Clearview AI's First Amendment: A Dangerous Reality?

*Bonnie E. Devany**

On May 9, 2022, Clearview AI and the ACLU settled a two-year long dispute over the Illinois Biometric Information Privacy Act (BIPA), which prohibits companies like Clearview from scraping mass amounts of data from the internet. The ACLU sued Clearview for collecting billions of our personal—but publicly available—photos, a violation not only of BIPA but also of the user agreements of websites like Facebook, LinkedIn, and Twitter. Clearview uses these photos to create the largest known facial recognition database. Clearview's technology, which it licenses to law enforcement agencies across the country, can identify a face in a matter of seconds. As privacy and technology continue to clash, ACLU v. Clearview, Inc. *provided an opportunity to address the underlying constitutional tension between the First Amendment and privacy. But since the suit settled, these questions remain unanswered.*

Clearview claims it has a First Amendment right to scrape data and sell its facial recognition service. Legal scholars have disposed of this argument as "simplistic," "at odds with long-established First Amendment doctrine," "far from convincing," and even "dangerous." But whether we like it or not, Clearview's claims might not be so far off from current First Amendment jurisprudence, which has recently taken an aggressive and deregulatory turn. This Note explores current First Amendment jurisprudence and Clearview AI's interpretation of the First Amendment, which might be a reality. This Note also addresses the advantages and risks associated with facial recognition technology (FRT). Finally, this Note proposes a template for legislation that can regulate FRT in a way that is consistent with modern notions of privacy and current First Amendment doctrine.

---

* The University of Texas School of Law, J.D. 2022. Bonnie Devany would like to thank her Professor, Adam Klein, for teaching a wonderful seminar and providing instrumental guidance on this project; the outstanding members and editors of Volume 101 of the *Texas Law Review* for their assistance; Kallen Dimitroff for her helpful feedback and constant encouragement; and Alex Gaudio for his endless support.

Introduction

In the summer of 2019, Sergei Abanichev threw an empty paper cup at a protest in Moscow.[1] A week later, nine police officers barged through his apartment door and arrested him for "rioting and mass disorder."[2] He was identified by one of Moscow's 189,000 surveillance cameras with facial recognition capabilities.[3] Although his charges were eventually dropped, spending a month in prison was enough to deter him from participating in the

1. Robyn Dixon, *Russia's Surveillance State Still Doesn't Match China. But Putin Is Racing to Catch Up.*, WASH. POST (Apr. 17, 2021, 4:00 AM), https://www.washingtonpost.com/world/europe/russia-facial-recognition-surveillance-navalny/2021/04/16/4b97dc80-8c0a-11eb-a33e-da28941cb9ac_story.html [https://perma.cc/9GHQ-N5Y9].

2. *Id.*

3. *Id.*

next year's protest.[4] "Instead of the system being used for the benefit of the city," he said, "it is being used as a tool of total surveillance and total control of citizens."[5] Civil rights advocates worry that "[s]preading fear and deterring activism may be just the point" of Moscow's new facial recognition system.[6]

As much as our face is our own, it is also a piece of data waiting to be harvested, which is exactly what Clearview AI is doing—harvesting billions of our personal photos without our consent from Facebook, LinkedIn, and Twitter to create an application that allows law enforcement to identify a face within seconds.[7] What used to be a little-known company has since come to the forefront of headlines, as Clearview's facial recognition application was used to identify protestors during the 2020 Black Lives Matter protests[8] and suspects of the January 6 Capitol Insurrection.[9]

Facial recognition will likely be remembered as the technology that changed the early twenty-first century.[10] But its uses are something we might not always be comfortable with. As technology and privacy continue to clash, facial recognition technology looms over us. Clearview AI claims it has a First Amendment right to scrape data and sell its facial recognition service.[11] Many critics in the legal community have disposed of this argument as "baseless,"[12] "simplistic,"[13] "at odds with long-established First Amendment

4. *Id.*

5. *Id.*

6. *Id.*

7. Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/X6PF-2VZH] (Nov. 2, 2021).

8. *See, e.g.*, Elizabeth Lopatto, *Clearview AI CEO Says 'Over 2,400 Police Agencies' Are Using Its Facial Recognition Software*, VERGE (Aug. 26, 2020, 4:40 PM), https://www.theverge.com/2020/8/26/21402978/clearview-ai-ceo-interview-2400-police-agencies-facial-recognition [https://perma.cc/7BBW-5RDR] (reporting on the use of FRT by the New York Police Department to arrest activists during the Black Lives Matter protests).

9. *See, e.g.*, Kashmir Hill, *The Facial-Recognition App Clearview Sees a Spike in Use After Capitol Attack*, N.Y. TIMES, https://www.nytimes.com/2021/01/09/technology/facial-recognition-clearview-capitol.html [https://perma.cc/GP7L-FBUT] (Jan. 31, 2021) (reporting on the use of FRT by the Miami Police Department and Oxford Police Department in Alabama to assist the FBI in identifying Capital rioters).

10. *See, e.g.*, *Emerging Technologies that Will Change the World*, MIT TECH. REV., Jan./Feb. 2001, at 97, 106 (discussing biometrics, in particular facial recognition technology, in review of ten emerging technologies that will change the world).

11. Vera Eidelman, *Clearview's Dangerous Misreading of the First Amendment Could Spell the End of Privacy Laws*, ACLU (Jan. 7, 2021), https://www.aclu.org/news/privacy-technology/clearviews-dangerous-misreading-of-the-first-amendment-could-spell-the-end-of-privacy-laws/ [https://perma.cc/33DX-RXEC].

12. Daniel Levin, *Face the Facts, or Is the Face a Fact?: Biometric Privacy in Publicly Available Data*, 32 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1010, 1059 (2022).

13. Margot E. Kaminski & Scott Skinner-Thompson, *Free Speech Isn't a Free Pass for Privacy Violations*, SLATE (Mar. 9, 2020, 2:53 PM), https://slate.com/technology/2020/03/free-speech-privacy-clearview-ai-maine-isps.html [https://perma.cc/5LPY-SLFJ].

doctrine,"[14] "far from convincing,"[15] and even "dangerous."[16] But, whether we like it or not, Clearview's claims might not be so far off from current First Amendment jurisprudence, which has recently taken an "aggressive, deregulatory turn."[17]

This Note proceeds in four parts. Part I introduces facial recognition technology, law enforcement's use of biometric technologies, and Clearview AI. Part II conceptualizes facial recognition technology as a modern panopticon, explores facial recognition technology use across the globe, and introduces what makes data privacy regulation in the United States unique—the First Amendment and the values surrounding it. Part III evaluates facial recognition technology as it relates to the First Amendment.

First, Part III suggests that facial recognition data likely falls within the scope of protected speech under the First Amendment. Second, it overviews relevant First Amendment jurisprudence, including uncertainties about the applicable judicial standard under the commercial speech doctrine. Finally, Part III grapples with the tension between the First Amendment and data privacy concerns. Considering this tension, Part IV offers an evaluation of current state regulatory efforts and recommends a legislative template to regulate law enforcement's use of facial recognition technology within the bounds of the First Amendment.

I. An Introduction to Facial Recognition Technology

A. Law Enforcement's Use of Biometric Technology: From Thumbprints to Faceprints

The use of biometric[18] technology to aid policing dates back to the nineteenth century, when anthropologist Alphonse Bertillon created the first biometric database of criminals.[19] The database included a variety of measurements—such as the circumference of the head or the length of the

14. Eidelman, *supra* note 11.

15. Kaminski & Skinner-Thompson, *supra* note 13 (referring to the "myth" that "there's no such thing as privacy in public").

16. Woodrow Hartzog & Neil Richards, *Getting the First Amendment Wrong*, BOS. GLOBE, https://www.bostonglobe.com/2020/09/04/opinion/getting-first-amendment-wrong/ [https://perma.cc/3DWX-GSQC] (Sept. 4, 2020, 3:03 AM).

17. G.S. Hans, *No Exit: Ten Years of "Privacy vs. Speech" Post*-Sorrell, 65 WASH. U. J.L. & POL'Y 19, 39 (2021).

18. "Biometrics" are biological measurements or physical characteristics that can be used to identify a person—such as fingerprints, speech patterns, or irises. KELSEY Y. SANTAMARIA, CONG. RSCH. SERV., R46541, FACIAL RECOGNITION TECHNOLOGY AND LAW ENFORCEMENT: SELECT CONSTITUTIONAL CONSIDERATIONS 4 (2020).

19. Alexander T. Nguyen, *Here's Looking at You, Kid: Has Face-Recognition Technology Completely Outflanked the Fourth Amendment?*, 7 VA. J.L. & TECH., Spring 2002, at 1, 4.

middle finger—used to identify criminals.[20] After friction ridge skin identification became more prevalent, fingerprints would also be added to anthropometric records.[21] Sir Francis Galton, the cousin of Charles Darwin, published the first book establishing that the ridges in the skin of fingerprints were unique in 1892.[22] And that same year, the Rojas murder case was the first homicide case to be solved using fingerprint evidence.[23] By 1902, law enforcement agencies in the United States were developing fingerprint classification systems.[24] Soon after, prisons throughout the United States acquired large databases of fingerprints.[25] But as fingerprint databases began to rapidly grow, matching fingerprints became inefficient—staffers had to shift through thousands of index cards to find a match.[26] In 1985, a detective in Los Angeles trying to identify a fingerprint would have to look through nearly two-million index cards, which would take a single technician sixty-seven years to complete.[27] Today, with the development of the Automatic Fingerprint Identification System (AFIS), a computer can do it in minutes.[28] AFIS is a computer program that reduces fingerprints to a set of coordinates and is able to match fingerprints quickly and accurately.[29] The use of fingerprinting—now commonplace—is an invaluable tool.[30]

In the late 1980s and the early 1990s, the Department of Defense received significant funding to embark on creating a similar system but for identifying faces.[31] Facial recognition technology (FRT) is a biometric technology that compares images of faces to determine whether the images are of the same individual.[32] Similar to our fingerprints and DNA profiles, our "faceprints" rely on our unique features—like the distance between our

20. *Id.*

21. Jeffery G. Barnes, *Chapter 1: History*, *in* THE FINGERPRINT SOURCEBOOK 5, 12 (2010).

22. *Id.* at 13. Everyone—even identical twins—has unique fingerprints, as fingerprints result from "random processes during pregnancy." Nguyen, *supra* note 19, at 4.

23. Barnes, *supra* note 21, at 13–14. Francisca Rojas accused a man of murdering her two children in Buenos Aires in 1892, after she refused to marry him because she was in love with a different man. *Id.* at 13. The accused man was brutally beaten by local authorities but maintained that he did not kill the children. *Id.* An investigator found a bloody fingerprint on the door of Rojas's home. *Id.* at 13–14. After analyzing the fingerprint, the investigator concluded that it did not match the accused but instead matched Rojas. *Id.* at 14. When Rojas was confronted with this evidence, she confessed to having murdered her own children; and Argentina became the first country to rely solely on fingerprints as a method of identification. *Id.*

24. *Id.* at 16.

25. *Id.* at 20.

26. Nguyen, *supra* note 19, at 5.

27. *Id.*

28. *Id.*

29. *Id.*

30. Barnes, *supra* note 21, at 7.

31. Nguyen, *supra* note 19, at 5.

32. SANTAMARIA, *supra* note 18, at 4.

eyes and nose or the shape of our cheekbones—to identify us.[33] FRT uses machine-learning algorithms to detect and measure these distinctive facial features, creating a unique faceprint formula based on facial geometry.[34]

FRT can be used in several functions, the two most common being (1) *face verification*—which confirms a person's claimed identity to do things like unlock an iPhone and (2) *face identification*—which compares an unknown face against a series of known faces to do things like identify a criminal suspect.[35] Despite initial technical reliability concerns, "numerous public and private entities are incorporating FRT into their operations, "as part of the larger biometric technology boom."[36] And law enforcement agencies are increasingly using FRT to identify suspects.[37] Today, thirty-seven states maintain FRT searchable databases of driver's license photos.[38] But for many law enforcement agencies, this was just the beginning, and a free trial of a service from a small startup company—Clearview AI—would open up FRT possibilities they had never imagined.

B. An Introduction to the Company That Changed the Game: Clearview AI

On January 18, 2020, Kashmir Hill's *New York Times* article introduced Clearview AI—and what might be the end of privacy as we know it—to the world.[39] Clearview developed an application that even the big tech companies strayed from "because of its radical erosion of privacy."[40] Its application can scan over a billion faces in less than a second.[41] While the application's capabilities are far beyond anything the federal government or Silicon Valley tech giants have ever produced, it's not the algorithms Clearview uses that are particularly novel.[42] Rather it's Clearview's method of gathering facial images that makes it unique. An FRT system is "only as

33. Eidelman, *supra* note 11.

34. John M. McNichols, *Keeping One's Public Face Private*, LITIG. NEWS, Spring 2021, at 2, 2.

35. SANTAMARIA, *supra* note 18, at 4.

36. Douglas A. Fretty, *Face-Recognition Surveillance: A Moment of Truth for Fourth Amendment Rights in Public Places*, 16 VA. J.L. & TECH. 430, 434 (2011).

37. SANTAMARIA, *supra* note 18, at 5.

38. Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409, 430 (2014).

39. Hill, *supra* note 7.

40. *Id.*

41. Ryan Mac, Caroline Haskins, Brianna Sacks & Logan McDonald, *Surveillance Nation*, BUZZFEED NEWS, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition [https://perma.cc/XP6P-TKA9] (Apr. 9, 2021, 6:52 PM).

42. *See* Hill, *supra* note 7 (describing how companies have been capable of producing similar technology but have refrained from doing so due to privacy concerns).

useful as its photo database,"[43] and Clearview has the largest.[44] Without our consent, and in violation of the sites' user agreements, Clearview scraped billions of personal—but publicly available—photos from social media sites, including Facebook, Twitter, and LinkedIn.[45] Clearview's business model is simple. After scraping images of people's faces from across the internet, the algorithm converts all the facial images into faceprints.[46] When a user uploads a photo to the application, it matches the photo with all the photos with similar faceprints.[47] The application returns to the user links to the publicly available images on the internet, which often include additional information about the person identified.[48] Clearview sells its application in the form of annual licenses.[49]

Clearview's most effective sales technique, which it began in 2017, was offering police departments thirty-day free trials.[50] Police departments have had access to facial recognition tools for almost twenty years, but these tools were limited to government-provided images, such as mug shots.[51] Clearview's application, on the other hand, isn't limited to just straight-on images of criminal suspects but includes millions of average Americans from different angles and in different kinds of lighting. The departments had never used a tool as effective as Clearview. Within seconds of their free trials, police officers were able to identify shoplifters, sex offenders, and suspects in identity-fraud and dead-end cases.[52] In one instance, a police department was able to identify a person accused of sexually abusing a child whose face matched with a person who appeared in the mirror of someone else's gym

43. Fretty, *supra* note 36, at 436.

44. *Company Overview*, CLEARVIEW AI, https://www.clearview.ai/overview [https://perma.cc/D78E-QE7C].

45. Hill, *supra* note 7.

46. *Id.*

47. *Id.*

48. ACLU v. Clearview AI, Inc., No. 2020 CH 04353, 1 (Ill. Cir. Ct. Aug. 27, 2021).

49. Hill, *supra* note 7. A data breach revealed that Clearview's customers aren't limited to only law enforcement. Ryan Mac, Caroline Haskins & Logan McDonald, *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA*, BUZZFEED NEWS, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement [https://perma.cc/YB22-Y9WC] (Feb. 27, 2020, 10:37 PM). While there are greater concerns with commercial use of FRT, those are beyond the scope of this Note.

50. Hill, *supra* note 7. The free trials have continued. On the top right-hand corner of Clearview's website is a prominent "Request a Demo" button. CLEARVIEW AI, https://www.clearview.ai [https://perma.cc/8CBR-JC2J]. Following the January 6 Capitol Insurrection, police officers reached out to Clearview salespeople asking for free access to identify rioters, which Clearview granted "because it was an emergency situation." Kashmir Hill, *Your Face Is Not Your Own*, N.Y. TIMES: MAG. (Mar. 18, 2021), https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html [https://perma.cc/Q72P-KRB2] [hereinafter Hill, *Your Face Is Not Your Own*].

51. Hill, *supra* note 7.

52. *Id.*

photo.[53] The officers, impressed with the successes of their free trials, would then encourage their departments to sign up for licenses.[54]

Just eighteen months after the *New York Times* article broke, Clearview AI was named one of *Time*'s "100 Most Influential Companies" of 2021.[55] Self-described as "the world's largest facial network,"[56] Clearview's database now has over 20 billion facial images.[57] But Clearview's business model has been met with harsh criticism. Professor Woodrow Hartzog, for example, believes that Clearview is "the latest proof that facial recognition should be banned in the United States."[58] Clearview considers it "an honor to be at the center of the debate"[59] and includes links to various controversial articles on its website's "Media Highlights" page.[60] Clearview is facing multiple lawsuits for alleged privacy violations.[61] It argues, however, that these lawsuits should be dismissed because it has a First Amendment right to collect and use public photos that appear on the internet.[62] While the marketplace of ideas—a dominant First Amendment theory—advocates for the dissemination of information in the search for truth, the marketplace of *digital* ideas poses new challenges to privacy rights.[63]

II. The Panopticon Problem of FRT Use Across the Globe

As an architectural structure, "[a] panopticon allows a watcher[] to observe occupants without the occupants knowing whether or [when] they are being watched."[64] As a metaphor, beginning in the twentieth century, the panopticon represents the "surveillance tendencies of disciplinarian

53. *Id.*

54. *Id.*

55. Juliette Pearse, *2021 TIME100 Most Influential Companies: Clearview AI*, TIME (Apr. 26, 2021, 11:52 AM), https://time.com/collection/time100-companies/5953748/clearview-ai/ [https://perma.cc/DP65-YKRJ].

56. Leigh Mc Gowran, *Clearview AI Plans to Put Almost Every Human Face in Its Database*, SILICONREPUBLIC (Feb. 17, 2022), https://www.siliconrepublic.com/enterprise/clearview-ai-100-billion-photos-facial-recognition-database [https://perma.cc/8JGX-NUAX].

57. *Company Overview*, *supra* note 44.

58. Hill, *supra* note 7.

59. Lopatto, *supra* note 8.

60. *Media Highlights*, CLEARVIEW AI, https://www.clearview.ai/highlights [https://perma.cc/L3P2-C2HR] (citing, among others, Hill's 2020 *New York Times* article on Clearview).

61. Mac et al., *supra* note 41.

62. *E.g.*, Defendant's Memorandum of Law in Support of Its Motion to Dismiss at 16, ACLU v. Clearview AI, Inc., No. 2020 CH 04353 (Ill. Cir. Ct. Aug. 27, 2021).

63. *See* Alexander Tsesis, *Marketplace of Ideas, Privacy, and the Digital Audience*, 94 NOTRE DAME L. REV. 1585, 1586–87 (2019) (arguing that "massive retention of personal information poses a substantial harm to the privacy interests of data subjects").

64. Thomas McMullan, *What Does the Panopticon Mean in the Age of Digital Surveillance?*, GUARDIAN (July 23, 2015, 3:00 AM), https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham [https://perma.cc/8C77-PV5D].

societies" and the societal response of unease and fear.[65] Jeremy Bentham introduced the concept of a panopticon in 1791.[66] A panopticon is a circular building with prison cells lining the circumference.[67] At the center is a tower where the watchperson sits.[68] A bright light shines from the tower, so the watchperson can observe the prisoners, but the prisoners cannot see the watchperson.[69] Bentham envisioned a panopticon to be both a more humane and more efficient means of surveillance.[70] But in 1975, French philosopher Michel Foucault revitalized the concept: "He is seen, but he does not see; he is the object of information, never a subject in communication."[71] Foucault addressed the interplay of power and animosity.[72] What Foucault feared the most was that the panopticon operated via "power of mind over mind."[73] Because the prisoner never knows when they are being watched, the prisoner self-polices out of fear of punishment.[74]

Today, the central tower of the panopticon is not a physical structure. Instead, it is the digital and data-driven surveillance methods that loom over society. Like a panopticon, FRT capabilities can cause a considerable infringement on personal privacy and give rise to the fear of always being watched.[75] FRT is increasingly being used globally by law enforcement.[76] But there are concerns about abusing the technology. For some countries, FRT is a means of controlling citizens, what I deem the panopticon problem of FRT use. For others, FRT represents a dangerous encroachment on the privacy of citizens. Looking at other countries' uses of FRT sheds light on the dangers and benefits of FRT that embodies the debate surrounding its use. Comparing these approaches offers policy considerations when deciding whether and how to regulate FRT use. Across the globe, FRT use ranges widely. Perhaps the most drastic disparity in use is illustrated by China and

65. *Id.*

66. *See generally* 1 JEREMY BENTHAM, PANOPTICON: OR, THE INSPECTION-HOUSE (Dublin, Thomas Byrne, 1791) (outlining a plan for an institutional panopticon through a series of letters).

67. *Id.* at 4.

68. *Id.*

69. *Id.* at 5.

70. *Id.* at 25, 27–28 (emphasizing that an institutional panopticon would require few watchpersons, reduce the burden on judges and other magistrates, and decrease the danger of infection).

71. MICHEL FOUCAULT, PANOPTICISM, *in* DISCIPLINE AND PUNISH (Alan Sheridan trans., 1977) (1975), *as reprinted in* 2 RACE/ETHNICITY: MULTIDISCIPLINARY GLOBAL CONTEXTS 1, 5 (2008).

72. *Id.* at 7–9.

73. *Id.* at 10 (internal quotation marks omitted).

74. McMullan, *supra* note 64.

75. Anna Dorothea Ker, *Facial Recognition: A Privacy Crisis*, PRIVACY ISSUE, https://theprivacyissue.com/ai-and-biometrics/facial-recognition-privacy-crisis [https://perma.cc/S7G6-R4HL] (Jan. 31, 2020).

76. Dixon, *supra* note 1.

Russia on one end, and the European Union, UK, and Canada on the other end. But, as we'll see, the United States doesn't—and this Note argues shouldn't—fit on either of these polar ends.

A. Facial Recognition Technology Use in China and Russia

China is a leader in facial recognition and data collection.[77] China's surveillance system was designed to "apply the ideas of military cyber systems to civilian public security."[78] Across the country, police are being equipped with facial recognition glasses that enable real-time facial recognition surveillance.[79] The glasses are capable of "highly effective" crowd screening.[80] While these technologies can be useful in catching criminals, they also "make it easier for authorities to track political dissidents and profile ethnic minorities."[81] Almost all of China's 1.4 billion citizens are included in an FRT database.[82] And the Chinese government is using FRT to track Uighurs[83] and to identify Hong Kong dissidents.[84] The Henan province is building a system with real-time FRT that will be used to detect and monitor "people of concern," including foreign journalists.[85] One journalist said it is not clear whether or not the Chinese government is capable of using facial recognition software in the way it claims but adds: "It doesn't even matter whether it's true or not, as long as people believe it . . . . Once you believe it's true, it's like you don't even need the policemen at the corner anymore, because you're becoming your own policeman."[86] Like the hidden watchperson in the center of the panopticon, the Chinese government is

77. *See* Dave Davies, *Facial Recognition and Beyond: Journalist Ventures Inside China's 'Surveillance State,'* NPR (Jan. 5, 2021, 12:50 PM), https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-chinas-surveillance-sta [https://perma.cc/7DDN-U56K] (discussing the rise of security cameras and FRT in China and detailing how China became "a leader in artificial intelligence and data collection").

78. Chris Buckley & Paul Mozur, *How China Uses High-Tech Surveillance to Subdue Minorities*, N.Y. TIMES (May 22, 2019), https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html [https://perma.cc/DLY5-4T6P] (internal quotation marks omitted).

79. Josh Chin, *Chinese Police Add Facial-Recognition Glasses to Surveillance Arsenal*, WALL ST. J. (Feb. 7, 2018, 6:52 AM), https://www.wsj.com/articles/chinese-police-go-robocop-with-facial-recognition-glasses-1518004353 [https://perma.cc/KX5H-5HWY].

80. *Id.*

81. *Id.*

82. Ker, *supra* note 75.

83. *Id.*

84. Floyd Abrams & Lee Wolosky, *The Promise and Peril of Facial Recognition*, WALL ST. J. (Jan. 13, 2021, 6:10 PM), https://www.wsj.com/articles/the-promise-and-peril-of-facial-recognition-11610579445 [https://perma.cc/U8AH-DZ6Y].

85. James Clayton, *China Surveillance of Journalists to Use 'Traffic-Light' System*, BBC NEWS (Nov. 29, 2021), https://www.bbc.com/news/technology-59441379 [https://perma.cc/QL7J-V4AA].

86. Davies, *supra* note 77 (quoting German journalist Kai Strittmatter).

denying its citizens the freedom to live a life free from being watched—or at least from the fear of being watched.

While Russia's surveillance status does not yet match that of China, Russian authorities are rapidly ramping up their FRT capabilities.[87] Moscow rolled out its first FRT system in January 2020, which has since expanded to at least ten other Russian cities.[88] Moscow's system includes over 189,000 cameras with facial recognition capabilities.[89] The system is now used in 70% of criminal investigations.[90] And while Moscow officials purported that the FRT system was meant only to find criminal suspects, it was repurposed during the COVID-19 pandemic to enforce lockdowns.[91] FRT systems have also been used in Russia to "identify sex workers, porn stars and protestors."[92] And with the collection of facial-recognition surveillance data has been the rise of a "thriving" black market where corrupt officials sell faceprint data.[93] For the equivalent of $400, you can purchase live access to all system cameras.[94] Now, it's not just Russian law enforcement that have access to the data but also criminals.[95]

B. Facial Recognition Technology Use in the European Union, UK, and Canada

The European Union sits on the polar-opposite end of the FRT-use spectrum, as it is attempting to drastically restrict police use of FRT. The Artificial Intelligence Act is pending legislation that proposes a ban on private facial recognition databases, like the one Clearview operates.[96] It also limits the use of FRT "in public places unless it is to fight a 'serious' crime, such as kidnapping or terrorism."[97] Several political groups in the European Parliament are calling for a "blanket ban on facial recognition."[98] But this sentiment is not shared by all EU policymakers. German politician Thorsten Frei, for example, argues that FRT makes the world safer, as German police

87. Dixon, *supra* note 1.
88. *Id.*
89. *Id.*
90. *Id.*
91. Hill, *Your Face Is Not Your Own*, *supra* note 50.
92. *Id.*
93. Dixon, *supra* note 1.
94. *Id.*
95. *Id.*
96. Melissa Heikkilä, *European Parliament Calls for a Ban on Facial Recognition*, POLITICO (Oct. 6, 2021, 10:34 AM), https://www.politico.eu/article/european-parliament-ban-facial-recognition-brussels/ [https://perma.cc/9T82-7476].
97. *Id.*
98. *Id.*

are increasingly using FRT to identify criminals—with a false match rate of only 0.00018%.[99]

France put Clearview on formal notice to cease its "unlawful processing" of faces in violation of Europe's General Data Protection Regulation (GDPR).[100] The GDPR created the European "right to be forgotten," which allows a citizen to request the removal of certain personal data.[101] The UK, which retained the GDPR as national law after leaving the EU, has already held that Clearview's service violates privacy laws.[102]

Like the UK, Canada has also ruled that Clearview violated privacy laws and ordered Clearview to stop collecting data on Canadians and delete all previously collected data.[103] An investigation by the Office of the Privacy Commissioner of Canada found that police use of FRT resulted in "billions of people essentially [finding] themselves in a '24/7' police line-up," which it concluded "represented mass surveillance and was a clear violation" of Canada's federal privacy law.[104]

C. Facial Recognition Technology Use in the United States

By mid-2020, over 2,400 police agencies in the United States were using Clearview's facial recognition software.[105] The New York Police Department made 2,878 arrests pursuant to FRT searches in just five and a half years.[106] The Jacksonville Sheriff's Office runs on average 8,000 searches per month.[107] Clearview's "success stories" include testimony from agencies solving dead-end cases and identifying murderers and child sex

99. Thorsten Frei, *Facial Recognition Can Make Us Safer*, ABOUT:INTEL (Nov. 10, 2020), https://aboutintel.eu/facial-recognition-germany/ [https://perma.cc/M7BS-QGK6].

100. Natasha Lomas, *France Latest to Slap Clearview AI with Order to Delete Data*, TECHCRUNCH (Dec. 16, 2021, 12:28 PM), https://techcrunch.com/2021/12/16/clearview-gdpr-breaches-france/ [https://perma.cc/BJT2-7X38].

101. Kristie Byrum, *The European Right to Be Forgotten: A Challenge to the United States Constitution's First Amendment and to Professional Public Relations Ethics*, 43 PUB. RELS. REV. 102, 103 (2017).

102. Lomas, *supra* note 100.

103. Zack Whittaker, *Clearview AI Ruled 'Illegal' by Canadian Privacy Authorities*, TECHCRUNCH (Feb. 3, 2021, 5:55 PM), https://techcrunch.com/2021/02/03/clearview-ai-ruled-illegal-by-canadian-privacy-authorities/ [https://perma.cc/52YB-YDPJ].

104. OFF. OF THE PRIV. COMM'R OF CAN., POLICE USE OF FACIAL RECOGNITION TECHNOLOGY IN CANADA AND THE WAY FORWARD: OVERVIEW OF INVESTIGATION INTO RCMP'S USE OF CLEARVIEW AI (2021), https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/ [https://perma.cc/YGQ4-MJPG]. Canada's federal private sector privacy law is the Personal Information Protection and Electronic Documents Act (PIPEDA). *Id.*

105. Lopatto, *supra* note 8. FRT is also being used to identify undocumented immigrants for purposes of deportation and proceedings. Ker, *supra* note 75.

106. Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEO. L. CTR. ON PRIV. & TECH (May 16, 2019), https://www.flawedfacedata.com [https://perma.cc/KGR9-7RXB].

107. *Id.*

offenders.[108] Just how fingerprinting identification opened up possibilities of discovering truth and achieving justice,[109] many of Clearview's success stories would not have been possible without the use of FRT.[110]

However, seeing how FRT has been used as a means of control in other parts of the world, organizations like the ACLU argue that "[o]nce powerful surveillance systems like these are built and deployed, the harm will be extremely difficult to undo."[111] Critics are also concerned that searching billions of innocent faces without cause "negates the fundamental democratic principle of the presumption of innocence"; and that in eroding such protections, the use of FRT is essentially "altering the nature of democracy."[112] Some legal scholars argue that we ought to follow the EU's lead in severely limiting or banning police use of FRT.[113]

The right to privacy is deeply rooted in American history and legal jurisprudence.[114] The Supreme Court has acknowledged that a threat to privacy is "implicit in the accumulation of vast amounts of personal information in computerized data banks."[115] And contemporary Americans recognize the ability to move about in public or online without being tracked as an important aspect of privacy.[116] Yet there is a stark difference between

108. *Success Stories*, CLEARVIEW AI, https://www.clearview.ai/blog/categories/success-stories [https://perma.cc/3PC3-W5QX].

109. For a discussion on the Rojas murder case, the first case to be solved using fingerprinting, see *supra* note 23.

110. *See generally Success Stories*, *supra* note 108 (providing links to articles detailing successful uses of Clearview's FRT).

111. Matt Cagle & Nicole A. Ozer, *Amazon Teams Up with Law Enforcement to Deploy Dangerous New Face Recognition Technology*, ACLU N. CAL. (May 22, 2018), https://www.aclunc.org/blog/amazon-teams-law-enforcement-deploy-dangerous-new-face-recognition-technology [https://perma.cc/R69F-X88B].

112. Ker, *supra* note 75.

113. *See, e.g.*, Hartzog & Richards, *supra* note 16 (reporting on a European Court of Justice ruling that "imperiled" the ability of companies to process European data in the United States); *see also supra* note 58 and accompanying text.

114. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) ("That the individual shall have full protection in person and in property is a principle as old as the common law . . . ."). The Fourth Amendment protects against "unreasonable searches and seizures." U.S. CONST. amend. IV. Whether the use of facial recognition technology is a "search" within the meaning of the Fourth Amendment is beyond the scope of this Note. However, there has been rich academic discussion on the matter. *See, e.g.*, Matthew Doktor, *Facial Recognition and the Fourth Amendment in the Wake of* Carpenter v. United States, 89 U. CIN. L. REV. 552, 553 (2021) (evaluating whether *Carpenter* extends Fourth Amendment protections to facial recognition searches); Nguyen, *supra* note 19, at 3 (arguing that the "'reasonable expectation of privacy' doctrine outlined in Katz has outlived its usefulness and is helpless against face recognition software in public").

115. Whalen v. Roe, 429 U.S. 589, 605 (1977); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) (describing that under the third-party doctrine, "a person has no legitimate expectation of privacy [for Fourth Amendment purposes] in information he voluntarily turns over to third parties") (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

116. Brown, *supra* note 38, at 415.

the European and American approaches to privacy. And that difference lies in our Constitution's first—and arguably most important[117]—amendment. The First Amendment solidifies the American values of the free flow of information in society and the discovery of truth. Notions like the "right to be forgotten" challenge these long-established principles.[118] As Richard Posner once observed, "one aspect of privacy is the withholding or concealment of information."[119] But, as discussed in Part III below, First Amendment values often clash with these privacy values.[120]

III. Facial Recognition Technology and the First Amendment

When people think about the First Amendment, data analytics doesn't often come to mind. But the First Amendment's application to data analytics and FRT is a question working its way through the lower federal courts. This Part proceeds in three subparts. Subpart III(A) argues that facial recognition data is protected speech under the First Amendment; subpart III(B) explores current First Amendment jurisprudence; and subpart III(C) explains why the state of freedom of speech is at odds with privacy interests.

A. Facial Recognition Data Is Likely Protected Speech Under the First Amendment

Clearview's claim that it has a protected right to collect and sell faceprints may not run as afoul of First Amendment jurisprudence as many of the commentators in the legal field assert.[121] The Free Speech Clause of the First Amendment provides that the government "shall make no law . . . abridging the freedom of speech."[122] What the First Amendment protects as "speech" is more than just the verbal expressions we make.[123] While "nonexpressive" conduct is not protected,[124] the First Amendment *does* protect the "creation and dissemination of information."[125] There has

117. *See* BURT NEUBORNE, MADISON'S MUSIC: ON READING THE FIRST AMENDMENT 22 (2015) (interpreting the First Amendment as a "meticulously organized road map of a well-functioning egalitarian democracy").

118. Byrum, *supra* note 101, at 103.

119. Richard A. Posner, *An Economic Theory of Privacy*, REGULATION, May/June 1978, at 2, 19.

120. *See infra* subpart III(C).

121. *See supra* notes 11–16 and accompanying text.

122. U.S. CONST. amend. I. The clause was incorporated against the states in 1925. Gitlow v. New York, 268 U.S. 652, 666 (1925).

123. *See, e.g.*, Winters v. New York, 333 U.S. 507, 510 (1948) (holding First Amendment protections expand beyond the mere "exposition of ideas"); Sorrell v. IMS Health Inc., 564 U.S. 552, 570 (2011) ("[T]he creation and dissemination of information are speech within the meaning of the First Amendment."); *see also* Buckley v. Valeo, 424 U.S. 1, 15 (1976) ("The First Amendment protects political association as well as political expression.").

124. *Sorrell*, 564 U.S. at 567.

125. *Id.* at 570.

been a rich academic debate about if and when data can be considered speech.[126] And Clearview argues that the creation and use of its application constitutes the "creation and dissemination of information" protected by the First Amendment.[127]

Both access to and distribution of information are essential to the purpose of the First Amendment—to promote the discovery of truth and protect the free flow of opinions and ideologies.[128] In 1965, the Supreme Court first recognized the right to receive information and ideas,[129] which is now considered a principal "fundamental to our free society."[130] The Court acknowledges that "[f]acts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs."[131] Lower courts across the country are applying this notion to data. The Second Circuit, for example, has held that a software program qualified as protected speech under the First Amendment when the computer code combined both "nonspeech and speech elements."[132] The D.C. district court has similarly held that data scraping "plausibly falls within the ambit of the First Amendment."[133] In a variety of contexts, the Supreme Court has protected the right to gather and use public information.[134] Some scholars have interpreted these decisions as meaning that "freedom of speech carries an implicit right to create knowledge," and that when the government restricts an individual's right to create knowledge, the suppression is a restriction of free speech and must withstand judicial scrutiny.[135] But other scholars argue that this is the wrong interpretation of the First Amendment, particularly in relation to commercial speakers—like Clearview—because at its core, "the First Amendment's commitment to free speech is protecting

126. *See generally, e.g.*, Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1151 (2005) (rejecting the claim that "regulating databases regulates speech, [such] that the First Amendment is thus in conflict with the right of data privacy"); Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 63 (2014) (arguing that "for all practical purposes, and in every context relevant to the current debates in information law, data is speech").

127. ACLU v. Clearview AI, Inc., No. 2020 CH 4353, 8 (Ill. Cir. Ct. Aug. 27, 2021).

128. *See* Dennis v. United States, 341 U.S. 494, 503 (1951) ("[T]he basis of the First Amendment is the hypothesis that speech can rebut speech . . . [and that] free debate of ideas will result in the wisest governmental policies."); *see also* Whitney v. California, 274 U.S. 357, 375 (1927) (Brandeis and Holmes, JJ., concurring) ("[The founders] believed that freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth . . . .").

129. Lamont v. Postmaster Gen., 381 U.S. 301, 305 (1965).

130. Stanley v. Georgia, 394 U.S. 557, 564 (1969).

131. Sorrell v. IMS Health Inc., 564 U.S. 552, 570 (2011).

132. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 449, 451 (2d Cir. 2001).

133. Sandvig v. Sessions, 315 F. Supp. 3d 1, 15 (D.D.C. 2018).

134. *See, e.g.*, Globe Newspaper Co. v. Superior Ct., 457 U.S. 596, 605 (1982) (protecting public access to criminal trials); Fla. Star v. B.J.F., 491 U.S. 524, 526 (1989) (protecting the right to publish information from a police report made available in a press release).

135. *Id.*

individual speakers like protestors and journalists . . . , not giving constitutional protection to dangerous business models that inhibit expression."[136] However, in light of the Supreme Court's opinion in *Sorrell v. IMS Health Inc.*,[137] it seems increasingly more likely that Clearview's collection and use of data falls within the scope of the First Amendment.

In *Sorrell v. IMS Health Inc.*, the Supreme Court held that the sale, disclosure, and use of pharmacy records "[are] a form of expression protected by the Free Speech Clause of the First Amendment."[138] When pharmacies process prescriptions, they receive prescriber-identifying information.[139] Many pharmacies sell this information to "data miners," who analyze the information and produce reports on the prescribers' behaviors.[140] The data miners then lease these reports to pharmaceutical companies, who use the information to refine their marketing tactics and increase sales.[141]

Vermont enacted a law that prohibited pharmacies from selling these pharmacy records or using the data for marketing purposes.[142] Vermont argued that its law did not implicate the First Amendment because it did not regulate speech, only access to information.[143] The Court, however, rejected the State's argument, reasoning that an individual's freedom of speech is implicated when *information* is "subjected to 'restraints on the way in which the information might be used' or disseminated."[144] Even though the respondents—the data miners and pharmaceutical companies—did not themselves possess the information, the information was nevertheless "in the hands of pharmacies and other private entities," which the Court held was sufficient to implicate the respondents' own speech interests.[145] In doing so, the Court emphasized that a restriction on the disclosure of information could either "facilitate or burden the expression of *potential* recipients" and thus implicate the First Amendment.[146] It also underscored that "the '*sale*' of [information] is simply disclosure of information for profit," which doesn't negate the information's status as protected speech.[147]

136. Hartzog & Richards, *supra* note 16.

137. 564 U.S. 552 (2011).

138. *Id.* at 557.

139. *Id.* at 558.

140. *Id.*

141. *Id.*

142. *Id.* at 557. The law provided exceptions in instances where the prescriber consented. *Id.* at 559.

143. *Id.* at 567.

144. *Id.* at 568 (quoting Seattle Times Co. v. Rhinehart, 467 U.S. 20, 32 (1984)).

145. *Id.* at 569–70.

146. *Id.* at 569 (emphasis added).

147. *Id.* at 570 (emphasis added) (alteration in original) (quoting IMS Health Inc. v. Sorrell, 631 F. Supp. 2d 434, 445 (D. Vt. 2009)).

Like the prescriber-identifying information in *Sorrell*, Clearview has a "strong argument" that the faceprints it collects are speech for First Amendment purposes.[148] The Court has declared that "information is speech."[149] Just as the data miners analyzed data and created reports from the prescriber-identifying information,[150] Clearview analyzes the data points of faces and creates reports—or faceprints—of the collection of the geometric values of the faces.[151] While the *Sorrell* opinion did produce a dissent, the dissent took issue with the majority's application of heightened scrutiny,[152] not the Court's classification of the data as speech.[153]

Along the same line, courts have on several occasions held that the activities of search engines constitute protected speech under the First Amendment.[154] In *Search King, Inc. v. Google Tech., Inc.*,[155] for example, an Oklahoma district court held that Google's search engine results amounted to "constitutionally protected opinions" and were "entitled to 'full constitutional protection'" because the ranking of results reflected "subjective result[s]" analogous to a publisher's protected right to decide what information to publish.[156] Clearview's application similarly makes "judgments about what information will be most useful to users"[157] and contributes to the dissemination of information.

A trial court in Cook County, Illinois, was the first court tasked with determining whether Clearview's operations constitute protected speech under the First Amendment.[158] The case sparked the involvement of several

148. *See id.* ("There is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes.").

149. *Id.*

150. *Id.* at 558.

151. Hill, *supra* note 7.

152. For a discussion on the applicable judicial standard, see *infra* subpart III(B).

153. *See Sorrell*, 564 U.S. at 581 (Breyer, J., dissenting) (arguing that "[t]he First Amendment does not require courts to apply a special 'heightened' standard of review when reviewing" a regulation on commercial speech).

154. *See, e.g.*, Search King, Inc. v. Google Tech., Inc., No. CIV-02-1457-M, 2003 U.S. Dist. LEXIS 27193, at *11–12 (W.D. Okla. May 27, 2003) (holding that results of Google search engines constitute protected speech); *see also* Memorandum of Points and Authorities in Support of Defendant Google Inc. to Strike Plaintiff's Complaint Pursuant to Civ. Proc. Code § 425.16 at 3, Martin v. Google Inc., No. CGC-14-539972, 2014 WL 6478416 (Cal. Super. Ct. Nov. 13, 2014) (noting that "[e]very court to consider the question of whether a search engine's ordering of search results constitutes constitutionally protected opinion has answered in the affirmative" in arguing to strike the plaintiff's complaint); *Martin*, 2014 WL 6478416, at *1 (granting the defendant's motion to strike because "the claims asserted against [the defendant] arise from constitutionally protected activity").

155. No. CIV-02-1457-M, 2003 U.S. Dist. LEXIS 27193 (W.D. Okla. May 27, 2003).

156. *Id.* at *11–12 (quoting Jefferson Cnty. Sch. Dist. No. R-1 v. Moody's Inv.'s Servs, Inc., 175 F.3d 848, 852 (10th Cir. 1999)).

157. Defendant's Memorandum of Law, *supra* note 62, at 17.

158. ACLU v. Clearview AI, Inc., No. 2020 CH 4353, 8 (Ill. Cir. Ct. Aug. 27, 2021).

amici, all of whom "agreed or assumed that Clearview's activities involve[d] speech" and were thus "entitled to some level of First Amendment protection."[159] The trial court agreed and held that "Clearview's activities involve expression and its predicates, which are entitled to some First Amendment protection."[160] Given the Court's recent developments in First Amendment jurisprudence, this conclusion is consistent with cases like *Sorrell*. What is not as clear, however, is what level of scrutiny a restriction on the use of FRT would have to survive.

B. Current First Amendment Jurisprudence

The First Amendment prohibits government entities from retaliating against individuals for engaging in protected speech.[161] While the First Amendment does not protect against "restrictions on economic activity," it does protect against burdens on speech that result from an economic motive.[162] Commercial speech, defined as speech that explicitly or implicitly "propose[s] a commercial transaction," has historically received less protection than other constitutionally protected expressions, such as political speech.[163] Data mining constitutes commercial speech because the data-mining industry "primarily exists to sell consumer data to third parties" and "profits are being made based off of the data information collected."[164] However, the current state of commercial speech is "uncertain."[165] After the Court's decision in *Sorrell*, "laws that regulate commercial activity might be much more likely . . . to be subject . . . to strict scrutiny."[166]

The early First Amendment cases addressing commercial speech seemed to "indicat[e] that commercial speech is unprotected."[167] But the Court backtracked in 1976 in *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.*,[168] in which the Court struck down a Virginia statute that prohibited advertising the prices of prescriptions.[169] The

159. *Id.* at 9.

160. *Id.*

161. Nieves v. Bartlett, 139 S. Ct. 1715, 1722 (2019).

162. Sorrell v. IMS Health Inc., 564 U.S. 552, 567 (2011).

163. *See* Va. Pharmacy Bd. v. Va. Consumer Council, 425 U.S. 748, 758, 760 (1976) (recounting previous Supreme Court decisions affording commercial speech no protection).

164. Kathryn Peyton, *The First Amendment and Data Privacy: Securing Data Privacy Laws that Withstand Constitutional Muster*, 2019 PEPP. L. REV. 51, 75–76 (2019).

165. Hans, *supra* note 17, at 29.

166. *Id.*

167. *Va. Pharmacy Bd.*, 425 U.S. at 758; *see* Valentine v. Chrestensen, 316 U.S. 52, 54 (1942) (noting that although "the streets are proper places for the exercise of the freedom" of speech, and that states could "not unduly burden" the streets' use in this manner, it was "equally clear that the Constitution imposes no such restraint on government as respects purely commercial advertising").

168. 425 U.S. 748 (1976).

169. *Id.* at 770.

Court explained that "speech does not lose its First Amendment protection because money is spent to project it."[170] Even if the advertiser's interest was a "purely economic one,"[171] society nevertheless has "a strong interest in the free flow of commercial information."[172] Emphasizing the "public interest" in being well-informed, the Court struck down the statute as an unconstitutional restriction on the "indispensable" free flow of information.[173] But in concluding that commercial speech, like other speech, is constitutionally protected, the Court added, "we of course do not hold that [commercial speech] can never be regulated in any way" and that "[s]ome forms of commercial speech regulation are surely permissible."[174]

Thus, as construed in *Virginia State Board of Pharmacy*, the First Amendment "does not prohibit the State from insuring that the stream of commercial information flow[s] cleanly as well as freely."[175] The Court left open which specific forms of commercial speech regulation are permissible but included that the Court had "often approved restrictions of that kind provided that they are justified without reference to the content of the regulated speech, that they serve a significant governmental interest, and that in so doing they leave open ample alternative channels for communication of the information."[176]

Four years later in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*,[177] the Supreme Court established a test for evaluating when a state can constitutionally restrict commercial speech that "is neither misleading nor related to unlawful activity."[178] The Court noted that "the protection available for [a] particular commercial expression turns on the nature both of the expression and of the governmental interests served by its regulation."[179] In commercial speech contexts, the principle First Amendment concern "is based on the informational function of advertising."[180] Following *Central Hudson*, it was widely thought that commercial speech was subject only to intermediate scrutiny.[181]

---

170. *Id.* at 761.

171. *Id.* at 762.

172. *Id.* at 764.

173. *Id.* at 765, 770.

174. *Id.* at 770; *see also id.* at 771 n.24 ("In concluding that commercial speech enjoys First Amendment protection, we have not held that it is wholly undifferentiable from other forms.").

175. *Id.* at 771–72.

176. *Id.* at 771.

177. 447 U.S. 557 (1980).

178. *Id.* at 564.

179. *Id.* at 563.

180. *Id.*

181. *See* Hans, *supra* note 17, at 29 (noting that laws in the future may be subject to strict scrutiny rather than the current intermediate scrutiny standard).

But the Court again addressed the standard of evaluating the constitutionality of restrictions of commercial speech in its 2011 decision, *Sorrell v. IMS Health Inc.*, discussed in subpart III(A). In *Sorrell*, although the Vermont law at issue prohibited pharmacies from selling prescriber-identifying information or using any such data for *marketing purposes*, the law allowed the information to be sold for purposes *other than* marketing.[182] Thus, the law "on its face burden[ed] disfavored speech by disfavored speakers"—marketing by marketers.[183] Because the law was "designed to impose a specific, content-based burden on protected expression," the Court applied strict scrutiny.[184] The Court rejected Vermont's argument that strict scrutiny was not warranted when a law is "a mere commercial regulation."[185] Instead, to "sustain the targeted, content-based burden" the law imposed, Vermont would have to "show at least that the statute directly advance[d] a substantial governmental interest and that the measure [was] drawn to achieve that interest."[186] While the Court assumed that medical privacy concerns were implicated in disclosing prescriber-identifying information, the Vermont statute was not narrowly drawn to serve that interest because pharmacies could still share the information for other purposes, just not marketing.[187] The Court left open the possibility of whether a state could address physician confidentiality through "a more coherent policy."[188] For example, the Court noted a statute that "advanced its asserted privacy interest by allowing the information's sale or disclosure in only a few narrow and well-justified circumstances" would "present quite a different case" than the one presented in *Sorrell*.[189] However, "[g]iven the information's widespread availability and many permissible uses," the Court held that the State's asserted interest in physician confidentiality did not justify the restriction on protected expression.[190]

Sorrell represents the Court's reluctance to apply *Central Hudson*'s more relaxed intermediate scrutiny standard.[191] The result? The Supreme

182. Sorrell v. IMS Health Inc., 564 U.S. 552, 559–60 (2011). For example, the information could be sold to "those who wish to engage in certain 'educational communications.'" *Id.* at 564.

183. *Id.* at 564.

184. *Id.* at 565.

185. *Id.* at 566–67. The Court emphasized that Vermont's law did "not simply have an effect on speech," but was "directed at certain content" and "aimed at particular speakers." *Id.* at 567.

186. *Id.* at 572.

187. *Id.* at 572–73.

188. *Id.* at 573 (quoting Greater New Orleans Broad. Ass'n., Inc. v. United States, 527 U.S. 173, 195 (1999)).

189. *Id.* at 573.

190. *Id.*

191. *See* Hans, *supra* note 17, at 29 (describing the Court's ambivalence with the *Central Hudson* framework).

Court is moving "perilously close towards a jurisprudence under which privacy laws are nearly impossible to craft."[192]

C. The Tension Between the First Amendment and Data Privacy

Data privacy regulations give rise to a tension between a right to speak absent of government restrictions and a right to be free of revelation of private information.[193] There is a "historic tension between privacy and speech interests"[194] because of the inherent clash in an "audience's right to information and a subject's right to privacy."[195] Chief Justice Warren and Justice Brandeis first addressed this tension in their famous article, *The Right to Privacy*.[196] The Justices articulated the public desire for the "right to be left alone."[197] They recognized that "[f]or years there ha[d] been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons."[198] Privacy, the Justices argued, was central to liberty.[199] And an individual "is entitled to decide whether that which is his shall be given to the public."[200] However, that "right is lost . . . when the author himself communicates his production to the public."[201] More so, the Court made clear in *Cox Broadcasting Corp. v. Cohn*[202] and *Florida Star v. B.J.F.*[203] that "absent a need to further a state interest of the highest order," information privacy speech restrictions are unconstitutional when they involve "truthful information about a matter of public significance."[204]

In *Cox Broadcasting Corp.*, a broadcasting company included the name of a rape victim when reporting on a rape case in violation of a state statute that prohibited the broadcasting of rape victims' names.[205] The broadcasting

192. *Id.* at 39.

193. Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1107 (2000).

194. Kaminski & Skinner-Thompson, *supra* note 13; *see also* Fla. Star v. B.J.F, 491 U.S. 524, 530 (1989) (noting the Court had "addressed several times" the "tension between the right which the First Amendment accords to a free press, on the one hand, and the protections which various statutes and common-law doctrines accord to personal privacy"); Hans, *supra* note 17, at 21 ("[P]rivacy and speech are . . . endlessly pitted as oppositional.").

195. Tsesis, *supra* note 63, at 1588.

196. *See generally* Warren & Brandeis, *supra* note 114 (discussing the point at which the right to privacy yields to the public welfare).

197. *Id.* at 195 (internal quotation marks omitted).

198. *Id.*

199. *Id.* at 196.

200. *Id.* at 199.

201. *Id.*

202. 420 U.S. 469 (1975).

203. 491 U.S. 524 (1989).

204. *Id.* at 533.

205. *Cox Broad. Corp.*, 420 U.S. at 473–74.

company obtained the victim's name from indictments in a public record.[206] The Court held that the statute was unconstitutional because once information is disclosed to the public, "the press cannot be sanctioned for publishing it."[207] The Court recognized that "even the prevailing law of invasion of privacy generally recognizes that the interests in privacy fade when the information involved already appears on the public record."[208] Holding otherwise, the Court noted, would "very likely lead to the suppression of many items that would otherwise be published and that should be made available to the public."[209]

Similarly, in *Florida Star*, a newspaper published a rape victim's full name in violation of a state statute that prohibited the publication of names of sexual assault victims.[210] The victim suffered severe emotional distress as a result of the publication.[211] The victim had to change her phone number, move, seek police protection, and obtain mental health counseling.[212] Her mother even received phone calls from a man threatening to rape the victim again.[213] Yet the Court held the statute prohibiting the publication of a sexual assault victim's name violated the First Amendment.[214] The Court reasoned that when a newspaper "lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order."[215] The Court held that the published information was a matter of "public interest, secured by the Constitution, in the dissemination of truth."[216] Thus, once the information was "'publicly revealed' or 'in the public domain' the court could not constitutionally restrain its dissemination."[217]

Like the information in *Cox Broadcasting Corp.*, the photos Clearview is scraping are publicly available, so a state may face challenges in constitutionally restricting their collection and use. And, based on the Court's *Florida Star* holding that reporting on criminal activities was a matter of

206. *Id.* at 472–73.

207. *Id.* at 496–97.

208. *Id.* at 494–95.

209. *Id.* at 496.

210. Fla. Star v. B.J.F., 491 U.S. 524, 526–27 (1989). The newspaper obtained the name from an incident report released by the police department. *Id.* at 528.

211. *Id.*

212. *Id.*

213. *Id.*

214. *Id.* at 532.

215. *Id.* at 533 (quoting Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 103 (1979)). The Court has also upheld the press's right to publish information of great public concern obtained unlawfully by a third party. Bartnicki v. Vopper, 532 U.S. 514, 517–18 (2001).

216. *Fla. Star*, 491 U.S. at 533 (quoting Cox Broad. Corp. v. Cohn, 420 U.S. 469, 491 (1975)).

217. *Id.* at 535 (quoting *Smith*, 443 U.S. at 103).

public significance, Clearview has a strong argument that its collection and use of faceprints are similarly a matter of public significance.

Clearview's database is a collection of publicly available information. All of the photos Clearview scrapes are publicly posted.[218] Some scholars argue that this is different than information made available via "public forums" because the places where expression occurs, such as Facebook, are privately owned as opposed to on government lands or physical public structures.[219]

But for the purpose of protecting dissemination, however, this distinction is minimal because social media sites like Facebook and Twitter have become "important places for people to engage in a wide variety of activity protected by the First Amendment."[220] More so, the Supreme Court has held that a person cannot maintain a reasonable sense of privacy for what that person "knowingly exposes to the public."[221] And even though social media sites are privately owned, they are open to the public, just like a shopping mall.[222] In balancing privacy interests and the collection and use of faceprints from publicly available photos, prohibiting the "dissemination of information which is already publicly available is relatively unlikely to advance the interests in the service of which the State seeks to act."[223]

Some scholars have argued that because of just how different technology is from traditional forms of speech, it ought to be analyzed under a different standard to determine whether it *is* speech.[224] Lucas Evans, for example, argues that "[t]he prospect of a company like Clearview being immune from a regulation such as BIPA is alarming" and that "courts should analyze potential *systemic effects* of the activity in question" and their relation to First Amendment values when considering whether such activities are protected under the First Amendment.[225] It is certainly true that many of the foundational First Amendment cases involved the historical values of the

218. Hill, *supra* note 7.

219. *E.g.*, Dawn C. Nunziato, *The Death of the Public Forum in Cyberspace*, 20 BERKELEY TECH. L.J. 1115, 1117 (2005); *see also* Beth Simone Noveck, *Designing Deliberative Democracy in Cyberspace: The Role of the Cyber-Lawyer*, 9 B.U. J. SCI. & TECH. L. 1, 25 (2003) ("[T]he Public Forum Doctrine cannot be applied in cyberspace because there is no public space.").

220. VALERIE C. BRANNON, CONG. RSCH. SERV., R45650, FREE SPEECH AND THE REGULATION OF SOCIAL MEDIA CONTENT 1 (2019).

221. Katz v. United States, 389 U.S. 347, 351 (1967).

222. *Cf.* Pruneyard Shopping Ctr. v. Robins, 447 U.S. 74, 87–88 (1980) (holding that once a shopping mall open its door to the public, it could not deny people the ability to exercise their free speech rights at the mall).

223. Fla. Star v. B.J.F., 491 U.S. 524, 535 (1989).

224. *See generally, e.g.*, Lucas Evans, *Uncovered: Facial Recognition and a Systemic Effects Approach to First Amendment Coverage*, 6 GEO. L. TECH. REV. (forthcoming 2022) (characterizing traditional tests as "unsatisfying" for determining First Amendment coverage of technology as speech and calling for a different assessment).

225. *Id.* (manuscript at 16).

First Amendment—the dissemination of information regarding public significance and the prioritization of the discovery of truth.[226] Indeed, the obvious difference between Clearview's constitutional claims and those in *Cox Broadcasting Corp.* and *Florida Star* is that Clearview is not a member of the press. But even if courts were to adopt a different standard in analyzing whether technologically enhanced conduct constitutes speech, Clearview would likely still survive such an analysis because Clearview's technologies serve, in many ways, the same function of the press that qualifies their dissemination of information as speech.

Clearview has a strong argument that its collection and use of faceprints is a matter of public significance. The public has an interest, "secured by the Constitution, in the dissemination of truth."[227] And the public has a "right to know about matters of general concern," which sometimes must trump an individual's privacy right.[228] The Court has recognized that the investigations of crimes are "matter[s] of paramount public import."[229] Clearview's stated mission is just that: to facilitate law enforcements' abilities to "investigate crimes, enhance public safety, and provide justice to victims."[230] The use of facial recognition has already made a "significant impact" on law enforcement's "fight against the growing crime of online child sexual abuse."[231] After the January 6 Capitol riot, which President Biden said "posed an existential crisis and a test of whether our democracy could survive,"[232] Clearview's application was used to identify potential rioters.[233] Following Clearview's success in identifying rioters, Clearview began "slowly winning people over."[234]

Arguing that Clearview's First Amendment claims are a "lost cause" fails to account for the public interest in the matters that Clearview's application facilitates and the reality that the Court is turning to a deregulatory approach to free speech.[235] Daniel Levin, for example, argues that Clearview does not meet the threshold to constitute a matter of public concern because Clearview is "primarily motivated to profit" and its data

226. *See supra* notes 204–09, 215–17 and accompanying text.

227. *Fla. Star*, 491 U.S. at 533.

228. *Id.* at 551 (White, J., dissenting) (citing Warren & Brandeis, *supra* note 114).

229. *Id.* at 536–37 (majority opinion).

230. *Company Overview*, *supra* note 44.

231. Johann Hofmann, *How Facial Recognition Is Helping Fight Child Sexual Abuse*, BIOMETRIC TECH. TODAY, Mar. 2020, at 7, 8.

232. Statement on the Six-Month Anniversary of the Insurrection on the United States Capitol, 2021 DAILY COMP. PRES. DOC. 1 (July 6, 2021), https://www.govinfo.gov/content/pkg/DCPD-202100566/pdf/DCPD-202100566.pdf [https://perma.cc/DC2Q-3FRT].

233. Hill, *supra* note 9.

234. Hill, *Your Face Is Not Your Own*, *supra* note 50 (quoting Hoan Ton-That, Clearview's chief executive officer).

235. *But cf.* Levin, *supra* note 12, at 1062–63 (arguing that *Sorrell*'s breadth is "overstated").

collection is "indiscriminate.[236] But most newspapers are for-profit ventures,[237] and that has never implicated the significance they have in disseminating information or the First Amendment protection they receive.[238] Indeed, the Supreme Court has held that the sale of information is nevertheless disclosure of information, a restriction on which is a regulation of speech.[239]

Moreover, when weighing privacy interests, the Court in *Sorrell v. IMS Health Inc.* rejected the argument that the state should be able to regulate the collection and analysis of data because it "makes people 'anxious.'"[240] This argument, the Court said, was "contrary to basic First Amendment principles," as "[s]peech remains protected even when it may 'stir people to action,' 'move them to tears,' or 'inflict great pain.'"[241] Thus, even if Clearview's collection of our photos makes us uncomfortable, that's not sufficient to deprive Clearview of First Amendment protection. Perhaps when the question ultimately works its way through the courts, the Supreme Court will revisit the breadth of First Amendment protections, but, until then, legislatures ought to be mindful in drafting regulations to withstand a heightened scrutiny.

IV. An Evaluation of Current Regulations and Recommendations

A. BIPA as a Case Illustration

United States privacy law is a "patchwork" of federal regulations, state-by-state legislation, and common-law torts.[242] There is currently no federal framework specifically directed at FRT use.[243] However, there are state statutes that regulate the collection and use of biometric data.[244] The Illinois

236. *Id.* at 1054.

237. Christian Trejbal, *Nonprofit Newspapers Might Be One Path to Sustainability*, SEATTLE TIMES (Aug. 14, 2021, 1:12 PM), https://www.seattletimes.com/opinion/nonprofit-newspapers-might-be-one-path-to-sustainability/ [https://perma.cc/LH78-JC2G].

238. *See, e.g.*, Neb. Press Ass'n v. Stuart, 427 U.S. 539, 559–60 (1976) (noting the "extraordinary protections afforded by the First Amendment" to the press); Cox Broad. Corp. v. Cohn, 420 U.S. 469, 495 (1975) ("[T]he First and Fourteenth Amendments command nothing less than that the States may not impose sanctions on the publication of truthful information . . . .").

239. *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 568 (2011) ("An individual's right to speak is implicated when information he or she possesses is subjected to 'restraints on the way in which the information might be used' or disseminated." (quoting Seattle Times Co. v. Rhinehart, 467 U.S. 20, 32 (1984))).

240. *Id.* at 576.

241. *Id.* (quoting Snyder v. Phelps, 562 U.S. 433, 460–61 (2011)).

242. Tsesis, *supra* note 63, at 1601.

243. SANTAMARIA, *supra* note 18, at 7.

244. Currently, Illinois, Texas, and Washington have enacted biometric laws. Molly S. DiRago, Kim Phan, Ronald I. Raether Jr. & Robyn W. Lin, *A Fresh "Face" of Privacy: 2022 Biometric*

Biometric Information Privacy Act (BIPA) is the most commonly cited state law addressing FRT,[245] which provides a test case for regulating the collection and use of faceprints.

Enacted in 2008, BIPA regulates private entities' abilities to collect people's biometric identifiers or biometric information.[246] The statute defines a "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" and defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[247] BIPA requires private entities that possess biometric identifiers or information to develop written policies, available to the public, that establish retention schedules and guidelines for destroying the data.[248] BIPA also imposes notice and consent requirements for the collection of biometric identifiers and information.[249] Significantly, BIPA prohibits private entities from "sell[ing], leas[ing], trad[ing], or otherwise profit[ing] from a person's or a customer's biometric identifier or biometric information."[250] Clearview's business model is a clear violation of BIPA.

The ACLU challenged Clearview's application under BIPA in March 2020, seeking to "remedy an extraordinary and unprecedented violation of Illinois residents' privacy rights" and "to put a stop to its unlawful surreptitious capture and storage of millions of Illinoisans' sensitive biometric identifiers."[251] Although the trial court agreed that Clearview's actions were "entitled to some First Amendment protection," it recognized that "[t]hat does not end the inquiry" and "[t]o determine whether a law violates the First Amendment, the Court must first decide what level of scrutiny to apply."[252] Clearview argued that BIPA should be subject to strict scrutiny because it imposes a content-based regulation of speech.[253] The ACLU, on the other hand, argued that intermediate scrutiny should apply

Laws, TROUTMAN PEPPER 1 (Apr. 5, 2022), https://www.troutman.com/print/content/54394/A-Fresh-Face-of-Privacy-2022-Biometric-Laws.pdf?q=render_mode=pdf [https://perma.cc/34WC-Y53U]. California, Kentucky, Maine, Maryland, Massachusetts, Missouri, and New York have all introduced biometric laws. *Id.*

245. *See id.* (discussing how no fewer than seven states have introduced laws based on BIPA).

246. 740 ILL. COMP. STAT. ANN. 14/15(b) (West 2008).

247. *Id.* 14/10.

248. *Id.* 14/15(a).

249. *Id.* 14/15(b).

250. *Id.* 14/15(c).

251. Complaint at 1, ACLU v. Clearview AI, Inc., No. 2020 CH 04353, 2021 Ill. Cir. LEXIS 292 (Ill. Cir. Ct. May. 28, 2020).

252. ACLU v. Clearview AI, Inc., No. 2020 CH 4353, 9 (Ill. Cir. Ct. Aug. 27, 2021).

253. *Id.*

"because it [BIPA] is a content-neutral regulation that only incidentally burdens speech."[254]

Clearview's argument that BIPA should be subject to strict scrutiny was two-fold. First, Clearview argued that BIPA is content-based because it targets specific content—biometric information—and not other content, such as photos.[255] The court rejected this argument, saying this distinction is one between the types of media, not their content.[256] Second, Clearview argued that BIPA is content-based because it makes a speaker-based distinction between private entities, which are prohibited from using faceprints, and public entities, which are exempt from the statute.[257] The court rejected this argument, relying on *Sorrell*, stating that "[s]peaker-based distinction should lead to strict scrutiny *only if* those exemptions are hiding content- or viewpoint-based preferences."[258] The court instead held that BIPA imposes "content-neutral time, place or manner restrictions" and, as such, ought to be subject to intermediate scrutiny.[259]

In applying intermediate scrutiny, the court held that "BIPA's restrictions on Clearview's First Amendment freedoms are no greater than what's essential to further Illinois' interest in protecting its citizens' privacy and security" and denied Clearview's motion to dismiss.[260] But how the court got there may be at odds with current First Amendment jurisprudence.[261] For one, the Supreme Court "tends to favor an audience's right to access, receive, and obtain information."[262] And as discussed in subpart III(B), the Court is moving further away from *Central Hudson*'s relaxed intermediate scrutiny standard towards the application of strict scrutiny, as was the case in *Sorrell*.[263] For now, the applicable standard remains an open question, as the case between the ACLU and Clearview settled on May 9, 2022.[264]

254. *Id.*

255. *Id.*

256. *Id.*

257. *Id.* (emphasizing that the law exempts any "subcontractor, contractor, or agent of a State agency") (internal quotation marks omitted) (quoting 740 ILL. COMP. STAT. ANN. 14/25(e) (West 2008)).

258. *Id.* (emphasis added).

259. *Id.*

260. *Id.* at 12.

261. *See supra* subparts III(B)–(C).

262. Tsesis, *supra* note 63, at 1588.

263. Hans, *supra* note 17, at 29.

264. John C. Cleary, Dmitry Shifrin & Catherine A. Green, *Facial Recognition: Clearview-ACLU Settlement Charts a New Path for BIPA and the First Amendment*, NAT'L. L. REV. (May 12, 2022), https://www.natlawreview.com/article/facial-recognition-clearview-aclu-settlement-charts-new-path-bipa-and-first [https://perma.cc/6FZC-BWGP].

B. Recommendations on How to Regulate the Use of Facial Recognition Technology

Complete bans on FRT use not only raise constitutional concerns but would also deprive law enforcement agencies of an important tool. In 2020, as a part of legislation regulating police surveillance technology, Oakland and San Francisco, California, and Somerville, Massachusetts, all banned the government's use of FRT.[265] Yet the best FRT is even more accurate than humans at matching images.[266] An open letter to Congress signed by a coalition of thirty-nine law enforcement and technology groups warned that these bans would "mak[e] it harder for them to do their jobs efficiently, stay safe, and protect our communities."[267] But there is a middle ground. As opposed to prohibiting the scraping and use of publicly available images (like BIPA), states can regulate FRT use in a way that would allow law enforcement agencies to continue to use the technology while still maintaining privacy interests, addressing accuracy and security concerns, and minimizing potential abuse of FRT. Five examples, discussed below, include (1) implementing accuracy testing requirements before engaging an FRT vendor; (2) establishing security testing before engaging an FRT vendor; (3) establishing reporting requirements and procedures; (4) requiring reasonable suspicion for conducting searches; and (5) enacting proactive legislation prohibiting suspect FRT use.

1. Implementing Accuracy Testing Requirements Before Engaging an FRT Vendor.—A major concern with FRT use in policing is inaccuracy and the risk for misidentification. Although FRT has always been "highly accurate" when identifying white men, it was historically less accurate in identifying transgender and non-binary people and people of color, especially women of color.[268] This discrepancy likely arose because early algorithms were often trained with datasets primarily made up of white men.[269] Organizations like the ACLU are concerned that police use of FRT "pos[es] a particular threat to communities already unjustly targeted in the current

265. Elizabeth A. Rowe, *Regulating Facial Recognition Technology in the Private Sector*, 24 STAN. TECH. L. REV. 1, 43 (2020).

266. James A. Lewis & William Crumpler, *Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape*, CTR. FOR STRATEGIC & INT'L STUD. 1 (2021).

267. Melissa Hellmann, *Tech and Police Groups Urge Lawmakers to Not Ban Facial-Recognition Technology*, SEATTLE TIMES, https://www.seattletimes.com/business/technology/tech-and-police-groups-urge-lawmakers-not-to-ban-facial-recognition/ [https://perma.cc/9G5B-C5MN] (Sept. 28, 2019, 10:24 AM).

268. Ker, *supra* note 75. FRT is around 99% accurate when identifying white men. *Id.*

269. Laura Feiner & Annie Palmer, *Rules Around Facial Recognition and Policing Remain Blurry*, CNBC, https://www.cnbc.com/2021/06/12/a-year-later-tech-companies-calls-to-regulate-facial-recognition-met-with-little-progress.html [https://perma.cc/FJ35-R4DK] (June 14, 2021, 10:52 AM).

political climate"[270] and that FRT use could lead to disproportionately high false arrest rates among people of color.[271] However, Clearview was recently subjected to two rounds of federal testing in October 2021 to determine which AI tools were the most accurate.[272] Clearview was among the top ten most accurate of nearly one-hundred FRT vendors.[273] Because 70% of wrongful convictions result from eyewitness lineups, accurate FRT could actually mitigate biased policing[274] because AI technology can be more accurate than the human eye.[275]

The National Institute of Standards and Technology (NIST) is a federal agency that administers Face Recognition Vendor Tests every few months.[276] NIST has been administering tests for two decades, but participation in the testing is voluntary, and testing is not required for government agencies to purchase the technology.[277] Although Clearview scored comparatively well in the testing, it was the first time the company used a third party to test its accuracy, and thousands of agencies had been using Clearview for years before any third-party testing was conducted.[278] Instead of allowing agencies to sign up for free trials of FRT services, states should evaluate the algorithms before using them. In particular, evaluations must include a determination of the discrepancy in the identification of different races, as well as of transgender and nonbinary people, to account for the high accuracy rates in identifying white men.[279] Enacting an approval process for both state and local authorities would allow the state to ensure departments are following these guidelines and requirements.[280] The Seattle Police Department, for

270. Cagle & Ozer, *supra* note 111.

271. Ker, *supra* note 75 ("[T]he inordinately negative effect that the technology has on African Americans and other communities of color is only being further entrenched as adoption of the technology races ahead with minimal accountability.").

272. Kashmir Hill, *Clearview AI Does Well in Another Round of Facial Recognition Accuracy Tests.*, N.Y. TIMES (Nov. 23, 2021), https://www.nytimes.com/2021/11/23/technology/clearview-ai-facial-recognition-accuracy.html [https://perma.cc/2XKY-THMS].

273. *Id.*

274. Thomas Brewster, *A "Threat to Black Communities": Senators Call on Immigration Cops and FBI to Quit Using Clearview Facial Recognition*, FORBES (Feb. 9, 2022, 8:00 AM), https://www.forbes.com/sites/thomasbrewster/2022/02/09/a-threat-to-black-communities-senators-call-on-immigration-cops-and-fbi-to-quit-using-clearview-facial-recognition/?sh=3cd73f196d06 [https://perma.cc/9ES6-3SMP].

275. Lewis & Crumpler, *supra* note 266 at 1.

276. Kashmir Hill, *Clearview AI Finally Takes Part in a Federal Accuracy Test.*, N.Y. TIMES (Oct. 28, 2021), https://www.nytimes.com/2021/10/28/technology/clearview-ai-test.html [https://perma.cc/74FV-AMAD].

277. *Id.*

278. Hill, *supra* note 272.

279. *See supra* notes 268–69 and accompanying text.

280. *See* Lewis & Crumpler, *supra* note 266, at 5 ("Arizona's proposed legislation on surveillance technologies is the only current example of a bill that would mandate this approval process for both state and local authorities.").

example, requires a 96% accuracy rate before using any FRT algorithm.[281] Ensuring accuracy in FRT services also mitigates some of the unease the public feels towards the police use of FRT.

2. Establishing Security Testing Before Engaging an FRT Vendor.—In addition to testing the accuracy of FRT vendors, FRT programs' security should be tested as well to minimize the risk of data breaches. There are valid concerns that FRT security systems are not "sufficiently regulated" and that law enforcement agencies are "misplacing trust in vendors, for whom public safety and cybersecurity may not be a primary concern[]."[282] In 2019, for example, the U.S. Customs and Border Protection agency announced that a database of photo IDs managed by a subcontractor had been hacked.[283] The year prior, India's biometric system was hacked.[284] To prevent these kinds of breaches, state legislatures should impose security requirements and regular testing.

Another way to ensure the security of FRT software is to limit its access and use. In Russia, for instance, corrupt officials sell access to law enforcement's real-time surveillance footage on the black market.[285] This can be prevented both by limiting the number of organizations that have access to FRT and limiting the number of individuals who are authorized to run searches. If an agency wanted to conduct a search, they would need to submit a request with one of the few authorized operators.[286] Massachusetts and Utah have both taken this approach, requiring all local police departments to produce written requests to state agencies which then determine whether to conduct the search on the local department's behalf.[287]

3. Establishing Reporting Requirements and Procedures.—Not only should there be accuracy and security requirements for engaging FRT vendors, but once FRT is in use, states should also impose reporting requirements to continue to monitor the use, success, and risks of FRT. Many agencies don't currently keep track of how many arrests are made or searches

281. Steve Miletich, *Seattle Police Win Praise for Safeguards with Facial-Recognition Software*, SEATTLE TIMES, https://www.seattletimes.com/seattle-news/law-justice/seattle-police-wins-praise-for-safeguards-with-facial-recognition-software/ [https://perma.cc/38JB-8GGR] (Oct. 19, 2016, 7:10 PM).

282. Ker, *supra* note 75 (quoting Electronic Frontier Foundation's Davis Maass).

283. DJ Pangburn, *Due to Weak Oversight, We Don't Really Know How Tech Companies Are Using Facial Recognition Data*, FAST CO. (July 5, 2019), https://www.fastcompany.com/90372734/due-to-weak-oversight-we-dont-really-know-how-tech-companies-are-using-facial-recognition-data [https://perma.cc/UAV7-AVDP].

284. *Id.*

285. *See supra* notes 93–95 and accompanying text.

286. Lewis & Crumpler, *supra* note 266, at 5.

287. *Id.*

run,[288] and unless reporting requirements are implemented, we may never know. The Seattle Police Department, on the other hand, has received praise for "some of the best safeguards and practices in their use of facial-recognition technology."[289] It's also one of the few departments that has any kind of regulation requirements.[290] Working with the ACLU of Washington, the department developed a policy that allows it to use FRT—but with limitations.[291] The city conducts regular auditing and publishes information about its FRT program online.[292] Reporting not only helps identify potential flaws or concerns about FRT use, but it also assists in bettering the public perception of and combatting misinformation about FRT. Many of the concerns about the accuracy of FRT, for example, are based on old data and old technology.[293] As seen in Clearview's federal testing results, the software is rather accurate and does not suffer from the racial biases some of the earlier FRTs did.[294] Making reporting available to the public would help combat the level of confusion and misinformation surrounding the discussion of FRT[295] and shine some light on the otherwise dark watchperson in the panopticon problem of FRT use.

4. Requiring Reasonable Suspicion for Searches.—Another concern about FRT use is that many agencies do not yet have regulations in place as to what images agents can submit to algorithms to generate leads.[296] In contrast to the traditional requirement for reasonable suspicion of guilt that law enforcement usually needs to obtain a warrant for surveillance, an FRT search scans publicly available images regardless of whether the pictured person is a suspect.[297] Law enforcement agencies across the country "can—and do—submit all manner of 'probe photos,'" which are test images used

288. Garvie, *supra* note 106.

289. Miletich, *supra* note 281.

290. *Id.*

291. Rowe, *supra* note 265, at 44.

292. Miletich, *supra* note 281.

293. Lewis & Crumpler, *supra* note 266, at 1.

294. *See* Hill, *supra* note 272 (reporting that "accuracy of the tool is no longer a prime concern"); *see also* Lewis & Crumpler, *supra* note 266, at 1 (arguing that "[c]laims about FRT inaccuracy are either out of date or mistakenly talking about facial characterization").

295. *See* Lewis & Crumpler, *supra* note 266, at 2 ("Transparency requirements could include annual reporting, public consultation, and making information publicly available on how FRT is being used.").

296. Garvie, *supra* note 106.

297. Ker, *supra* note 75. This phenomenon has been labeled the perpetual lineup. *E.g.*, *id.*; Clare Garvie, Alvaro M. Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIV. & TECH. 8 (Oct. 18, 2016), https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf [https://perma.cc/D8TF-BSMC].

for matching purposes.[298] Records from police departments also show they have used computer-generated facial features or police sketches in FRT searches.[299]

In one case, the New York Police Department ran an FRT search of a grainy photo from a surveillance video of a man stealing beer, which produced no search results.[300] The officer thought the suspect in the grainy photo resembled Woody Harrelson.[301] So the officer resorted to a "'celebrity comparison' technique" and ran an FRT search of a photo of Woody Harrelson—not in search of Woody Harrelson but of Woody Harrelson's doppelgänger.[302] The police found a match, and the doppelgänger was arrested for petit larceny.[303] Police reliance on these "questionable" FRT techniques "appears all too common."[304] These techniques give rise to the "garbage in, garbage out" issue: when you input low-quality or nonsensical data into a system, it will produce low-quality or nonsensical results.[305] But these techniques are avoidable.

State regulations can—and should—be crafted to ensure that FRT is only used in a manner that is consistent with civil liberties and civil rights.[306] In Seattle, for example, the police department can only run a search if they have a "reasonable suspicion" that the person pictured committed a crime.[307] Legislation can clarify when a warrant is required for FRT use and create procedures that dictate when an FRT search is appropriate and for what purposes. Massachusetts, for example, imposes judicial oversight of FRT use by requiring law enforcement officers to obtain a warrant or court order before running an FRT search.[308] Kentucky and Louisiana are both considering similar legislation.[309]

5. Enacting Proactive Legislation Prohibiting Suspect FRT Uses.— Another vehicle to limiting FRT use that states are pursuing is to proactively restrict the scope of FRT uses. While it is impossible to predict all technology

298. Garvie, *supra* note 106.

299. *Id.* ("At least half a dozen police departments across the country permit, if not encourage, the use of face recognition searches on forensic sketches . . . .").

300. *Id.*

301. *Id.*

302. *Id.*

303. *Id.*

304. *Id.*

305. *Id.*

306. Lewis & Crumpler, *supra* note 266, at 2.

307. Miletich, *supra* note 281.

308. Lewis & Crumpler, *supra* note 266, at 5.

309. *Id.* This can, of course, also be done at the federal level for federal agencies. *Id.* Two bills were introduced in the 116th Congress that proposed warrant requirements for FRT searches for federal law enforcement. *Id.*

advancements, we can look to other countries' FRT uses to identify what makes us uncomfortable and attempt to proactively prohibit such uses, such as real-time tracking, lock-down enforcement, or targeting of political dissenters.[310] Examples of proactive FRT legislation include the California legislature's ban on the use of facial recognition software in body cameras, even though no law enforcement agency in California uses such technology.[311] Similarly, the Seattle Police Department began using FRT in 2014,[312] but one safeguard is that the software can never be used for real-time tracking.[313] In New York, a proposed bill would require court authorization for any state agency or contractor to retain images or share those images with third parties.[314]

Proponents of this kind of "proactive legislation" hope that it will allow the government to keep up with the pace of rapid technological developments.[315] In some technology sectors, it could very well be successful. But in areas like FRT, these regulations run the risk of facing heightened scrutiny because of their impact on First Amendment rights.[316] The problem is that when you have First Amendment heightened scrutiny at play, as discussed in Part III, there needs to be a more substantial justification for the restrictive legislation. But proactive legislation doesn't have a definite injury yet—that's the whole point of being proactive.[317] While a predictive harm would survive rational basis review, it certainly wouldn't survive strict scrutiny—and likely not even intermediate heightened scrutiny.[318] Many may find the idea of proactive legislation comforting as an attempt to prevent the use of FRT similar to that of the Russian and Chinese governments from ever happening in the United States. But in practice, proactive legislation in the First Amendment realm will not survive. While challenges to newly adopted or proposed legislation have not yet come from this angle, they surely will. But that isn't to say the fear of impending surveillance can't be mitigated. Regular reporting and monitoring, as discussed in section IV(B)(3) is essential. And unlike proactive legislation, requiring a warrant for a search, as discussed in section IV(B)(4), can be justified by the concrete injury of

310. For a discussion of FRT use by the Chinese and Russian governments, see *supra* subpart II(A) and notes 1–6 and accompanying text.

311. Rowe, *supra* note 291, at 42–43.

312. Miletich, *supra* note 281.

313. Rowe, *supra* note 291, at 44.

314. Lewis & Crumpler, *supra* note 266, at 5.

315. Stuart Minor Benjamin, *Proactive Legislation and the First Amendment*, 99 MICH. L. REV. 281, 282 (2000).

316. *See id.* at 286 ("When a legislature acts specifically against a speech-manipulation activity or company, its action likely will, and should, raise serious First Amendment concerns.").

317. *See id.* at 289 (noting that "predictive harms" lack a "weighty justification").

318. *See id.* 288–90 (discussing the inability of predictive harms to satisfy the "more serious threshold" of heightened scrutiny).

being warrantlessly searched. By focusing on concrete injuries to civil rights and liberties, states *can* constitutionally regulate FRT use.

Conclusion

How to regulate the commercial use of private information posted publicly online is "[o]ne of the most complex puzzles in constitutional law."[319] And Clearview has come under attack by fellow vendors who worry that the controversy surrounding Clearview "will cause problems for the facial recognition industry as a whole."[320] Even Clearview says it would "welcome federal regulation" to allow for its "legitimate use and [to] prevent abuse," in hopes that such regulation would "unravel the tangle of sometimes inconsistent and unconstitutional state and local laws."[321] As demonstrated by *ACLU v. Clearview AI, Inc.*, there are currently debates in the legal community over whether privacy laws should fall into content-based regulations classifications[322] and which level of scrutiny to apply to restrictions on the collection and analysis of data.[323] The answer to this question will likely depend on the specific provisions of the law at issue,[324] which legislatures can be mindful of as they draft privacy regulations. Although the freedom of speech is fundamental, it is not absolute.[325] And even if laws regulating the use of FRT are content-based regulations, it is possible to satisfy strict scrutiny.[326] Chances are, a privacy statute will come before the Court in the near future,[327] and legislatures should craft their regulations in a way that can withstand a strict scrutiny application. As Vice President of Artificial Intelligence at Meta, Jerome Pesenti, said concerning facial recognition, "every new technology brings with it potential for both

319. Tsesis, *supra* note 63, at 1586.

320. Hill, *supra* note 276.

321. Abrams & Wolosky, *supra* note 84.

322. *See, e.g.*, Hans, *supra* note 17, at 23 (arguing that privacy laws "should not automatically fall into the category of content-based regulations"); Volokh, *supra* note 193, at 1051 (arguing that "information privacy rules are not easily defensible under existing free speech law").

323. *See, e.g.*, Tsesis, *supra* note 63, at 1620 (accepting "monitoring technologies" as commercial speech and arguing that "intermediate scrutiny should enable courts to balance the interests of government and [the] private party").

324. Hans, *supra* note 17, at 22–23.

325. Whitney v. California, 274 U.S. 357, 371 (1927).

326. *See* Hans, *supra* note 17, at 23 (arguing that even if privacy laws automatically fell into the category of content-based regulations, "it would be possible to satisfy strict scrutiny").

327. *Id.* at 39.

benefit and concern, and we want to find the right balance."[328] By narrowly tailoring the compelling interests of regulating FRT use in their policies, as demonstrated above, states can craft legislation and implement regulations that take into account both the First Amendment and privacy interests implicated in FRT use.

328. Kashmir Hill & Ryan Mac, *Facebook, Citing Societal Concerns, Plans to Shut Down Facial Recognition System*, N.Y. TIMES, https://www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.html [https://perma.cc/7MPS-76YX] (Nov. 5, 2021) (internal quotation marks omitted).