ramifications of the Misuse or Mishandling of Facial Recognition Technology

While FRT benefits are exponential, so are the risks that accompany the many advantages it affords. Ironically, the same technology touted to prevent identity theft and fraud could

35. *See TSA Launches Cutting-Edge Passenger Identification Technology at LAX Security Checkpoints*, TRANSP. SEC. ADMIN. (Mar. 18, 2022), https://www.tsa.gov/news/press/releases/2022/03/18/tsa-launches-cutting-edge-passenger-identification-technology-lax [hereinafter *2022 TSA Press Release*]; Tyler Choi, *Miami International Airport Plans for Biometric Boarding at all Gates by 2023*, BIOMETRIC UPDATE (May 17, 2022, 6:07 PM), https://www.biometricupdate.com/202205/miami-international-airport-plans-for-biometric-boarding-at-all-gates-by-2023.

36. *2022 TSA Press Release*, *supra* note 35.

37. *Id.* The new TSA program utilizes Credential Authentication Technology ("CAT") to decrease the need for physical contact between travelers and TSA agents as well as eliminate the need for physical documents. *Id.*

38. *Id.*

39. Choi, *supra* note 35.

40. *Id.*

41. *Id.*

42. *Id.*

potentially aid sophisticated bad actors in stealing an individual's faceprint, leaving the individual with little option to remedy.[43]

### *1. Identity Theft*

A recent study revealed an alarming new method employed by bad actors to outwit biometric authentication systems and unlock personal devices to gain access to an individual's personal information—presentation attacks.[44] Deep faking is a form of presentation attack that involves the creation of a "master face," a biometric sample that an actor may construct using a standard computer and resources found on the internet—all without obtaining any personal information about the target.[45] When the actor presents the "master face," in the form of a printed photo or replayed video, to the targeted facial recognition system, the actor interferes with the system on a sublevel and essentially tricks the system's face-mapping function to deliver a false match of the "master face" with multiple faces in the system's database.[46] Frightening implications abound once a bad actor gains entry to an individual's devices and sensitive information through this form of deep fake technology—particularly the actor's ability to potentially impersonate the individual.[47]

### *2. Stolen Biometrics Could Lead to Permanent Identity Theft*

Arguably the greatest pitfall in the normalization of using FRT as a form of access to sensitive personal information is the lack of remedy once an individual's biometric faceprint is stolen.[48] A person can change a password or even their social security number, but it is extremely difficult to change biometric features—

43. *See* Donnan & Bass, *supra* note 3. Prospective data breaches of content containing faceprints could lead to a bad actor stealing a victim's identity and denying the victim access to their own information. *Id.*

44. Nguyen et al., *supra* note 6. The study particularly warns of the security risk involving vulnerable algorithms used to unlock smartphones. *Id.*

45. *Id.*

46. *Id.* at 400–01.

47. Ensar Seker, *Deepfake to Bypass Facial Recognition by Using Generative Adversarial Networks (GANs)*, TOWARDS DATA SCI. (May 17, 2020), https://towardsdatascience.com/deepfake-to-bypass-facial-recognition-by-using-generative-adversarial-networks-gans-37a8194a87b1; *Identity Theft*, USA.GOV, https://www.usa.gov/identity-theft (last visited Feb. 9, 2023).

48. Kugler, *supra* note 19, at 132.

particularly a face.[49] At the height of the COVID-19 pandemic, Erica Worthy attempted to apply online for a job with a commercial airline.[50] As part of the application, Worthy followed a link to the ID.me website where she was prompted to upload documents and take a selfie to verify her information.[51] Unfortunately for Worthy, the job posting was a sham, and she had actually given bad actors her biometric information, which was then used by the actors to file a fraudulent state unemployment claim in California.[52] To make matters worse, the suspicious California filing was flagged as potentially fraudulent and triggered a hold on Worthy's actual unemployment benefits that she was receiving in Florida.[53] Worthy's experience is not only a cautionary tale regarding the dangers of online fraud, but also a stark reminder of the inherent sensitivity of an individual's biometric data. And while Worthy may have ultimately proven her identity in the case of her Florida unemployment benefits, some bad actors—somewhere—likely still have her faceprint and sensitive information that may be used to impersonate her again.[54] And there is nothing she can do about it.[55]

## *III. GOVERNMENTAL USE OF COMMERCIAL FACIAL RECOGNITION TECHNOLOGY COMPANIES*

Given the prevalence of governmental use of FRT, many government agencies have relied on commercial FRT companies for various applications. Still, government outsourcing to commercial FRT companies is problematic when government agencies require citizens to use the technology in order to access

49. *Id.* "Essentially, biometrics are the equivalent of a PIN that is impossible to change. The theft of biometric information amounts to permanent identity theft, and thus may be extremely difficult to counteract." *Id.* (quoting Steven C. Bennett, *Privacy Implications of Biometrics*, 53 PRAC. LAW. 13, 16–17 (2007)).

50. Donnan & Bass, *supra* note 3.

51. *Id.*

52. *Id.*

53. *Id.*

54. *Id.*

55. Grant Gross, *Regulation of Facial Recognition May Be Needed, US Senator Says*, CSO ONLINE (July 18, 2012, 7:00 AM), https://www.csoonline.com/article/2131974/regulation-of-facial-recognition-may-be-needed--us-senator-says.html; *see also* Donald L. Buresh, *Should Personal Information and Biometric Data Be Protected Under a Comprehensive Federal Privacy Statute That Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?*, 38 SANTA CLARA HIGH TECH. L.J. 39, 55–56 (2022) (detailing the harms of violating biometric privacy).

government services. Further, such a requirement is particularly alarming when commercial FRT companies' biometric storage and handling practices are not subject to government regulation.

### A. Commercial Facial Recognition Technology Companies

The increased demand for FRT—driven by the societal benefits afforded by the technology—led to the emergence of numerous commercial FRT companies in the last ten to fifteen years. Indeed, some FRT companies have become well-known while others quietly lurk in the background. Clearview AI and ID.me are examples of commercial FRT companies whose practices have proven to be of particular interest in the national conversation concerning FRT.

#### *1. Clearview AI*

Over the last couple of years, Clearview has undeniably emerged as a leading force in the FRT industry. Through its searchable database of images, Clearview technology aided police in identifying and arresting protesters during the Black Lives Matter movement as well as identified rioters in the January 6th United States Capitol Riots.[56] And when Russia invaded Ukraine in early 2022, Clearview gave Ukraine's defense ministry access to its FRT database; presumably to identify dead or wounded soldiers and reunite Ukrainian refugees with their families.[57] However, Clearview AI should now be a household name, if for no other reason than its goal of making every person in the world identifiable by expanding its database to 100 billion photos.[58]

Clearview's ambition of obtaining approximately fourteen pictures per person across the globe certainly reflects the hubris engrained in the company and its practices.[59] Clearview built its

56. Jon Brodkin, *Clearview AI Aims to Put Almost Every Human in Facial Recognition Database*, ARS TECHNICA (Feb. 16, 2022, 5:00 PM), https://arstechnica.com/tech-policy/2022/02/clearview-ai-aims-to-put-almost-every-human-in-facial-recognition-database/.

57. Paresh Dave & Jeffrey Dastin, *Exclusive: Ukraine Has Started Using Clearview AI's Facial Recognition During War*, REUTERS (Mar. 14, 2022, 5:12 PM), https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/.

58. Brodkin, *supra* note 56.

59. Drew Harwell, *Facial Recognition Firm Clearview AI Tells Investors It's Seeking Massive Expansion Beyond Law Enforcement*, WASH. POST (Feb. 16, 2022, 12:47 PM),

current database of over 20 billion pictures[60] by "scraping" photos from the internet, particularly from Google and other heavily frequented sites like Facebook, YouTube, and Venmo.[61] Initially, Clearview focused its services on law enforcement and federal agencies to assist in generating leads, identifying persons of interest, and accelerating investigations.[62] But the government's prevalent use of Clearview's technology has been publicly scrutinized by many over Clearview's controversial image collection methods that do not allow individuals to consent to the use of their photos.[63]

Despite the noise surrounding Clearview, the United States government shows no sign of slowing Clearview's momentum, particularly with the United States Patent and Trademark Office recently approving Clearview's patent for its "search engine for faces."[64] Further, a recent National Institute of Standards and Technology ("NIST") draft of ongoing face recognition vendor tests assessed the accuracy and speed in which an FRT algorithm positively matches an unknown individual by comparing the individual's photo to a vast database containing over 30 million pictures.[65] Notably, the November 2021 NIST draft not only found Clearview's algorithm effective but also placed it among the top United States biometric providers.[66]

Most recently, Clearview expanded its services to include "consent-based facial recognition identity and verification

---

https://www.washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition/.

60. *Mobile*, CLEARVIEW AI, https://www.clearview.ai/mobile (last visited Feb. 9, 2023). "Clearview AI's 30+ Billion Image Database Built from Open Source Intelligence (OSINT)." *Id.*

61. Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Nov. 2, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

62. *Law Enforcement*, CLEARVIEW AI, https://www.clearview.ai/law-enforcement (last visited Feb. 9, 2023).

63. Alexandra S. Levine, *Clearview AI on Track to Win U.S. Patent for Facial Recognition Technology*, POLITICO (Dec. 4, 2021, 9:00 AM), https://www.politico.com/news/2021/12/04/clearview-ai-facial-recognition-523735.

64. *Id.*

65. Patrick Grother et al., *Face Recognition Vendor Test (FRVT) Part 2: Identification*, NIST (Dec. 18, 2022), https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf (working draft supplement) (because NIST conducts ongoing FRVT testing and releases reports every four months, there is no finalized version of this report). The NIST photo database contains mugshots, profile shots, webcam stills, and candid or "in the wild" photos. *Id.* at 19.

66. Chris Burt, *Clearview Joins Leaders in NIST Face Biometrics Accuracy Testing*, BIOMETRIC UPDATE (Nov. 24, 2021, 6:31 PM), https://www.biometricupdate.com/202111/clearview-joins-leaders-in-nist-face-biometrics-accuracy-testing.

applications."[67] Rather than accessing Clearview's existing massive database, the new service matches photos uploaded—with the individual's consent—to authenticate a visitor's identity in a physical or digital space.[68] The move undoubtedly aims to strengthen Clearview's grip on the FRT space with hopes of also improving its reputation.[69]

### *2. ID.me*

Public scrutiny of the government's use of commercial FRT companies has not been limited to Clearview. Numerous federal and state agencies have mandated the use of the identification verification service ID.me to access individuals' claims, subsequently igniting a firestorm around the company, whose services are aimed at fraud prevention.[70] At least thirty state agencies—along with multiple federal agencies—currently employ ID.me to verify the identity of over 70 million Americans attempting to access government services.[71] However, the company came under fire during the COVID-19 pandemic when many state unemployment agencies required citizens filing unemployment claims to use the application.[72]

Indeed, the overwhelming need for state unemployment agencies to allow their citizens to securely file unemployment claims and access benefits online massively affected the growth of

67. *Commercial*, CLEARVIEW AI, https://www.clearview.ai/commercial (last visited Feb. 9, 2023).

68. Ben Wodecki, *Clearview AI to Offer 'Consent-Based' Facial Recognition After Privacy Controversy*, AI BUS. (Apr. 8, 2022), https://aibusiness.com/document.asp?doc_id=776668. Clearview specifically targeted gig companies like Airbnb and Uber, but those companies denied any interest in using Clearview's services. *Id.*; *see also* Paresh Dave, *Clearview AI's Facial Recognition Tool Coming to Apps, Schools*, REUTERS (May 24, 2022, 3:53 PM), https://www.reuters.com/technology/clearview-ais-facial-recognition-tool-coming-apps-schools-2022-05-24/; *infra* pt. III.B (discussing new restrictions placed on Clearview prohibiting the company from selling access to its database to private businesses or entities).

69. Wodecki, *supra* note 68.

70. Rachel Metz, *After Face-Recognition Backlash, ID.me Says Government Agencies Will Get More Verification Options*, CNN BUS. (Feb. 9, 2022, 3:11 PM), https://www.cnn.com/2022/02/08/tech/idme-facial-recognition-bypass/index.html.

71. *About Us*, ID.ME, https://www.id.me/about (last visited Feb. 9, 2023); Michele Estrin Gilman, *Me, Myself, and My Digital Double: Extending Sara Greene's Stealing (Identity) from the Poor to the Challenges of Identity Verification*, 106 MINN. L. REV. HEADNOTES 301, 316–17 (2022); *see Individuals*, ID.ME, https://www.id.me/individuals/government (last visited Feb, 12 2023)*; see also Register and Apply for Unemployment Insurance*, EMP. DEV. DEP'T, ST. OF CAL., https://edd.ca.gov/en/Unemployment/apply (last visited Mar. 9. 2023).

72. Donnan & Bass, *supra* note 3.

ID.me and thrust the company into the national spotlight.[73] ID.me's process was meant to be simple, only requiring a claimant to upload a selfie, state-issued driver's license, and other relevant necessary government documents.[74] The user's selfie would then be compared to the driver's license photo to verify the individual's identity.[75] Nevertheless, many Americans struggled with the technology, complaining of numerous failed attempts to access their accounts while their requests for help from ID.me's customer support personnel, named "trusted referees," went unanswered for days and sometimes weeks.[76] In some instances when facial recognition failed to identify a user, the user had to wait for hours to receive verification of their identification via video chat.[77] Other issues arose when the platform denied access to transgender users whose gender did not match on certain documents.[78] Many user accounts were mistakenly flagged as fraudulent and put on hold for weeks, thus resulting in the withholding of desperately needed benefits.[79] Still, ID.me appears to be unfazed by the controversy and continues to add new services for both the public and private sectors.[80]

### B. Problems Associated with Government Outsourcing to Commercial FRT Companies

Governmental use of FRT, particularly faceprints obtained by commercial companies, has been and will continue to be a hotly debated topic in the United States.[81] Government exploitation of

---

73. *Id.* The first state unemployment contract for ID.me came at the onset of the COVID-19 pandemic, and within a little over a year, ID.me had contracts with twenty-seven state unemployment agencies. *Id.*

74. *Individuals*, *supra* note 71.

75. Dina Bass & Shawn Donnan, *California Should Pause ID.me Software Deal, Adviser Says (1)*, BLOOMBERG L. (Feb. 16, 2022, 10:00 AM), https://www.bloomberglaw.com/product/privacy/bloomberglawnews/bloomberg-law-news/X2A9FGR0000000.

76. Donnan & Bass, *supra* note 3, at 3–4.

77. Metz, *supra* note 70.

78. Bass & Donnan, *supra* note 75.

79. *Id.*

80. ID.ME, https://www.id.me/ (last visited Feb. 9, 2023) (touting an array of services from identity verification to an ID.me digital wallet).

81. *See generally* Alan Rappeport, *I.R.S. Will Allow Taxpayers to Forgo Facial Recognition Amid Blowback*, N.Y. TIMES (Feb. 21, 2022), https://www.nytimes.com/2022/02/21/us/politics/irs-facial-recognition.html; Christopher Burgess, *Clearview AI Commercialization of Facial Recognition Raises Concerns, Risks*, CSO ONLINE (Mar. 8, 2022, 2:00 AM), https://www.csoonline.com/article/3651455/clearview-ai-commercialization-of-facial-recognition-raises-concerns-risks.html.

commercial FRT systems that were developed by training their algorithms with images collected without the subject's consent is extremely problematic.[82] Current litigation against Clearview raises critical consumer biometric privacy issues; and so far, courts have rejected Clearview's First Amendment argument that the company's scraping practices are protected by free speech[83] and have allowed multiple suits against the FRT company to proceed.[84] Notably, Clearview ultimately settled a lawsuit filed by the American Civil Liberties Union ("ACLU") in 2020 after years of fighting in an Illinois state court.[85] The ACLU alleged that Clearview's collection practices violated some Illinois residents' biometric privacy and uniquely harmed those in vulnerable communities such as domestic violence and sexual assault survivors.[86] In a huge win for consumer privacy, the settlement restricts Clearview from contracting with Illinois government agencies and law enforcement for five years and permanently bans Clearview from selling access to its database to private companies and entities nationwide.[87] Yet Clearview continues to vigorously fight a separate consumer class action lawsuit that claims the company improperly collected and stored individuals' faceprints without proper disclosure or consent.[88] Clearview's unwillingness to settle could signal the company's intention to take the legal argument to the highest court possible.[89]

---

82. *See infra* pt. IV.B.

83. Geoffrey Xiao, *Bad Bots: Regulating the Scraping of Public Personal Information*, 34 HARV. J.L. & TECH. 701, 727 (2021).

84. *Illinois Court Rejects Clearview's Attempt to Halt Lawsuit Against Privacy-Destroying Surveillance*, ACLU (Aug. 27, 2021), www.aclu.org/press-releases/illinois-court-rejects-clearviews-attempt-halt-lawsuit-against-privacy-destroying?msclkid=ea2e17a7bccc11ec9dddca17bb647657 [hereinafter *ACLU Press Release*]; Adam Schwartz, *Victory! More Lawsuits Proceed Against Clearview's Face Surveillance*, ELEC. FRONTIER FOUND. (Feb. 15, 2022), https://www.eff.org/deeplinks/2022/02/victory-another-lawsuit-proceeds-against-clearviews-face-surveillance.

85. Cyrus Farivar, *Clearview AI Settles Facial Recognition Suit With ACLU, Will Alter Some Practices*, FORBES (May 9, 2022, 2:32 PM), https://www.forbes.com/sites/cyrusfarivar/2022/05/09/clearview-ai-facial-recognition-suit-with-aclu/?sh=1614ab3b7f41.

86. *ACLU Press Release, supra* note 84.

87. Farivar, *supra* note 85.

88. Christina Tabacco, *Clearview AI Asks Court to Take Second Look at Dismissal Order in Biometric Information Privacy MDL*, LAW ST. (Mar. 16, 2022), https://lawstreetmedia.com/news/tech/clearview-ai-asks-court-to-take-second-look-at-dismissal-order-in-biometric-information-privacy-mdl/?msclkid=04aef466bcd411ec8789524f45ab07d6.

89. *Id.*

Of additional concern is the requirement by government agencies that an individual's sole point of access to the agency be through ID.me's verification software.[90] The Department of Veteran Affairs, Social Security Administration, and other federal agencies employ ID.me as an identity authentication tool.[91] Similarly, the IRS planned to require user identity verification through ID.me but reversed course due to public backlash.[92] Alternatively, the IRS now allows taxpayers to opt-in to using the authentication tool.[93]

And while there is no current litigation against ID.me, the increased use of the FRT company's services by state and federal agencies remains a part of the national conversation concerning government agencies' blind trust that commercial companies are properly handling United States citizens' biometric data.[94] Of particular relevance, ID.me is now the focus of a congressional investigation of the FRT company's use by public services during the pandemic.[95] Additionally, in May 2022, several United States senators formally requested that the FTC investigate ID.me for violating unfair and deceptive trade practices when the company's CEO intentionally lied to the public to give the impression that the type of database comparison employed by the company was a less controversial method than what the company actually used.[96] Significantly, recent studies project the FRT global market to grow from an approximately $5 billion industry in 2020 to an estimated $13 billion industry over the next six years.[97] With North America

90. Donnan & Bass, *supra* note 3.

91. Rappeport & Hill, *supra* note 15.

92. *Id.*

93. *Id.*

94. Lauren Rosenblatt, *The IRS Dropped ID.me's Facial Recognition Tech After Backlash. WA Is Rolling It Out in June*, SEATTLE TIMES (Mar. 2, 2022, 1:28 PM), https://www.seattletimes.com/business/the-irs-dropped-id-mes-facial-recognition-tech-after-backlash-wa-is-rolling-it-out-in-june/?msclkid=84e7114dbcd711eca2510db46a138cc9.

95. *Maloney and Clyburn Launch Investigation into Use of ID.me Facial Recognition Technology in Public Services*, SELECT SUBCOMM. ON THE CORONAVIRUS CRISIS (Apr. 14, 2022), https://coronavirus.house.gov/news/press-releases/clyburn-maloney-idme-identity-unemployment-covid-oversight.

96. A one-to-one comparison is a more reliable method, and the one-to-many comparison has resulted in bias. Shawn Donnan & Dina Bass, *IRS Selfie-Tech Provider Stirs Senate Ire over Face Recognition*, BLOOMBERG L. (May 18, 2022, 12:14 PM), https://news.bloomberglaw.com/privacy-and-data-security/senators-seek-ftc-probe-of-irs-provider-id-me-selfie-technology?context=search&index=2.

97. Ayang Macdonald, *Two Analyses Project Facial Recognition Market at Around $13B by 2028*, BIOMETRIC UPDATE (Mar. 29, 2022, 5:48 PM), https://www.biometricupdate.com/202203/two-analyses-project-facial-recognition-market-at-around-13b-by-2028.

comprising the largest region and growth in the studies, it is clear that government oversight of commercial companies handling United States citizens' biometric data will be necessary moving forward.[98]

Americans trust government agencies to protect their information. Therefore, a government's use of a third-party company whose purpose is to create biometric information for an individual—in addition to collecting that person's driver's license image and social security number—is dangerous without proper regulation. And when an individual is required by the government to agree to use FRT or be denied access to essential governmental services, the issue of consent becomes a great concern.

Finally, it is worth acknowledging that many federal agencies use their own FRT systems, yet several of those agencies have still relied on commercial FRT companies.[99] Of particular note, both the United States Immigration and Customs Enforcement ("ICE") and United States Customs and Border Protection ("CBP") have accessed Clearview's database for border security purposes.[100] ICE admitted to temporarily testing Clearview's services in 2020 to verify identities of suspected victims and offenders in child exploitation cases that occurred both domestically and internationally.[101] Additionally, CBP officers employed Clearview's services in 2019 to identify suspected criminals and individuals with arrest records that had previously been deported and were attempting reentry at one of the United States borders.[102] Clearly, many governmental agencies on federal, state, and local levels exploit commercial FRT companies' services for a variety of reasons, making regulation of commercial FRT companies' practices imperative moving forward.

## *IV. BIOMETRIC DATA LEGAL PROTECTIONS*

Recent Supreme Court decisions have left many Americans questioning their fundamental rights; particularly the right to privacy.[103] However, privacy is not a right explicitly guaranteed by

98. *Id.*
99. AUGUST 2021 GAO REPORT, *supra* note 8, at 17.
100. *Id.* at 20.
101. *Id.*
102. *Id.*
103. *See* Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228 (2022) (overturning a woman's constitutional right to an abortion observed in *Roe v. Wade*); *see also* Dan Mangan,

the United States Constitution.[104] Instead, the right to privacy has developed through a rich history of case law, state legislation, and federal regulations.[105]

### A. State Regulations of Biometric and Privacy Data

Some states have consumer privacy protection laws that protect personal data, but only three—Illinois, Texas, and Washington—have comprehensive biometrics privacy protection acts.[106] And only Illinois' Biometric Information Privacy Act ("BIPA") affords citizens a private right of action.[107] Notably, California, Colorado, and Virginia have comprehensive consumer protection acts that include the protection of biometrics, and comprehensive consumer protection acts are proposed in New York, Florida, and Maryland.[108]

Accordingly, an onslaught of recent litigation against Clearview, Meta, and others for their FRT services has arisen in Illinois, Texas, and California.[109] Still, the potential threat to these companies is largely in Illinois because of BIPA's grant of the plaintiff's right of action, rather than other states which require suits be brought by the attorney general.[110]

---

*Supreme Court Justice Clarence Thomas Says Gay Rights, Contraception Rulings Should Be Reconsidered After Roe Is Overturned*, CNBC (June 24, 2022, 1:54 PM), https://www.cnbc.com/2022/06/24/roe-v-wade-supreme-court-justice-thomas-says-gay-rights-rulings-open-to-be-tossed.html.

104. *See* Griswold v. Connecticut, 381 U.S. 479 (1965). "[S]pecific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance." *Id.* at 484.

105. *See generally id.*; Loving v. Virginia, 388 U.S. 1 (1967); Obergefell v. Hodges, 576 U.S. 644 (2015).

106. Klosowski, *supra* note 17.

107. Biometric Information Privacy Act (BIPA) § 20, 740 ILL. COMP. STAT. 14/20 (2008).

108. Jake Holland, *As Biometric Lawsuits Pile Up, Companies Eye Adoption with Care*, BLOOMBERG L. (Feb. 9, 2022, 5:00 AM), https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/BNA%200000017ed4e8de63a7fffde92af10000?bna_news_filter=privacy-and-data-security.

109. Jake Holland, *2022 Privacy Legislation Success Viable as Three States Lead Way*, BLOOMBERG L. (Jan. 3, 2022, 5:00 AM) https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/X422PFIK000000?bna_news_filter=privacy-and-data-security#jcite.

110. *Id.*

### *1. Illinois' Biometric Privacy Information Act*

Biometric data is described by the Department of Homeland Security as "unique physical characteristics . . . that can be used for automated recognition."[111] However, BIPA provides a more in-depth definition of biometric information, noting it is information based on a person's biometric identifier such as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[112] BIPA regulates the collection and storage of biometric information, specifically prohibiting an entity from collecting an individual's biometric information without first providing written notification to the individual that details the type of biometric information being stored and the length of time the company will retain the information.[113] Additionally, the company must receive the individual's written consent agreeing to the collection and storage of the biometric data.[114] If a company violates an Illinois citizen's BIPA rights, the citizen has a private right of action to pursue liquidated or actual damages, injunctive relief, and reasonable court-associated costs—including attorneys' fees.[115]

In fact, Illinois residents have secured significant settlements in recent class action lawsuits brought under BIPA. In March 2021, Facebook settled a class action lawsuit for $650 million because the company performed automated face-tagging without obtaining consent from affected Illinois residents.[116] Kronos, Inc., a software company that provides employee time clocks, recently settled a class action suit for $15 million when it violated BIPA by collecting thousands of fingerprints without proper notification or consent of the collection and storage of the biometric data.[117]

As previously mentioned, the focus has turned to Clearview for scraping billions of photographs from the internet to extrapolate unique biometric identifiers for the creation of facial mapping for use in their identification software and searchable

111. *Biometrics*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/biometrics (Dec. 14, 2021).
112. BIPA § 10.
113. *Id.* § 15.
114. *Id.*
115. *Id.* § 20.
116. Hatmaker, *supra* note 20.
117. Chris Burt, *Kronos Agrees to Settle Biometric Data Privacy Lawsuit for $15M*, BIOMETRIC UPDATE (Feb. 15, 2022, 5:54 PM), https://www.biometricupdate.com/202202/kronos-agrees-to-settle-biometric-data-privacy-lawsuit-for-15m.

database.[118] In early 2022, a federal judge in the United States District Court for the Northern District of Illinois allowed a consumer class action lawsuit alleging that Clearview's practices violated BIPA to continue.[119] Most notably, the judge dismissed Clearview's First Amendment argument that the company's collection of photos was protected by free speech.[120] Clearview argued that because the images were public information, Clearview's conduct of collecting and analyzing the photos was protected speech, and therefore enforcing BIPA would violate Clearview's First Amendment right to analyze public information.[121] On the other hand, the plaintiffs contended that their biometric identifiers were not publicly available information, and Clearview's conduct of extracting the biometric identifiers without obtaining consent did not constitute protected speech.[122] The court agreed with the plaintiffs and determined that Clearview's conduct to create its database "involve[d] both speech and nonspeech elements," and minimal restrictions on First Amendment rights may be justified if an important governmental interest in regulating the nonspeech element exists.[123] After applying intermediate scrutiny, the court concluded that the First Amendment did not bar BIPA and thus denied Clearview's motion to dismiss in respect to that argument.[124] If the $650 million Facebook settlement may be used as an indicator, damages could be monumental if Clearview elects to settle.[125] However, this case has the potential of reaching the United States Supreme Court if Clearview pushes forward.[126]

118. *In re* Clearview AI, Inc., Consumer Priv. Litig., 585 F. Supp. 3d 1111, 1118 (N.D. Ill. Feb. 14, 2022), *clarified on denial of reconsideration*, No. 21-CV-0135, 2022 WL 2915627 (N.D. Ill. July 25, 2022); *see supra* pt. III.B.

119. *In re Clearview AI, Inc.*, 585 F. Supp. 3d at 1118.

120. *Id.* at 1120–21.

121. *Id.* at 1120.

122. *Id.*

123. *Id.*

124. *Id.* at 1221.

125. Hatmaker, *supra* note 20.

126. Andrea Vittorio, *Clearview AI Fails to Shake Consumer Face Scan Privacy Lawsuit*, BLOOMBERG L. (July 26, 2022, 12:02 PM), https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/X98QGGEO000000?bna_news_filter=privacy-and-data-security#jcite. Clearview continues to argue the plaintiffs do not have standing without a concrete injury and the Court continues to reject that argument. *Id.*

### *2. Texas' Capture and Use of Biometric Identifier Act*

Texas' biometric privacy law, Texas Capture and Use of Biometric Identifier Act ("CUBI"), was codified in 2009 and places the same meaning on "biometric identifiers" as BIPA does for "biometric information."[127] CUBI forbids a party from collecting or using an individual's biometric identifiers for a commercial purpose without first informing the individual and then receiving the individual's consent.[128] The Texas Act also regulates the storage, transmission, and destruction of Texans' biometric identifiers.[129] Notably, a CUBI violation carries a hefty fine of up to $25,000 per violation, though the remedy may only be pursued by the state's Attorney General on behalf of injured Texans.[130]

The Texas Attorney General attempted to test the strength of CUBI in 2022 when he sued Meta on behalf of Texas Facebook users over the social media site's decade-long practice of collecting its users' biometric data without informed consent.[131] The complaint calls out Facebook's "face-tagging" option that prompted users upon uploading photos to identify their friends and family—not for the user's convenience but instead for the users' and non-users' biometric identifiers lifted from the images—in order to build a database to train its Artificial Intelligence ("AI") to develop algorithms capable of deep fake technology.[132] Because the suit is on behalf of millions of Texans and Texas alleged *billions* of CUBI violations occurred, the monetary ramifications could be catastrophic to Meta and other companies doing business in Texas.[133]

127. TEX. BUS. & COM. CODE ANN. § 503.001(a) (West 2009).

128. *Id.* § 503.001(b).

129. *Id.* § 503.001(c).

130. *Id.* § 503.001(d); Buresh, *supra* note 55, at 81.

131. Hatmaker, *supra* note 20. Facebook's face mapping practices were already the subject of the Illinois BIPA lawsuit that settled for $650 million in 2022. *Id.*

132. Plaintiff's Petition at 12, Texas v. Meta Platforms, Inc., No. 22-0121 (Tex. Dist. Ct., Harrison Cnty. Feb. 14, 2022).

133. *Id.* at 3. Particularly, this could serve as precedence for a potential Texas lawsuit against Clearview or any other company using a database of photos pulled without consent to train its AI software to develop more accurate FRT. *Id.*

### *3. Washington's Biometric Privacy Law*[134]

In 2017, Washington enacted a biometric privacy law that prohibits the enrollment of an individual's biometric identifiers in a commercial database without notifying the individual, attaining consent, or ensuring the impossibility of future use of the biometric identifier for a commercial purpose.[135] Additionally, the law restricts the storage and protection of biometric identifiers for a commercial purpose but clarifies that none of the restrictions apply if advancing a security purpose.[136] Interestingly, Washington does not explicitly designate facial geometry in its definition of biometric identifiers, choosing only to allude to it as "data generated by automatic measurements of an individual's biological characteristics."[137] The Washington law also excludes financial institutions, health care administration, and law enforcement when acting within the scope of their duties.[138] As in Texas, a private right of action is not provided in Washington, placing the responsibility on the Attorney General to bring claims on behalf of injured Washingtonians under the Washington consumer protection act.[139] And in contrast to Illinois and Texas, Washington places no set fines on violations of its biometric identifier laws—a decision that arguably defangs the law.[140]

### *4.Other States' Consumer Privacy Protection Acts*

A growing number of states without specific biometric privacy laws have incorporated biometric protections in their state's consumer privacy laws.[141] The most prevalent is California's comprehensive consumer privacy act, the California Consumer

134. WASH. REV. CODE ANN. § 19.375.010–.900 (West 2017).

135. *Id.* § 19.375.020(1). The law defines a "Commercial purpose" as the:

> [F]urtherance of the sale or disclosure to a third party of a biometric identifier for the purpose of marketing of goods or services when such goods or services are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier.

*Id.* § 19.375.010(4).

136. *See id.* § 19.375.020.

137. *Id.* § 19.375.010(1).

138. *Id.* § 19.375.040.

139. *Id.* § 19.375.030.

140. *Id.*

141. Sheila A. Millar & Tracy P. Marshall, *The State of the State Privacy Laws: A Comparison*, NAT'L L. REV., Dec. 1, 2021, https://www.natlawreview.com/article/state-state-privacy-laws-comparison.

Protection Act ("CCPA") which includes biometric information in its definition of "personal information."[142] The CCPA prohibits companies that conduct business with California residents from obtaining, storing, or sharing a California resident's personal information without first attaining the person's consent and, among other things, giving the individual the chance to opt out of the company's sharing practices.[143] Notably, the CCPA provides a private right of action for individuals injured through a data breach, but other violations by offending companies must be enforced by the California Attorney General.[144]

Many other states now include biometric data in their definitions of personal information with respect to each state's data breach and identity theft laws.[145] Of particular note, New Hampshire forbids government agencies from demanding biometric data as a prerequisite for the receipt of an agency's services or to otherwise conduct business with a state agency.[146] Curiously, Florida's data protection law fails to include biometric data or identifiers in the definition of confidential personal information, yet the state's identity theft law prohibiting criminal use of personal identification information includes biometric data in its definition.[147] While piecemeal privacy laws afford some protection over individuals' biometric data, unless a person resides in Illinois or California, individuals must solely rely on their respective Attorneys General to enforce penalties against offending companies for violations.[148]

### B. Federal Regulations of Biometric Data

The path for individuals seeking federal regulation of biometric information currently runs through the Federal Trade

142. CAL. CIV. CODE § 1798.140(o)(E) (2022).
143. *Id.* §§ 1798.120–.130.
144. *Id.* § 1798.155.
145. Millar & Marshall, *supra* note 141. In addition to California, Colorado and Virginia have passed comprehensive consumer privacy acts that include biometric data as personal information. *Id.*
146. N.H. REV. STAT. § 359-N:2 (2022).
147. *Compare* FLA. STAT. § 501.171 (2019) (defining personal information broadly without the inclusion of biometric data regarding data security), *with* FLA. STAT. § 817.568 (2021) (including biometric data specifically in the definition of personal identification information as applied to identity theft).
148. Xiao, *supra* note 83, at 716.

Commission.[149] The FTC provides consumer protection against unfair or deceptive business practices, and FTC enforcement has mainly focused on a company obtaining the consumers' knowledge and consent to biometrics handling.[150] Yet enforcement through the FTC is far from ideal because consumers lack a private right of action under section 5 of the FTC Act,[151] and the Supreme Court decision in *AMG Capital Management, LLC v. FTC* limited the FTC's power to injunctive relief under section 13(b) of the FTC Act.[152]

Most recently, the FTC flexed its enforcement muscles with its first FRT mishandling settlement when it sued Everalbum, a California-based photo storage and organization company, in January 2021 for deceptive and unfair trade practices in violation of section 5 of the FTC Act.[153] Everalbum's questionable practices derived from the company's smartphone app that enabled customers to organize and store photos by uploading the pictures to a cloud-based storage system.[154] According to the FTC complaint, in 2017, Everalbum offered a new feature that grouped a user's photos by the faces in the pictures and allowed the user to label the friends in the photos by name.[155] Everalbum set the face recognition feature as a default on the app and provided no way for customers to disable it.[156] In fact, Everalbum waited over a year to request customer consent for the feature and even then only sent the notifications to customers who resided in Illinois, Texas, Washington, and the European Union.[157] Not coincidentally, those

149. *FTC Finalizes Settlement with Photo App Developer Related to Misuse of Facial Recognition Technology*, FED. TRADE COMM'N (May 7, 2021), https://www.ftc.gov/news-events/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse [hereinafter *FTC Everalbum Press Release*].

150. David Oberly, *Practical Guidance for Minimizing FTC Liability Exposure When Using Facial Biometrics*, BIOMETRIC UPDATE (Jan. 11, 2022, 7:43 AM), https://www.biometricupdate.com/202201/practical-guidance-for-minimizing-ftc-liability-exposure-when-using-facial-biometrics.

151. The Federal Trade Commission Act, 15 U.S.C. § 45.

152. 141 S. Ct. 1341, 1352 (2021).

153. Lesley Fair, *Facing the Facts About Facial Recognition*, FED. TRADE COMM'N (Jan. 11, 2021), https://www.ftc.gov/business-guidance/blog/2021/01/facing-facts-about-facial-recognition.

154. Complaint at 1, Everalbum, Inc., No. C-4743 (F.T.C. Jan. 11, 2021), 2021 WL 118893.

155. *Id.* at 2.

156. Richik Sarkar, *Developments in Advertising and Consumer Protection*, 77 BUS. L. 313, 319 (2021).

157. Complaint, *supra* note 154, at 2.

same geographically located customers were also given an option to disable the feature at any time.[158]

The company then rolled out a notification requesting customer consent for the feature to all of its customers—regardless of their geographical location—in April of 2019.[159] In 2018, between the launch of the customer consent request notifications, Everalbum posted an article in the "Help" section of its website informing customers that the company assumed customer consent to the use of face mapping if the facial recognition feature was turned on in the app.[160] Yet customers outside of Illinois, Texas, Washington, and the European Union had no way to disable the default feature, thus making the assumed "consent" misleading for those customers.[161]

To further muddy the waters, Everalbum began developing its own FRT by using its customers' photos combined with publicly available datasets to train a new algorithm.[162] Over the course of two years, Everalbum used millions of its users' photos to improve its FRT for the smartphone app.[163] Additionally, Everalbum used the photos to develop a new FRT service, Paravision, that it then sold to companies for the purpose of strengthening security and access as well as a means for the companies to facilitate payments.[164] Notably, Everalbum's privacy policy for the app stated that a user's information would be deleted as soon as possible following account deactivation, and the user's photos and videos would be deleted upon deactivation.[165] But instead the company retained the photos from deactivated accounts for an indeterminate time period until it implemented a new photo deletion process in October of 2019.[166]

Everalbum's misrepresentations to customers regarding the storage of customer photos along with the customer's inability to deny consent for the feature were unfair and deceptive practices that violated section 5 of the FTC Act and ultimately resulted in

158. *Id.*
159. *Id.* at 3.
160. *Id.*
161. *Id.* at 2.
162. *Id.* at 3.
163. *Id.*
164. *Id.* at 4.
165. *Id.* at 5–6.
166. *Id.* at 6.; Decision and Order at 4–5, Everalbum, Inc., No. C-4743 (F.T.C. May 6, 2021), 2021 WL 1922417 (explaining that the company's new practice required deletion of photos and videos following the deactivation of an account for three months or more).

the company reaching a settlement with the FTC.[167] The settlement required Everalbum to change its disclosure practices regarding user consent, storage, and deletion of illegally obtained photos or videos.[168] Importantly, the settlement not only required the deletion of the photos but also deletion of the algorithm developed through the use of the photos.[169]

Because the FTC cannot impose penalties against a company on its first offense—or obtain equitable monetary relief for consumers—at first blush, the lack of imposed penalties seemed like a wasted opportunity to make an example out of the company.[170] As noted before, the only Everalbum customers with a private right of action resided in Illinois, and Everalbum thoughtfully protected those customers in accordance with BIPA to avoid consumer litigation in that state.[171] However, the FTC's requirement of Everalbum to delete the unlawfully obtained photos as well as the algorithm trained through the use of those photos could prove significant if the FTC brings action against companies like Meta and Clearview for arguably implementing the same practices as Everalbum to develop their respective FRT algorithms.

### C. Proposed Federal Comprehensive Data Privacy Legislation

In July 2022, the House Energy and Commerce Committee introduced into federal legislation the American Data Privacy and Protection Act ("ADPPA"), a proposed comprehensive consumer privacy act that resembles the CCPA in its protection of biometric data much more than it resembles the biometric protections afforded by BIPA.[172] The bipartisan effort would allow claims to be brought by the FTC, state attorneys general, chief consumer

167. *Id.* at 1.

168. *Id.* at 4.

169. Rebecca Kelly Slaughter, Janice Kopec & Mohamad Batal, *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission*, 23 YALE J.L. & TECH. 1, 39 (2021).

170. FED. TRADE COMM'N, STATEMENT OF COMMISSIONER ROHIT CHOPRA 2 (Jan. 8, 2021), https://www.ftc.gov/system/files/documents/public_statements/1585858/updated_final_chopra_statement_on_everalbum_for_circulation.pdf (regarding *Everalbum*); *see also* AMG Cap. Mgmt., LLC v. FTC, 141 S. Ct. 1341, 1352 (2021).

171. FED. TRADE COMM'N, *supra* note 170, at 2.

172. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 204 (2022). Biometric information falls under "sensitive covered data" that requires an entity to obtain an individual's consent to collect, store, or transfer the data to a third party. *Id.* Individuals would also be afforded a right to opt out of sharing information in certain situations. *Id.*

protection enforcement officers, or—four years following the commencement of the act—through a private right of action.[173] The ADPPA would also establish a separate bureau under the FTC to assist in enforcement, though it is unclear what the bureau's duties would entail.[174] Relief under the Act depends upon the enforcer and includes civil penalties, compensatory damages, injunctive relief, and litigation costs, though this is not an exhaustive list.[175] Remarkably, the legislation proposes a blanket preemption of state laws yet excludes from preemption any state legislation that exclusively pertains to FRT and specifically exempts BIPA from preemption.[176] Arguably, the decision not to preempt state biometric laws signals the need for a detailed federal biometric privacy act.

## *V. RECOMMENDED LEGISLATION CREATING A NATIONAL BIOMETRICS SAFETY BOARD*

Clearly, FRT companies must be federally regulated to ensure the protection of Americans' privacy without hindering technological advances. Despite this necessity, the road to a federal biometric privacy act is littered with Congress' failed attempts over the past couple of years.[177] And while the introduction of the ADPPA is a step in the right direction, Congress' track record regarding the passage of comprehensive privacy legislation is hardly reassuring of the ADPPA's enactment.[178] Even if the ADPPA survives the Congressional battlefield, Congress must then shift its focus toward tailoring legislation to safeguard citizens' biometric privacy; particularly, the regulation of commercial FRT companies that contract with state or federal agencies.

173. *Id.* §§ 401–03.
174. *Id.* § 401(a).
175. *See id.* §§ 401–03.
176. *Id.* § 404(b)(2)(D), (K)–(L). The ADPPA also excludes from preemption state data breach reporting requirements, a curious choice to not standardize reporting requirements when given the opportunity. *Id.* § 404(b)(2)(D).
177. *See, e.g.*, Consumer Online Privacy Rights Act, S. 3195, 117th Cong. (2021); Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. (2019).
178. *See, e.g.*, S. 3195; S. 847.

### A. Proposed Federal Legislation

The current reactive approach of state privacy and FRT laws does nothing to discourage commercial FRT companies from forging ahead with laissez-faire attitudes toward obtaining an individual's consent for the collection and use of the person's images.[179] Indeed, Meta and Clearview theoretically could end up collectively paying billions of dollars in settlements, but that will likely be a relatively small price overall to train their respective algorithms that could ultimately bring in hundreds of billions of dollars.[180] Further, compelling companies to publicly maintain data storage and retention schedules is only effective if the companies are held accountable for their practices by an overseeing entity.[181] Accordingly, Congress should act with urgency to enact a federal biometric information privacy bill that specifically creates new standards and proactively regulates government contracted, commercial FRT companies that collect, store, and use biometric data or collect, store, or use images with the intent of deriving biometric data.

Whether enacted as a standalone federal biometric privacy bill or an addition to a federal comprehensive privacy bill (or act), it is essential that proposed biometric privacy legislation includes proactive steps to regulate FRT and other biometric companies to ensure biometric privacy protections occur at every stage of a biometric company's processes. Specifically, the promulgation of an independent biometric privacy safety board to regulate FRT and biometric companies' practices is imperative to protect citizens and businesses alike.

---

179. Bobby Allyn, *States Fight over How Our Data Is Tracked and Sold Online, as Congress Stalls*, NPR (June 4, 2021, 7:34 PM), https://www.npr.org/2021/06/04/1003205422/states-fight-over-how-our-data-is-tracked-and-sold-online-as-congress-stalls; *see also* Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14 (2008).

180. *Is Trending Stock Meta Platforms, Inc. (META) a Buy Now?*, YAHOO! FIN. (Aug. 2, 2022, 9:00 AM), https://finance.yahoo.com/news/trending-stock-meta-platforms-inc-130001350.html (projecting Meta's valuation at over $100 billion consecutively over the next two years, despite the overall poor performance of technology companies in the stock market); Kashmir Hill, *Clearview AI Raises $30 Million from Investors Despite Legal Troubles*, N.Y. TIMES (Oct. 28, 2021), https://www.nytimes.com/2021/07/21/technology/clearview-ai-valuation.html (indicating Clearview AI has a valuation of $130 million).

181. *ID.me Biometric Retention*, *supra* note 5.

### *1. Learning from Sarbanes-Oxley*

The enactment of the Sarbanes-Oxley Act of 2002 ("Sarbanes-Oxley") followed a series of corporate scandals that resulted in a shaken stock market, a fractured corporate business model, and thousands of workers left with little to no retirement.[182] Congress' swift reaction to the economic carnage included the establishment of the Public Company Accounting Oversight Board ("PCAOB").[183] The independent board provides external regulation of accounting firms and auditing practices as well as derives industry standards and guidance under the enforcement power of the Securities and Exchange Commission ("SEC").[184]

### *2. Proposed Establishment of an Independent Biometric Privacy Safety Board*

Waiting until disaster strikes millions of Americans to create biometric privacy protections is unacceptable, particularly when state and federal agencies mandate the use of commercial FRT companies for citizens' access to public services. Thus, somewhat akin to the solution provided by Sarbanes-Oxley, proposed biometric privacy legislation should create a biometrics safety board responsible for deriving standards and issuing guidance—in conjunction with NIST standards and guidelines—to companies that obtain or store biometric information as well as perform inspections of company practices and procedures, all under the enforcement power of the FTC.[185] This ensures companies' compliance with regulatory procedures but allows the public and private sector to benefit from necessary technological advances without compromising Americans' cherished personal biometric information. The regulation would further offer security to citizens required by governmental agencies to use FRT applications for the purpose of accessing public services. Moreover, a national biometrics safety board would protect and secure stored biometric information instead of waiting for individuals to suffer actual harm via a data breach. And unless Congress passes a comprehensive

182. 15 U.S.C. § 7211; Keith L. Johnson, *Rebuilding Corporate Boards and Refocusing Shareholders for the Post-Enron Era*, 76 ST. JOHN'S L. REV. 787, 787 (2002).

183. John Paul Lucci, *Enron—The Bankruptcy Heard Around the World and the International Ricochet of Sarbanes-Oxley*, 67 ALB. L. REV. 211, 222–23 (2003).

184. 15 U.S.C. §§ 7211–20.

185. *See FTC Everalbum Press Release*, *supra* note 149.

privacy act like the ADPPA allowing for a private right of action, consumers seeking monetary relief may continue to rely on state laws, but the objective is to limit the overall need for damages.[186]

### B. Elements of the Drafted Legislation

As a baseline, proposed legislation for a federal biometric information privacy bill or addition to any existing federal comprehensive privacy act should contain provisions specific to FRT companies that require the companies to not only notify affected individuals of the collection or capture of their images for the purpose of deriving biometric data, but also to obtain written consent for the storage, use, or transfer of the person's biometric data. Further, the law must require posted data storage, retention, and destruction schedules of which proof of destruction will be offered in accordance with the schedule or upon the individual's request—whichever is earlier. Provisions for exclusions from the bill would allow companies to comply with consumer privacy protections provided for in other relevant federal acts that govern financial and health information.[187] The law will preempt state laws to the extent that the baseline provisions of the bill are inconsistent or not provided for in those state laws. Finally, just as Sarbanes-Oxley created the PCAOB, the legislation will promulgate the aforementioned national biometrics safety board.[188]

Proposed legislation establishing the national biometrics safety board will contain the following detailed provisions:

#### *1. Purpose*

The Biometric Privacy Safety Board is established to oversee companies that house, process, or develop biometric information and technologies, including but not limited to FRT companies, regardless of the company's public or private status or government affiliation, to ensure compliance with National Institute of Standards and Technology ("NIST") standards and biometric information privacy laws in order to protect citizens' privacy

186. *See supra* pt. IV.A. (detailing state privacy laws).

187. *See* Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–09; Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936 (1996).

188. *See supra* pt. V.A.

interests in furtherance of the public interest in the highest level of safety and security of biometric information necessary to protect individuals and companies alike.

*2. Status*

The Board shall operate as a nonprofit organization and shall not be an agency of the United States Government nor will any agent or member of the Board be deemed an officer or employee of the United States Federal Government.

*3. Duties of the Board*

The Board shall be subject to the FTC and carry out responsibilities in accordance with the provisions of this Act including:

> (1) Proactive regulation and inspection of companies that house, process, or develop biometric information and technologies, including but not limited to FRT companies, and will ensure compliance with biometric privacy laws pertaining to the following:
>
> > a. proper notification and consent to obtain or transfer biometric data;
> >
> > b. proscribed data storage, retention, and deletion schedules; and
> >
> > c. following industry specific standards regarding the proper storage and security of biometric data.
>
> (2) Establishing and adopting reporting rules and standards, in conjunction with NIST standards and guidelines, for biometric companies to assist with compliance with this Act;
>
> (3) Conducting investigations and proceedings to determine recommendations to the Commission regarding disciplinary and enforcement actions;
>
> (4) Any other duties determined by the Board or commission deemed necessary to enforce compliance with this Act.

### *4. Members of the Board*

(1) Composition

> The Board will be comprised of five (5) members, individuals with specific knowledge and understanding of biometric technology and data security, proven integrity and of the highest reputation in the biometric technology and data security fields, to be appointed by the Commission.

(2) Dedicated Full-time Service

> Members must solely serve the Board on a full-time basis and hold no other professional or business obligations in the form of employment or profit otherwise from services relating to biometric technology or data security.

### *5. Reporting to the Commission*

The Board must submit a report to the Commission detailing all inspections, investigations, and findings to the Commission on an annual basis. All reports will be open to public inspection in accordance with rules of the Board, Commission, and applicable federal laws concerning the protection of confidential or proprietary information housed in the reports; and in all events, the Board shall protect from public disclosure a company's proprietary information.

## *VI. CONCLUSION*

The effect of recent technological innovations on modern society could previously have only been possible in a Hollywood script. Yet, Americans now experience cutting-edge technology in most aspects of their lives.[189] FRT arguably enriches the lives of citizens in many ways from identity verification for leisurely travel to defending the nation through the identification of known terrorists. Still, a dark side of FRT inevitably exists which makes the governmental allowance of FRT companies' unchecked

189. *Mobile Fact Sheet*, *supra* note 6.

practices in the collection and use of biometric data unacceptable. The government's continued use of the companies Clearview and ID.me—despite their questionable practices—requires legislative action to protect American citizens' biometric privacy. Further, the issue of governmental agencies essentially forcing individuals to consent to relinquish their biometric data to unregulated companies like ID.me in order to receive public services is intolerable. Protections provided by current state biometric privacy laws, particularly in Illinois, Texas, and Washington, have proven necessary to protect citizens' biometric data, but it is imperative that Congress enact a federal biometric privacy law.

Accordingly, this Article proposes the enactment of federal biometric information privacy legislation that specifically establishes a national biometric safety board under the enforcement power of the FTC to oversee FRT companies conducting business in the United States. The Article argues for the necessity of proactive legislation to protect citizens and companies alike by holding FRT and biometric companies accountable for their biometrics handling practices; particularly, the inspection and investigation of FRT companies that contract with the government and stand between citizens and public services. And if upon inspection the board finds a company engaged in illegal practices in order to train its algorithms, the FTC should follow its precedence set in *Everalbum* and force the elimination of the algorithms. The law has always struggled to catch up to technology. However, when the government puts Americans' most sensitive data in the hands of unregulated FRT companies, the government must figure out a way to proactively control those companies and in turn Americans' biometric data.