Loyola of Los Angeles Law Review

Volume 55 | Number 1 Article 6

Spring 2-17-2022

The First Amendment and Facial Recognition Technology

Katja Kukielski

THE FIRST AMENDMENT AND FACIAL RECOGNITION TECHNOLOGY

Katja Kukielski∗

As technology companies increase their deployment of facial recognition technology (FRT), consumers have begun to rebuff attempts to collect, use, and sell facial recognition data without restraint. The California Consumer Privacy Act (CCPA) and Privacy Rights and Enforcement Act (CPRA) constitute one such effort. However, consistent with an increasingly deregulatory view of the First Amendment taken by the United States Supreme Court over the past decade or so, commercial actors—including now-notorious Clearview AI—have begun to argue that regulation of FRT is incompatible with the First Amendment.

This Note pushes back against the notion that there is inherent tension between protecting consumers from unrestrained use of FRT and preserving free speech. Instead, this Note considers the free speech interests at stake during the three main phases of FRT data processing—collection, use, and disclosure—to determine whether a legislature may constitutionally regulate these activities. This Note concludes that the data collection phase is most appropriately analyzed as a form of information-gathering, while companies' use of the data could be comfortably regulated as a content-neutral law protecting consumers' reasonable expectations. While regulation at the disclosure phase presents greater free speech concerns, such regulation should be permissible when the disclosure does not contribute meaningfully to the purposes behind the First Amendment. Finally, this Note culminates by evaluating California's biometric privacy provisions in its CCPA/CPRA scheme, and provides suggestions as to how it might be altered to more coherently protect against the serious risks posed by FRT while ensuring that it sits comfortably with the First Amendment.

∗ Thanks to my family (three dogs included), friends, professors, and the editors and staff of the *Loyola of Los Angeles Law Review*. Special thanks to Sam, for listening to me talk about this paper for hours on end; to my editor, Alex Murcia, for his thoughtful feedback; and to Professor Rothman, who introduced me to privacy law and the First Amendment, and whose guidance was essential to this project's success.

TABLE OF CONTENTS

Those who already walk submissively will say there is no cause for alarm. But submissiveness is not our heritage.

– Justice William O. Douglas[1]

When the *New York Times* published an exposé on then-nascent technology company Clearview AI in January of 2020, many were shocked and concerned to find that the company was scraping the internet for photographs for use in its facial recognition app.[2] The app allows users to match photos they input with those that exist on the internet.[3] After the story came out, U.S. senators pressured the company to reconsider its activities domestically and abroad.[4] Plaintiffs in five states filed more than a dozen different lawsuits—including putative class actions.[5] While some plaintiffs had posted their photographs on public social media accounts, they were disturbed to find Clearview had indexed their photos for use in its app—enabling anyone to snap a photograph of them, input that photo into the app, and instantaneously identify them.[6] Although they had consensually shared their images with the general public, they had not contemplated that Clearview would use photos to create facial templates—or "faceprints"—that would then be integrated into a vast database of searchable images.[7] More concerning were instances in which Clearview used photos that were posted by others without the plaintiffs' knowledge or permission.[8] Such an app raises the chilling prospect that it could be used to identify people at protests, political rallies, abortion clinics, and

1. Laird v. Tatum, 408 U.S. 1, 28 (1972) (Douglas, J., dissenting).

2. *See* Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, N.Y. TIMES (Mar. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/CL4F-FY9G].

3. *Id.*

4. Ryan Mac et al., *Senators Are Probing Clearview AI on the Use of Facial Recognition by Gulf States and International Markets*, BUZZFEED NEWS (Mar. 4, 2020, 3:58 PM) https://www.buzzfeednews.com/article/ryanmac/senators-markey-wyden-clearview-ai-facial-recognition [https://perma.cc/87PB-XZKL].

5. Jessica Conditt, *Clearview to Rely on First Amendment to Defend Its Face-Tracking Tech*, ENGADGET (Aug. 11, 2020), https://www.engadget.com/clearview-first-amendment-lawsuit-defense-181859840.html [https://perma.cc/PA2G-WXGX]; *see* Complaint at 3–7, Renderos v. Clearview AI, Inc., No. RG21091138 (Cal. Super. Ct. Mar. 9, 2021).

6. *See* Complaint at 2–4, Broccolino v. Clearview AI, Inc., No. 20-cv-02222 (S.D.N.Y. Mar. 13, 2020).

7. *See* Complaint at 15–16, Marron v. Clearview AI, Inc., No. 20-cv-02989 (N.D. Ill. May 20, 2020).

8. *See id.*

Alcoholics Anonymous meetings.[9] These concerns have already become a reality in Hong Kong, where protesters have had to hide their faces to avoid recognition,[10] and in China, which employs an extensive network of surveillance cameras as part of its social credit system.[11]

In response to these lawsuits, Clearview raised several defenses. It has argued that Illinois's Biometric Information Privacy Act[12]—the statute under which many plaintiffs sued—does not apply to photographs.[13] It has also asserted that the federal Communications Decency Act, which protects online service providers from liability for certain material that appears on their platforms,[14] immunizes the company.[15] However, one defense may prove most difficult for the plaintiffs to overcome: the First Amendment.

The First Amendment arguments raised by the technology company are nothing new in data and informational privacy conversations.[16] Because of the First Amendment, courts have invalidated laws restricting use of medical information by pharmaceutical marketers,[17] laws aimed at shielding the identity of rape victims from widespread publication,[18] and a Federal Communications Commission order that

9. *See* Complaint at 2, ACLU v. Clearview AI, Inc., No. 2020CH04353 (Ill. Cir. Ct. May 28, 2020).

10. Trey Smith, *In Hong Kong, Protestors Fight to Stay Anonymous*, THE VERGE (Oct. 22, 2019, 10:03 AM), https://www.theverge.com/2019/10/22/20926585/hong-kong-china-protest-mask-umbrella-anonymous-surveillance [https://perma.cc/MX6A-93GC].

11. Alfred Ng, *How China Uses Facial Recognition to Control Human Behavior*, CNET (Aug. 11, 2020, 5:00 AM), https://www.cnet.com/news/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/ [https://perma.cc/KBY9-UJY4]. Interestingly, though many protest the government's deployment of facial recognition technology, some groups of Chinese citizens view its surveillance techniques as a positive development. *See* Genia Kostka, *China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval*, 21 NEW MEDIA & SOC'Y 1565, 1569 (2019).

12. 740 ILL. COMP. STAT. 14/1–14/99 (2021).

13. *See* Clearview Defendants' Memorandum of Law in Opposition to Plaintiff's Motion for Preliminary Injunction at 11, Mutnick v. Clearview AI, Inc., No. 20-cv-512 (N.D. Ill. May 6, 2020).

14. 47 U.S.C. § 230 (2018).

15. *See* Defendant's Reply to Vermont's Opposition to Defendant's Motion to Dismiss at 9, Vermont v. Clearview AI, Inc., No. 226-3-20 CNCV (Vt. Super. Ct. May 22, 2020).

16. *Compare* 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"), *and* 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 (2000) (outlining and responding to arguments for why privacy regulations do not violate the First Amendment), *with* Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1512, 1523 (2015) (arguing that "asking 'is data speech?' is a poor way to ask a very important question" and that, consequently, most data privacy laws are constitutional).

17. Sorrell v. IMS Health, Inc., 564 U.S. 552, 580 (2011).

18. Fla. Star v. B.J.F., 491 U.S. 524, 526 (1989).

restricted telecommunications companies from using customers' data to market additional products.[19]

The current expansive view of the First Amendment has worried a number of scholars precisely because it might give a pass to companies like Clearview and make protecting data very, very difficult, if not impossible.[20] While the Supreme Court has not spoken definitively on the question of whether and when data (including faceprints) constitutes speech, it has indicated that it is open to taking an expansive approach.[21] Recent decisions suggest that, unless the Court modifies its currently broad definition of "speech" for purposes of the First Amendment, the Supreme Court is likely to explicitly hold as such in the near future.[22] The most clear-cut—and, to many, worrisome—example of this occurred in *Sorrell v. IMS Health*,[23] in which the Supreme Court struck down as content- and viewpoint-discriminatory a law that prohibited the use of prescriber-identifying information by pharmaceutical companies for marketing purposes—despite the fact that it seemed to some like a clear case of commercial regulation.[24]

Clearview may be one of the most notorious examples of facial recognition technology (FRT) in recent years, but it is not alone. Despite widespread criticism of Clearview's tool, a company called PimEyes has recently launched an identical tool.[25] Unlike

19. U.S. West, Inc. v. Fed. Commc'ns Comm'n, 182 F.3d 1224, 1228 (10th Cir. 1999).

20. *See, e.g.*, Genevieve Lakier, *The First Amendment's Real* Lochner *Problem*, 87 U. CHI. L. REV. 1241, 1242–43 (2020); Nelson Tebbe, *A Democratic Political Economy for the First Amendment*, 105 CORNELL L. REV. 959, 1020 (2020); Amanda Shanor, *The New* Lochner, 2016 WIS. L. REV. 133, 133; Richards, *supra* note 16, at 1526–27; Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1151 (2005); Ashutosh Bhagwat, Sorrell v. IMS Health*: Details, Detailing, and the Death of Privacy*, 36 VT. L. REV. 855, 855 (2012); Margot Kaminski, *Privacy and the Right to Record*, 97 B.U. L. REV. 167, 173 (2017); *see also* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1185–86 (2016) (observing that "the First Amendment has become the most fertile source of constitutional defenses to business regulation"); *Sorrell*, 564 U.S. at 590 (Breyer, J., dissenting) ("If the Court means to create constitutional barriers to regulatory rules that might affect the *content* of a commercial message, it has embarked upon an unprecedent task—a task that threatens significant judicial interference with widely accepted regulatory activity.").

21. *See Sorrell*, 564 U.S. at 570; *see also* Bambauer, *supra* note 16, at 71 ("Justice Kennedy's opinion [in *Sorrell*] very nearly resolved whether data is protected speech.").

22. *See* Ashutosh Bhagwat, *When Speech Is Not "Speech,"* 78 OHIO ST. L.J. 839, 843 (2017) (pushing back against the *Sorrell* court's hint that data may be speech for First Amendment purposes).

23. 564 U.S. 552 (2011).

24. *See id.* at 593 (Breyer, J., dissenting); Richards, *supra* note 16, at 1506.

25. *See* Rachel Metz, *Anyone Can Use This Powerful Facial-Recognition Tool—And That's a Problem*, CNN BUS. (May 4, 2021), https://www.cnn.com/2021/05/04/tech/pimeyes-facial-recognition/index.html [https://perma.cc/7W6Y-QRLS].

Clearview—whose main clients are law enforcement—PimEyes makes its tool available to the general public for free.[26] Companies like Facebook[27] and Shutterfly[28] have been using facial recognition technology to identify the subjects of photographs since at least 2010.[29] Nor are social media platforms the only players. Facial recognition companies like Churchix,[30] FaceFirst, and Ellucian market their tools to schools and other venues for attendance monitoring.[31] Beyond taking attendance, Ellucian touts its technology's ability to monitor facial expressions in real time to detect student engagement and emotional responses to lecture material.[32] In the COVID era of online employment interviews, some employers may also use FRT to determine prospective employees' moods and personality traits.[33] The technology is also being rolled out in commercial and retail contexts to recognize individual customers who enter or (in the virtual world) interact with the business, to send targeted marketing, and to tailor customer experiences.[34] Stores also use these tools to identify undesirable customers, such as shoplifters or people who have otherwise been banned from particular venues.[35]

The growing prevalence of FRT, data collection by large firms, and other intrusive technologies has spawned legislative action to

---

26. *Id.*

27. *See* Patel v. Facebook, Inc., 932 F.3d 1264, 1268 (9th Cir. 2019); *see also* Jonathan Shaw, Comment, *FACEbook Confidential: The Privacy Implications of Facebook's Surreptitious and Exploitative Utilization of Facial Recognition Technology*, 31 TEMP. J. SCI. TECH. & ENV'T L. 149, 151 (2012) (arguing that the Federal Trade Commission should utilize its section 5 authority to enjoin Facebook's use of facial recognition technology).

28. *See* Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015).

29. *See* Camila Domonoske, *Facebook Expands Use of Facial Recognition to ID Users in Photos*, NPR (Dec. 19, 2017, 1:39 PM), https://www.npr.org/sections/thetwo-way/2017/12/19/571954455/facebook-expands-use-of-facial-recognition-to-id-users-in-photos [https://perma.cc/D77C-LF5V].

30. *Facial Recognition Software by Churchix for Biometric Attendance*, CHURCHIX, https://churchix.com [https://perma.cc/HP27-6ZYM].

31. Ronald Bailey, *Ban Facial Recognition on College Campuses, Activists Say*, REASON (Jan. 28, 2020, 4:10 PM), https://reason.com/2020/01/28/ban-facial-recognition-on-college-campuses/ [https://perma.cc/BQ9Q-VAFB].

32. Raja Saravanan, *Facial Recognition Can Give Students Better Service (and Security)*, ELLUCIAN, https://www.ellucian.com/blog/facial-recognition-campus-benefits-security-risks [https://perma.cc/G4EK-4UBB].

33. *See* Minda Zetlin, *AI Is Now Analyzing Candidates' Facial Expressions During Video Job Interviews*, INC. (Feb. 28, 2018), https://www.inc.com/minda-zetlin/ai-is-now-analyzing-candidates-facial-expressions-during-video-job-interviews.html.

34. Sharon Nakar & Dov Greenbaum, *Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy*, 23 B.U. J. SCI. & TECH. L. 88, 99 (2017).

35. *Id.*

protect privacy in many states.[36] For example, Illinois,[37] Texas,[38] and Washington,[39] among other states, now broadly regulate biometric information, including faceprints.[40] In 2018, California joined their ranks when voters passed the sweeping California Consumer Privacy Act[41] (CCPA), followed quickly by the California Privacy Rights Act (CPRA), which regulates faceprints, among other things.[42] Yet, despite the public support for these statutes and public concern regarding this technology, the CCPA's biometric regulations may be struck down if companies like Clearview successfully argue that the First Amendment protects their activities.[43]

Focusing on the use of facial recognition technology by private actors for commercial purposes, this Note will begin by describing the inherent risks. I select the commercial focus for three reasons: First, if limiting FRT in this context is unconstitutional, it is highly unlikely that uses in other contexts—for example, scientific research or investigative journalism—will be regulable. Given the Supreme Court's historically weaker First Amendment protections for commercial speech and similar types of commercial data usage,[44] regulating FRT when it is used for commercial purposes presents the clearest case for constitutionality. Second, limiting this inquiry to private actors eliminates obvious Fourth Amendment problems that would arise with

36. *See* Molly K. McGinley et al., *The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States*, NAT'L L. REV. (Mar. 25, 2019), https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states [https://perma.cc/FCJ6-C3Z6].

37. 740 ILL. COMP. STAT. 14/1–14/99 (2021).

38. TEX. BUS. & COM. CODE ANN. § 503.001 (West 2021).

39. WASH. REV. CODE § 19.375.010 (2021).

40. Various other states regulate facial recognition in more targeted contexts. For example, Florida prohibits public schools from collecting biometric information (including faceprints) of students, parents, or siblings. FLA. STAT. § 1002.222(1)(a) (2014).

41. CAL. CIV. CODE §§ 1798.100–.199 (West Supp. 2021).

42. Dominique-Chantale Alepin, Panel, *Social Media, Right to Privacy and the California Consumer Privacy Act*, 29 COMPETITION: J. ANTITRUST, UCL & PRIV. SEC. CAL. LAWS. ASS'N 96, 97 (2019); Brandon P. Reilly & Scott T. Lashway, *The California Privacy Rights Act has Passed: What's in It?*, MANATT (Nov. 11, 2020), https://www.manatt.com/insights/newsletters/client-alert/the-california-privacy-rights-act-has-passed [https://perma.cc/W8TP-PWW6]. In fact, the CCPA defines (and therefore regulates) personal information quite broadly. *See* CAL. CIV. CODE § 1798.140(v)(1).

43. *See* Margot E. Kaminski & Scott Skinner-Thompson, *Free Speech Isn't a Free Pass for Privacy Violations*, SLATE (Mar. 9, 2020), https://slate.com/technology/2020/03/free-speech-privacy-clearview-ai-maine-isps.html [https://perma.cc/GE2W-DNVG].

44. *See* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 562–63 (1980); Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 758–59 (1985); *see also* Felix T. Wu, *The Commercial Difference*, 58 WM. & MARY L. REV. 2005 (2017) (arguing that commercial and corporate speech rights are derivative of others' primary speech rights).

government use, though, as described below, private and public uses of data are tightly interwoven.[45] Finally, I take this approach because these are the kinds of uses on which states, including California, have chosen to focus their regulatory efforts.[46]

Next, I will consider whether states may restrict businesses' capture, use, and disclosure of citizens' faceprints for commercial purposes without running afoul of the First Amendment. The argument mobilized in favor of the position that FRT regulation is unconstitutional relies on the assertion that facial recognition data, like any other form of information, is speech subject to the full weight of the First Amendment.[47] Under this line of reasoning—which receives some support from dictum in the Supreme Court's opinion in *Sorrell*[48]—facial recognition tools create knowledge and thereby allow users of the technology to act based on the information that the technology provides. However, as I will show below, these arguments—while attractive in the abstract—not only miss the mark under any theory of the First Amendment, but actually endanger the purposes that the First Amendment is designed to further. This Note will therefore push back on the broader argument that faceprints are invariably speech.

Whether faceprints themselves are speech is not the right question to ask; instead, courts should ask whether various regulations present a serious risk to freedom of expression. I will next consider three activities pertaining to FRT—collection, use, and disclosure—to determine whether a legislature may regulate these activities in a manner consistent with the First Amendment. I argue that the collection of faceprints is most appropriately analyzed as a form of information-gathering subject to some level of intermediate scrutiny. I then argue that use restrictions are similarly permissible as content-neutral laws that require companies to act within consumers' reasonable expectations. By contrast, restrictions on data disclosure present a more difficult question because they appear more like traditional conceptions of speech with a speaker, listener, and message. However, when companies sell FRT data for purposes that do not contribute meaningfully to

45. *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1951–52 (2013).

46. *See* CAL. CIV. CODE § 1798.140(d); Joseph J. Lazzarotti et al., *Does the CCPA Apply to Your Business?*, NAT'L L. REV. (Aug. 14, 2019), https://www.natlawreview.com/article/does-ccpa-apply-to-your-business [https://perma.cc/5SAH-YYX4].

47. *See* Richards, *supra* note 16, at 1524; Bambauer, *supra* note 16, at 60.

48. Sorrell v. IMS Health Inc., 564 U.S. 552, 571 (2011).

the purposes behind the First Amendment, regulation on such disclosures should be subject only to some form of intermediate scrutiny.

Finally, I apply this analysis to the CCPA/CPRA's biometrics provisions, making recommendations for how the statute could be altered to more coherently protect against the serious harms raised by FRT while ensuring that it sits comfortably with the First Amendment.

Two notes before we continue: First, this Note presumes that FRT identifies subjects accurately. In the context of commercial use, FRT is dangerous precisely because of the breadth of accurate information it conveys about its subjects.[49] Second, I limit my inquiry to private use of FRT because government use thereof raises a slew of concerns related to the Fourth Amendment right against unreasonable search and seizure.[50] Nonetheless, even if the government's direct deployment of FRT were restricted, one must recall that public and private uses are intertwined.[51] In the current state of Fourth Amendment law, allowing private actors to capture and make use of faceprints means that the government may acquire that data from private actors.[52] Perhaps the most jarring example is that of Clearview. The company has formed institutional arrangements with law enforcement to provide them with information on all citizens (irrespective of suspicion of any

---

49. *See* Bambauer, *supra* note 16, at 66. Additionally, false statements of fact present First Amendment concerns that are beyond the scope of this Note.

50. *See, e.g.*, Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409 (2014); Adriana Bass, Note, *Smile! You're on Camera: Police Departments' Use of Facial Recognition Technology and the Fourth Amendment*, 55 LOY. L.A. L. REV. (forthcoming 2022). These concerns are only exacerbated by the tendency for facial recognition technology to be less accurate when identifying subjects who are not white and male, causing the potential for misidentification and, consequently, false arrests of minorities. Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, WASH. POST (July 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/ [https://perma.cc/C5KN-69UY]. Others worry that even if this bias is eliminated, law enforcement groups might use the technology to target vulnerable populations, such as undocumented immigrants. *Id.*; *see* Kashmir Hill, *Your Face Is Not Your Own*, N.Y. TIMES (Mar. 18, 2021), https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html [https://perma.cc/DAW9-KUBT]. For example, some believe that states have allowed undocumented immigrants to obtain drivers' licenses so that ICE can then use the photographs to create faceprints. *See* Alex Najibi, *Racial Discrimination in Face Recognition Technology*, SCI. IN THE NEWS (Oct. 24, 2020), http://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/ [https://perma.cc/8WSK-9HJY].

51. Richards, *supra* note 45, at 1951–52.

52. *See* Joel R. Reidenberg, *Privacy in Public*, 69 U. MIA. L. REV. 141, 144 (2014); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1431 (2000) [hereinafter Cohen, *Examined Lives*]; Julie E. Cohen, *How (Not) to Write a Privacy Law*, KNIGHT FIRST AMENDMENT INST. AT COLUM. UNIV. (Mar. 23, 2021) [hereinafter Cohen, *How (Not) to Write a Privacy Law*], https://knightcolumbia.org/content/how-not-to-write-a-privacy-law [https://perma.cc/8ZF7-423Y].

one individual) that it likely could not ascertain on its own.[53] Thus, federal and state governments can—and do—contract with private businesses to acquire vast amounts of personal information on ordinary people, effectively outsourcing their surveillance to circumvent direct restrictions on governmental data collection.[54] This phenomenon is not unique to FRT, but it is particularly worrisome given the widespread surveillance enabled by the technology.

I. FACIAL RECOGNITION TECHNOLOGY AND PRIVACY HARMS

Any discussion of facial recognition—or data privacy in general—would be incomplete without a meaningful appreciation of the risks imposed by the technology. Further, embarking on a constitutional analysis will require an identification of the relevant state interests furthered by FRT regulations.

One might argue that FRT is nothing truly new—in some sense, FRT replicates the human capacity to identify faces. Of course, no one would argue that it violates their privacy to be recognized by an acquaintance or even some other person with whom one has an indirect relationship. Critically, however, FRT enhances this ability far beyond ordinary human capacity, allowing companies to instantaneously and accurately identify consumers—even when they think they are alone.[55] FRT can also discern information about a person's age, gender,[56] attention span, and emotional reaction to various stimuli.[57] Accordingly, facial recognition technology allows individuals to be identified and analyzed by entities with whom they may have never interacted. It also enables these activities to occur at great distances and, if surreptitiously captured through the cameras in people's devices, in contexts in which people would reasonably assume they are alone.[58] More insidiously, when it combines information in the

53. Isadora Neroni Rezende, *Facial Recognition in Police Hands: Assessing the 'Clearview Case' from a European Perspective*, 11 NEW J. EUR. CRIM. L. 375, 376 (2020).

54. Richards, *supra* note 20, at 1159.

55. For example, Walgreens and Kroger have installed facial scanners in their stores to determine shoppers' age and gender to deliver targeted ads. Anthony Tacconi, *Walgreens and Kroger Sued for Using Cameras with Facial Recognition*, GOODMAN ALLEN DONNELLY (Oct. 15, 2020, 10:54 AM), https://www.goodmanallen.com/blog/walgreens-and-kroger-sued-for-using-cameras-with-facial-recognition [https://perma.cc/GU2U-5W2Q].

56. *Id.*

57. Andy Lau, *Facial Recognition in Global Marketing*, TOWARDS DATA SCI. (Apr. 25, 2020), https://towardsdatascience.com/facial-recognition-in-global-marketing-8d0ca0b313c7 [https://perma.cc/ECX8-DV77].

58. *See* Nakar & Greenbaum, *supra* note 34, at 96.

aggregate, facial recognition technology can effectively be used to surveil individuals by constructing comprehensive, permanent records of their whereabouts.[59] The Ninth Circuit has formally acknowledged these risks as not only real but also legally cognizable in cases discussing Article III standing—another issue that has plagued courts in data privacy cases.[60] In *Patel v. Facebook, Inc.*,[61] the court addressed the issue of whether plaintiffs whose faceprints had been nonconsensually captured by Facebook had sufficiently demonstrated an injury-in-fact.[62] Holding that they had, the court articulated the problem with Facebook's conduct:

> [T]he facial-recognition technology at issue here can obtain information that is "detailed, encyclopedic, and effortlessly compiled," which would be almost impossible without such technology. Once a face template of an individual is created, Facebook can use it to identify that individual in any of the other hundreds of millions of photos uploaded to Facebook each day, as well as determine when the individual was present at a specific location. Facebook can also identify the individual's Facebook friends or acquaintances who are present in the photo. Taking into account the future development of such technology . . . it seems likely that a face-mapped individual could be identified from a surveillance photo taken on the streets or in an office building.[63]

59. *See id.* at 91.

60. *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms* (Feb. 9, 2021) (GWU Legal Studies Research Paper No. 2021-11), https://ssrn.com/abstract=3782222 [https://perma.cc/H4K8-NQ5V].

61. 932 F.3d 1264 (9th Cir. 2019).

62. *Id.* at 1273. It is worth noting that the Northern District of Illinois has approached the question of injury-in-fact in FRT-based BIPA cases with more skepticism. *See* Rivera v. Google, Inc., 366 F. Supp. 3d 998, 1010–11 (N.D. Ill. 2018). However, in concluding that the plaintiffs had not sufficiently alleged a sufficiently concrete harm, the court expressly based its holding on the fact that the legislative findings had not articulated any specific harms other than the risk of identity theft. *See id.* The court expressly noted that its evaluation might change if the Illinois Legislature updated these findings, observing that "[i]t is not hard to imagine more concrete concerns arising from facial-recognition technology, especially as it becomes more accurate and more widespread (along with video-surveillance cameras) to the point that private entities are able to use the technology to pinpoint where people have been over extended time periods." *Id.* at 1011 n.15.

63. *Patel*, 932 F.3d at 1273.

Based on such capabilities, there are three core harms that private use of accurate FRT can cause: chilling effects,[64] disclosure harms,[65] and loss of autonomy.[66]

First, because FRT can allow for mass surveillance (as exemplified by Clearview), it can cause chilling effects on behavior. While any mass amalgamation of data could in effect chill activities, the risk is particularly salient in the context of FRT both because of the amount of information it can reveal to users of the technology, and because it is extraordinarily difficult to avoid. While one might be able to avoid sharing, for example, an embarrassing video purchase history simply by not purchasing such videos, there is no comparable choice when it comes to showing one's face in public. Even when FRT collects imagery posted publicly on the internet (as Clearview purports to[67]), these photos often collect information about people who never consented to the photo or its publication.[68] Thus, the continuous monitoring of people that FRT enables is distinct from the usual manner in which our activities are visible to those around us.[69] This risk is particularly prominent when FRT data is combined with other forms of information such as location data, past purchases, emails, and internet browsing history.[70] In the aggregate, this enables companies to construct comprehensive records of individuals' daily activities and—to the extent that people's facial expressions[71] and online activities reflect their inner lives—even their thoughts. As Professor Margot Kaminski writes, the architecture of our world—walls, physical distance, forgetfulness over time—generally permits us to make informed choices about what activities to engage in so as to manage our own

64. *See* Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 478 (2015).

65. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 529 (2006).

66. *See* Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 149–50 (2017).

67. Defendant's Memorandum of Law in Support of Its Motion to Dismiss at 1, ACLU v. Clearview AI, Inc., No. 2020CH04353 (Ill. Cir. Ct. Oct. 7, 2020).

68. *See* Metz, *supra* note 25.

69. *See* Solove, *supra* note 65, at 493 ("Certainly, we all watch or listen, even when others may not want us to, and we often do not view this as problematic. However, when done in a certain manner—such as continuous monitoring—surveillance has problematic effects.").

70. For example, Clearview allegedly harvests not only faceprints but also associated metadata, such as time and location information. Thornley v. Clearview AI, Inc., 984 F.3d 1241, 1243 (7th Cir. 2021).

71. *See* Kiely Kuligowski, *Facial Recognition Advertising: The New Way to Target Ads at Consumers*, BUS. NEWS DAILY (Jul. 18, 2019), https://www.businessnewsdaily.com/15213-walgreens-facial-recognition.html [https://perma.cc/9FSG-MRHD].

exposure to others.[72] Of course, sometimes increased transparency can be good: for example, by making sure police officers and other public officials do not abuse their power. Other times, it forecloses people from engaging in socially productive and valuable behaviors, such as checking out a controversial book at a library, seeking appropriate medical care, or attending a religious service.[73]

As Professor Julie E. Cohen argues, these chilling effects threaten activities essential to free speech and innovation—concerns that, paradoxically, feature prominently in arguments opposing data privacy.[74] For example, though some argue that increased data privacy regulations will limit developments in technology, Professor Cohen asserts that surveillance actually hampers innovation because it requires space to experiment and therefore freedom from surveillance.[75] Innovation "thrives most fully when circumstances yield serendipitous encounters with new resources and ideas, and afford the intellectual and material breathing room to experiment with them."[76] Her observations in this respect are supported by a multitude of studies documenting the chilling effect that surveillance has on human behavior.[77] Michel Foucault theorized that surveilled prisoners would conform their behavior in the knowledge that they were being watched.[78] Ultimately, per Foucault, this ingrained expectation would render guards superfluous; as long as the possibility existed that they were being watched, the prisoners would act accordingly.[79] In a more contemporary context, researchers have found that the perceived ubiquity of social networking has caused humans to alter their offline behavior out of concern that their actions will be nonconsensually captured and uploaded to social

72. Kaminski, *supra* note 20, at 171.

73. *See* Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591, 1608 (2017).

74. *See* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1919 (2013).

75. *Id.* at 1918.

76. *Id.* at 1920.

77. *See, e.g.*, Ben Marder et al., *The Extended 'Chilling' Effect of Facebook: The Cold Reality of Ubiquitous Social Networking*, 60 COMPUTS. HUM. BEHAV. 582 (2016); Jonathon W. Penney, *Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study*, INTERNET POL'Y REV., May 2017, at 1; Kaminski & Witnov, *supra* note 64; Dawinder S. Sidhu, *The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans*, 7 U. MD. L.J. RACE, RELIGION, GENDER & CLASS 375 (2007); Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior* (Feb. 17, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564 [https://perma.cc/HMZ8-BWD9]. *See generally* Richards, *supra* note 45, at 1962–64 (describing the dangers of surveillance and proposing suggestions to guide the future development of laws targeting surveillance).

78. Brown, *supra* note 50, at 414.

79. *Id.*; Solove, *supra* note 65, at 495.

networks.[80] Accordingly, because processes of experimentation often involve engaging with controversial or unpopular ideas, and such experimentation is a necessary precursor to innovation and free speech, this chilling effect threatens activities that are vital to our society.[81] This illuminates the flaw in the argument that privacy and free speech are diametrically opposed.[82]

Separately from chilling effects, widespread facial recognition also exacerbates the risk of harmful disclosures that leave people embarrassed or otherwise overly exposed—such as by increasing the risk of identity theft. The more widespread the technology is (and the more secretive), the more likely that such technology will ultimately capture information about a subject that they might prefer others not to know. Sometimes disclosure of this information will lead to a merely dignitary harm—such as if FRT were to catch a person visiting a sex shop. However, it can also allow a user to uncover information about a person's whereabouts or activities that might leave the depicted individual vulnerable to stalking or harassment. In some respects, disclosure harms are related to the harm of chilling effects in that it is generally the risk of such disclosures that cause people to act differently. However, the ultimate disclosure is not necessary to cause chilling effects; the mere risk of disclosure is itself sufficient.[83] Perhaps the most common type of disclosure harm is the heightened risk of identity theft that accompanies data breaches.[84] Unlike credit card information or social security numbers, faceprints cannot realistically be changed. Even if no such theft occurs, people often experience emotional distress and must spend a great deal of time and money to detect and protect against fraudulent activity.[85]

Beyond chilling effects and the risk of disclosure, mass collection of FRT results in a loss in autonomy that is perhaps subtler—but even

80. Marder et al., *supra* note 77, at 585–86.

81. Cohen, *supra* note 74, at 1920; *see also* Richards, *supra* note 45, at 1935 ("Such intellectual surveillance is especially dangerous because it can cause people not to experiment with new, controversial, or deviant ideas.").

82. For a detailed argument to this effect, see NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE (2015). *See also* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 110 (2019) ("The Constitution is exploited to shelter a range of novel practices that are antidemocratic in their aims and consequences and fundamentally destructive of the enduring First Amendment values intended to protect the individual from abusive power.").

83. *See* Solove, *supra* note 65, at 494–95.

84. *See id.* at 488–91.

85. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 738–39 (2018).

more fundamental. Most crucial to Professor Cohen's argument is that surveillance threatens democratic society not just by inhibiting innovation and free speech but by allowing data processors to access information that gives them immense power over the ideas and products to which people are exposed.[86] In the context of FRT, collection of this information can reveal powerful inferences about human behavior and even inner thoughts. The cameras in our devices both at home and in public make this even more so.[87] In the "massively-intermediated environments" in which we now live, technology companies have a huge degree of power to affect people's environments,[88] and they rely on vast amounts of information about individuals in order to further their own economic and political agendas. When technology companies have such comprehensive knowledge about consumers, it threatens the capabilities essential to producing individuals who can effectively engage in self-government.[89] In other words, the huge amount of data that companies capture about individuals through surveillance processes allows these companies to subtly affect consumers' ideas and choices through personalized feedback loops, or "filter bubbles."[90]

Thus, FRT can cause three different harms: First, because of its ability to provide huge amounts of information about anything a person does inside or outside their home, it can cause behavioral alterations that are socially undesirable, many of which actually inhibit free speech. Second, because FRT has the power to pick up images of people that contain sensitive information (either individually, or when combined), it can cause unanticipated dignitary harms and exposure. Finally, even when data does not result in the publication of any information whatsoever, the data can be used to amalgamate information that can then be used to exercise control over a consumer.

Of course, facial recognition, like all other technologies, can also serve as a tool for good. For example, many Apple consumers have come to enjoy the convenience of unlocking their devices with their faces, as well as the added security that comes with linking access to one's unique faceprint. Because faceprints are unique and often

86. *See* Cohen, *supra* note 66, at 149–50; *see also* ZUBOFF, *supra* note 82, at 94.

87. Margot E. Kaminski, *Regulating Real-World Surveillance*, 90 WASH. L. REV. 1113, 1120 (2015).

88. Cohen, *supra* note 66, at 150.

89. Cohen, *supra* note 74, at 1917.

90. *Id.*

durable over a person's lifespan,[91] faceprints are, somewhat ironically, useful for preventing security breaches.[92] In fact, facial recognition tool PimEyes markets itself as a tool for managing one's online presence, such as by determining whether someone else is using one's photos.[93] Touchless security systems may also be more desirable in light of increased hygiene concerns arising out of the COVID-19 pandemic.[94]

However, problems with the technology lurk beneath the palatable surface of convenience and personalization. Privacy laws must be built to address the above concerns stemming from nonconsensual collection of faceprints, their sale to third parties, and their use for unexpected purposes.

II. ARE FACEPRINTS A FORM OF SPEECH?

The argument that laws regulating FRT like the CCPA/CPRA are content-based and merit strict scrutiny might go something like this: Faceprints are information, and information is speech, so faceprints are speech.[95] Because faceprints are speech, regulating the capture or collection of faceprints is a regulation on speech-creation (akin to the act of writing a book), without which protection of the faceprint would have no meaning.[96] Regulating the disclosure and/or use of faceprints is a content-based regulation on speech because one would need to examine whether the information being disclosed or used is a faceprint. Accordingly, all laws regulating the capture, use, and/or disclosure of faceprints require strict scrutiny.[97] Thus, the preliminary

91. Nakar & Greenbaum, *supra* note 34, at 95.

92. *See* Thorin Klosowski, *Facial Recognition Is Everywhere. Here's What We Can Do About It*, N.Y. TIMES (July 15, 2020), https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/ [https://perma.cc/CQ2Z-LT7C].

93. PIMEYES, https://pimeyes.com/en [https://perma.cc/BU3S-YCU5].

94. *See* Lofred Madzou, *Facial Recognition Can Help Re-Start Post-Pandemic Travel. Here's How to Limit the Risks*, WORLD ECON. F. (Dec. 16, 2020), https://www.weforum.org/agenda/2020/12/facial-recognition-technology-and-travel-after-covid-19-freedom-versus-privacy/ [https://perma.cc/7KW7-GVYJ].

95. *See* Richards, *supra* note 16, at 1524; Sorrell v. IMS Health Inc., 564 U.S. 552, 570 (2011) (observing that "[t]his Court has held that the creation and dissemination of information are speech within the meaning of the First Amendment"); *see also* Kaminski, *supra* note 20, at 190 (acknowledging that if recording is speech the same way a movie is, then regulation of all recordings would always be subject to strict scrutiny).

96. *See* Anderson v. City of Hermosa Beach, 621 F.3d 1051, 1061–62 (9th Cir. 2010).

97. Cohen, *Examined Lives*, *supra* note 52, at 1409 ("The First Amendment argument against data privacy protection begins by assuming that the collection, processing, and exchange of personally-identified data are 'speech,' and then asserts that regulation of these activities cannot survive the requisite scrutiny."); *see also* Richards, *supra* note 16, at 1524 ("The 'data-is-speech'

inquiry would seem to be whether faceprints themselves are a form of speech.[98]

This line of reasoning is alluringly simple, and, admittedly, it may be most consistent with the Court's recent tendency to make broad statements about its First Amendment jurisprudence and undergo rigid free speech analyses.[99] For example, in *Reed v. Town of Gilbert*,[100] the Court suggested that a regulation would undergo strict scrutiny "if

argument has a certain superficial appeal. After all, if the First Amendment is about protecting people's ability to share ideas and information, and data is information, then the First Amendment should protect people's ability to share data.").

Interestingly, Clearview has not made this precise argument in the lawsuit filed against it by the ACLU in Vermont state court. That is, it has not expressly argued that faceprints themselves are speech. Instead, in its motion to dismiss, Clearview's argument first focuses on its search engine as the relevant "speech" restricted by BIPA: "BIPA's restrictions on the collection of 'biometric information' in publicly-available photographs violate the First Amendment because they inhibit Clearview's ability to use this public information in Clearview's search engine," which is "protected speech under the First Amendment." Defendant's Memorandum of Law in Support of Its Motion to Dismiss, ACLU v. Clearview AI, Inc., *supra* note 67, at 16–17. This is perhaps a less daunting argument for the Illinois Circuit Court to accept, given that the Supreme Court has not expressly held that all information is always speech, and such an argument, if successful, would jeopardize a great number of informational privacy laws that regulate certain categories of private information. Yet, Clearview's argument runs into problems at the next step of the inquiry: whether BIPA is content-based. BIPA does not regulate only speech with a particular content or viewpoint the way that the statute did in *Sorrell* because it does not target particular expressive uses of the data. *Compare* 740 ILL. COMP. STAT. 14/15 (2021) ("No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information . . . ."), *with* Sorrell v. IMS Health Inc., 564 U.S. 552, 558–59 (2011) ("A . . . pharmacy . . . shall not sell, license, or exchange for value regulated records containing prescriber-identifiable information . . . *for marketing or promoting a prescription drug* . . . ." (emphasis added) (quoting VT. STAT. ANN. tit. 18, § 4631(d) (2011))). That is, while the Vermont statute specifically targeted pharmaceutical marketing, BIPA does not target search engines. Clearview appears to anticipate this distinction between its case and *Sorrell*; it pivots later on in its brief when it argues that BIPA is a content-based restriction because it targets "biometric identifiers"—not search engines. Defendant's Memorandum of Law in Support of Its Motion to Dismiss, ACLU v. Clearview AI, Inc., *supra* note 67, at 19.

98. At risk of stating the obvious, faceprints do not fall into any of the traditional exceptions from First Amendment coverage outlined in *Chaplinsky v. New Hampshire*, 315 U.S. 568 (1942): fighting words, true threats, obscenity, and (to some extent) false statement of facts. *Id.* at 571–72. Inaccurate faceprinting might well present a different issue with regard to the Court's differential treatment of false statements of fact, but FRT is presumed accurate for purposes of this Article. Alternatively, one might argue that courts should create a new categorical exception for regulations on either privacy regulations more broadly, or even FRT specifically. Yet, the Court has set the bar extremely high for the government to establish a new categorical exception in addition to those outlined in *Chaplinsky*. Per the Court's holding in *United States v. Stevens*, 559 U.S. 460 (2010), one cannot not "create" a new category of wholly unprotected speech unless that category has been "historically unprotected," even if the Court had not yet overtly acknowledged it. *Id.* at 472. It would be impossible to make such a showing for new technologies.

99. *See, e.g.*, *Sorrell*, 564 U.S. 552; Reed v. Town of Gilbert, 135 S. Ct. 2218 (2015); Robert C. Post & Jennifer E. Rothman, *The First Amendment and the Right(s) of Publicity*, 130 YALE L.J. 86, 134 (2020).

100. 135 S. Ct. 2218 (2015).

[the] law applies to particular speech because of the topic discussed or the idea or message expressed," even if that content-based restriction clearly did not indicate any censorial motive.[101] However, even if one considers the controversial definition of "content based" as articulated in *Reed*, regulating faceprints would seem to pass muster. A regulation on faceprints does not apply "because of the topic discussed or the idea or message expressed."[102] These regulations would apply irrespective of the particular information derived from a faceprint; one would not need to "read" the faceprint to determine the law's application. Further, consider the purpose of the general prohibition on content-based laws: such laws lend themselves to "invidious, thought-control" purposes because, instead of prohibiting a particular viewpoint, the government might wholly excise a topic from public conversation.[103] Realistically, no such concerns arise with regulation of FRT, which would not prohibit the public from discussing any particular topic, assuming the regulation did not target only people who wished to voice particular viewpoints.[104]

Regardless, I believe the speech-versus-privacy tensions are best resolved by considering the First Amendment and privacy interests at stake in various activities—collection, use, and disclosure—to determine whether such regulations run counter to the main theoretical purposes of the First Amendment: contributing to public discourse, enriching the marketplace of ideas, and furthering individual self-expression.[105] In such instances, the law would need to overcome strict scrutiny.

III. *WHEN* ARE FACEPRINTS "SPEECH" FOR PURPOSES OF THE FIRST AMENDMENT?

With the question of, "Are faceprints speech?" set aside, the more pertinent question now presents itself: When are restrictions on faceprints restrictions on speech? Or rather, to use the oft-quoted words of Professor Frederick Schauer**,** when are they speech that is "salient" to the First Amendment?[106]

101. *Id.* at 2227–28.
102. *Id.*
103. *See* Hill v. Colorado, 530 U.S. 703, 743 (2000) (Scalia, J., dissenting).
104. *See Reed*, 135 S. Ct. at 2238 (Kagan, J., concurring).
105. *See* Kaminski, *supra* note 20, at 180.
106. *See* Frederick Schauer, *The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience*, 117 HARV. L. REV. 1765, 1768 (2004).

Professor Schauer says "salient" because not all communications are considered speech subject to full First Amendment protection.[107] For example, holding an attorney liable for malpractice does not raise constitutional concern because attorney advice is not seen as implicating the kind of speech the First Amendment was intended to protect.[108] The same is true for sexual harassment, hiring assassins, and insider trading.[109] The Supreme Court has indeed acknowledged this principle: "[I]t has never been deemed an abridgment of freedom of speech or press to make a course of conduct illegal merely because the conduct was in part initiated, evidenced, or carried out by means of language, either spoken, written, or printed."[110]

Thus, scholars and courts alike have engaged with three main theoretical bases for the First Amendment to ascertain when that communication implicates core First Amendment values that merit stringent review prior to being restricted.[111] These three bases are loosely labelled as follows: public discourse, the "marketplace of ideas," and individual self-expression.[112] For example, Professors Danielle Keats Citron and Mary Anne Franks have relied on these theoretical frameworks to argue that criminalizing the disclosure of nonconsensual pornography (commonly termed "revenge porn") is consistent with the First Amendment notwithstanding that disclosure of images is a communicative act.[113] In fact, in upholding one such law, the Illinois Supreme Court made similar observations.[114] The federal Supreme Court has embarked on similar investigations in according a lower level of

107. *Id.*; Richards, *supra* note 16, at 1507; Bhagwat, *supra* note 22, at 843; Balkin, *supra* note 20, at 1210–11.

108. Bhagwat, *supra* note 22, at 867–68.

109. Richards, *supra* note 16, at 1507.

110. Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 456 (1978) (quoting Giboney v. Empire Storage & Ice Co., 336 U.S. 490, 502 (1949)); *see also* Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 758 n.5 (1985) (identifying the traditional exceptions to First Amendment coverage, as well as other laws that regulate language without any apparent conflict with the First Amendment); Tim Wu, *Machine Speech*, 161 U. PA. L. REV. 1495, 1529 (2013) ("[E]verything from nonpolitical vandalism through political assassination 'sends a message,' but not all of that can reasonably be speech."); Robert Post, *Recuperating First Amendment Doctrine*, 47 STAN. L. REV. 1249, 1274 (1995) ("Navigation charts for aircraft do not constitutionally register as speech because we perceive them as imbued with the same constitutional value as any other goods for sale in the marketplace.").

111. *See, e.g.*, Kaminski, *supra* note 20, at 180; Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 385–86 (2014).

112. Kaminski, *supra* note 20, at 180; Citron & Franks, *supra* note 111, at 385–86.

113. Citron & Franks, *supra* note 111, at 385–86.

114. *See* People v. Austin, 155 N.E.3d 439, 458 (Ill. 2019).

First Amendment protection to commercial speech[115] and in according full protections to highly distressing speech relating to matters of public import.[116] Accordingly, I consider each of the three theories of the First Amendment in turn to determine whether, under any of the theories, regulation of faceprints implicates these concerns.[117]

First, under a traditional public discourse or self-governance theory, speech is worthy of the highest degree of First Amendment protection when it contributes meaningfully to processes of democratic self-governance.[118] Broadly speaking, adherents of this theory see speech rights as a political right fundamentally tied to the existence and exercise of democratic citizenship.[119] Thus, speech that constitutes "public discourse" is seen as receiving the highest First Amendment protection.[120] However, even within this broader theory, scholars profusely debate its meaning. Many scholars see democratic citizenship as involving far more than just participation in elections; under this theory, democracy entails making people believe that they are invested in and capable of changing the law.[121] Even more broadly, other scholars define "public discourse" as "communicative acts deemed necessary for the formation of public opinion."[122] Thus, matters of public discourse deserve the highest level of judicial scrutiny because they

115. Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 765 (1976) (observing that commercial speech merits some level of First Amendment protection, because "[i]t is a matter of public interest that [private economic] decisions, in the aggregate, be intelligent and well informed" and that "it is also indispensable to the formation of intelligent opinions as to how [the free enterprise] system ought to be regulated").

116. Snyder v. Phelps, 562 U.S. 443, 452, 454, 458–59 (2011) (reasoning that a claim for intentional infliction of emotional distress could not lie where the speech at issue concerned matters of public concern because "[t]he First Amendment reflects 'a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open'" (quoting New York Times Co. v. Sullivan, 376 U.S. 254, 270 (1964))); *see also* Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 758–59, 758 n.5 (1985) ("We have long recognized that not all speech is of equal First Amendment importance. It is speech on 'matters of public concern' that is 'at the heart of the First Amendment's protection.'" (quoting First Nat'l Bank of Bos. v. Bellotti, 435 U.S. 765, 776 (1978))).

117. For a similar application of these theories in other contexts, see Citron & Franks, *supra* note 111, at 385–86 (laws criminalizing nonconsensual pornography); Barry P. McDonald, *The First Amendment and the Free Flow of Information: Towards a Realistic Right to Gather Information in the Information Age*, 65 OHIO ST. L.J. 249, 272–73 (2004) (information-gathering).

118. Robert Post, *Participatory Democracy and Free Speech*, 97 VA. L. REV. 477, 482 (2011).

119. *See* Bhagwat, *supra* note 22, at 873.

120. Post & Rothman, *supra* note 99, at 136.

121. *See* Post, *supra* note 118, at 482 ("Democracy is achieved when those who are subject to law believe that they are also potential authors of law.").

122. Post & Rothman, *supra* note 99, at 136; *see also* Balkin, *supra* note 20, at 1210 (defining "public discourse" as "the processes of communication through which ideas and opinions circulate in a community to produce public opinion").

influence culture, encompassing scientific knowledge, entertainment, and other activities that shape political and cultural values.[123] Under this broader approach to public discourse theory, the First Amendment comfortably protects less overtly political speech, such as abstract art, music, and even tabloid gossip.

Applying this standard, FRT regulations warrant strict constitutional scrutiny when they inhibit the free formation of public opinion. This might occur if the government were to restrain a newspaper from publishing a story using information derived from FRT data. It is clear, however, that any and all actions regarding faceprints do not always contribute to public opinion, particularly in the commercial context. When a business covertly collects individuals' faceprints to ultimately sell the data to a larger data broker, public opinion is not enriched at all. Nor does FRT further public discussion when companies collect the data to provide targeted advertising; advertising is generally thought to provide useful information for individuals to choose which products and services to buy, not to contribute meaningfully to public discussion.[124]

Second, the "marketplace of ideas" theory views the First Amendment as necessary to ensure that individuals have access to a wide variety of speech so that they can make their own judgments about what speech they deem most persuasive and thereby embark on a so-called "search for truth."[125] In other words, courts protect speech so that people "can shop amongst competing ideas in a search for 'truth.'"[126] The theory gets its roots from Justice Oliver Wendell Holmes's dissent in *Abrams v. United States*[127]: "the best test of truth is the power of the thought to get itself accepted in the competition of the market."[128] At first glance, this theory seems to provide the most support for lax privacy regulation because recordings of facts often play a role in individuals' searches for truth—for example, recordings published by the media often help the public to determine what is true, as Professor Kaminski has pointed out.[129] However, to observe that faceprints could theoretically contribute to the marketplace of ideas—

123. *See* Post & Rothman, *supra* note 99, at 136–38; Bhagwat, *supra* note 22, at 874.

124. *See* Post & Rothman, *supra* note 99, at 140.

125. Alexander Tsesis, *Free Speech Constitutionalism*, 2015 U. ILL. L. REV. 1015, 1038, 1040.

126. Kaminski, *supra* note 20, at 180.

127. 250 U.S. 616 (1919).

128. *Id.* at 630 (Holmes, J., dissenting); *see also* Tsesis, *supra* note 125, at 1038–39; Vincent Blasi, *Holmes and the Marketplace of Ideas*, 2004 SUP. CT. REV. 1, 2.

129. Kaminski, *supra* note 20, at 180–81.

for example, if a researcher used FRT to conduct psychological research—misses the mark. As Professor Julie E. Cohen argues, personally-identified data is generally not collected, used, or sold for its expressive content in the commercial context.[130] That is, companies generally do not collect data to "read" it, or even to produce forms of knowledge to which the public would be exposed.[131] Instead, it is used to "categoriz[e] and segment[] a customer base."[132] Of course, there may be instances where companies genuinely do inspect faceprints and create public discourse therefrom, such as if medical researchers were to rely on the data to reveal the efficacy—or absence—of social distancing. However, behind-the-curtain faceprint harvesting and use by private, commercial entities for commercial purposes does not contribute to any metaphorical "marketplace of ideas." The point here is that faceprints *might* be used in service of the marketplace of ideas, and therefore speech, depending on the context—but, in the commercial context, where private actors profit through having sole control over personal data, this is an unrealistic expectation.[133]

Finally, under a self-expression theory of free speech, the First Amendment exists in service of the free development and operation of the individual's mind.[134] Those who take issue with this view of the First Amendment often do so because of the doctrine's perceived shapelessness and the resulting difficulty in drawing lines as to whether and when something is "speech" for purposes of the First Amendment.[135] Moreover, some view this theory's emphasis on the value of autonomy as necessitating a laissez-faire approach to speech regulation.[136] However, proponents of the self-expression theory argue that this need not be so. According to Professor Seana Valentine

130. Cohen, *Examined Lives*, *supra* note 52, at 1413–14.

131. *See id.* at 1417–18.

132. *Id.*

133. The Supreme Court recognized a similar distinction in *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 762 n.8 (1985) (plurality opinion), in which the Court held that a particular credit report at issue warranted lower First Amendment protection because it did not involve a "matter of public concern." The Court left open the door as to whether other credit reports might theoretically fulfill that purpose. *Id.*

134. Seana Valentine Shiffrin, *A Thinker-Based Approach to Freedom of Speech*, 27 CONST. COMMENT. 283, 287 (2011).

135. *See, e.g.*, Post, *supra* note 118, at 479.

136. *See* Tsesis, *supra* note 125, at 1031; *see also* Post, *supra* note 118, at 480 ("Because both speech and autonomy are pervasive, using the value of autonomy to protect speech creates the distinct risk of Lochnerism."); Kaminski, *supra* note 20, at 181–82 (observing that adopting an autonomy view of the First Amendment encourages the broadest form of First Amendment protection).

Shiffrin, a true commitment to autonomy requires recognizing that there is a more complex relationship between individual autonomy, interpersonal relationships, and democratic self-rule.[137] Accordingly, an autonomy theory of free speech does not require prioritizing individual desires over all democratic outcomes.[138] Whatever the merits of these broader criticisms, one feature of the self-expression theory is most pertinent to the question of commercial use of FRT. Shiffrin makes much of the distinction between speech from human speakers and speech from corporations: "On the other hand, protection for commercial and non-press, business corporate speech is a less central matter, one that reasonably may involve weaker protections and may reasonably rely heavily on more instrumental concerns."[139] To the extent that FRT is employed by commercial entities (the focus of this Note), it would be difficult to say that the technology contributes meaningfully to self-expression when it is wholly automated and controlled by corporations. Thus, a self-expression theory most likely provides the weakest rationale for why the First Amendment would foreclose states from regulating FRT.

Recent debate about the right to record may complicate this inquiry somewhat. With increasing litigation surrounding recordings of police and agricultural facilities, both scholars and courts have been forced to confront the question of whether and when courts and legislatures can regulate the capture of audiovisual recordings, even though they are plainly speech protected by the First Amendment.[140] Accepting that there is a general First Amendment right to take photos or videos regardless of whether the matter depicted is one of public concern, the rationale for that right does not neatly map onto faceprints. Professor Seth Kreimer has described image capture as part of a culturally recognized form of expression and communication.[141] His argument has significant force in today's culture, where individuals frequently post and discuss each other's photographs on social media.

137. Seana Valentine Shiffrin, *Methodology in Free Speech Theory*, 97 VA. L. REV. 549, 553 (2011).

138. *Id.* at 553–54.

139. Shiffrin, *supra* note 134, at 286.

140. *See, e.g.*, Fields v. City of Philadelphia, 862 F.3d 353 (3rd Cir. 2017); Am. Civ. Liberties Union of Ill. v. Alvarez, 679 F.3d 583 (7th Cir. 2012); Food Lion, Inc. v. Capital Cities/ABC, Inc., 194 F.3d 505 (4th Cir. 1999); People for the Ethical Treatment of Animals, Inc. v. Stein, 466 F. Supp. 3d 547 (M.D.N.C. 2020); Seth F. Kreimer, *Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record*, 159 U. PA. L. REV. 335 (2011); Kaminski, *supra* note 20.

141. Kreimer, *supra* note 140, at 373.

Further, this argument fits comfortably with any theoretical framework for the First Amendment. Under a public discourse theory, photographs contribute to conversations about culture and help people to feel invested and involved in their societies. Under a self-expression theory, photographs are an increasingly common form of individual self-expression, especially considering the widespread use of social media platforms like Instagram. Even considering the marketplace of ideas theory, photographs and recordings often help people to determine what is true and what is not. However, no such across-the-board observations could be made with faceprints, particularly in the commercial context, given that faceprints do not constitute a "familiar mode" for corporations (or individuals) to express themselves.[142]

Of course, any neat resolution of the driving theory behind the First Amendment is beyond the scope of this Note (and perhaps indeed impossible). Yet, regardless of the theoretical framework one adopts—public discourse, the marketplace of ideas, or self-expression—faceprints do not always contribute to communications salient to the First Amendment. The proper inquiry, then, is when do they?

A. Collection: Information-Gathering

Although faceprints are not always speech, they may be an ingredient in protected speech, thus implicating the First Amendment on some level. Thus, the collection, use, and disclosure of faceprints implicates the First Amendment because FRT has the power to *contribute* to speech protected by the First Amendment, such as scientific studies or journalism. This proposition should be far less startling than the broader assertion that all information is speech. For example, one might intuitively feel that the First Amendment would have something to say about a law forbidding people from buying ink—or, as in *Minneapolis Star & Tribune Co. v. Minnesota Commissioner of Revenue.*,[143] burdensomely taxing it.[144]

There are two approaches one might take at this point: first, one might consider such a law a restriction on the "creation of speech."

142. *Cf. id.* at 372 (providing examples of common means of expression and communication, such as music, dancing, and parades); Marc Jonathan Blitz, *The Right to Map (and Avoid Being Mapped): Reconceiving First Amendment Protection for Information-Gathering in the Age of Google Earth*, 14 COLUM. SCI. & TECH. L. REV. 115, 139 (2012) (noting that "telling stories with photographically captured light has become . . . a familiar mode of expressing oneself").

143. 460 U.S. 575 (1983).

144. *Id.* at 583.

Framing collection as an act of speech-creation would likely subject laws regulating collection to increased scrutiny because such an act would be bound up in the ultimate speech.[145] Multiple scholars have suggested this approach in the context of rights to record and capture images.[146] They rely on the idea that such imagery is always speech because it is part of a recognized communications medium.[147]

Alternatively, one might consider it a form of information gathering. Collection restrictions would then receive a lower degree of scrutiny as an act that is not intrinsically expressive but nonetheless contributes to expression.[148] Because faceprints do not inherently contribute to public discourse, self-expression, or the marketplace of ideas absent some further use, I argue that the proper analytical framework would be to think of faceprint collection as a form of information-gathering rather than speech creation.

Accepting that a strong rationale exists as to why laws restraining information-gathering must warrant First Amendment scrutiny, courts have been clear that the right of free speech does not grant citizens full license to gather information however they wish.[149] For example, in *Bartnicki v. Vopper*,[150] the Supreme Court distinguished between the news-gathering act of illegally intercepting a phone call by one party, and the subsequent communicative act of disclosing the information by a third party unrelated to the interceptor.[151] The Court held that the latter clearly constituted speech.[152] However, the Court was clear to note that, while the disclosing or publishing of the recorded call constituted speech, its holding did not mean that the First Amendment immunized individuals who gather information unlawfully; indeed, it called such an argument "frivolous" and reaffirmed the idea that otherwise valid laws that may have the effect of restraining newsgathering do not draw First Amendment scrutiny.[153] Thus, though the original interceptor was not a party to the action, the Court suggested that the initial interception would have been regulable.[154] This is consistent

145. Jared Mullen, Note, *Information Gathering or Speech Creation: How to Think About a First Amendment Right to Record*, 28 WM. & MARY BILL RTS. J. 803, 804 (2020).
146. *See id.* at 805; Kreimer, *supra* note 140, at 373.
147. *E.g.*, Kreimer, *supra* note 140, at 373.
148. *See* Kaminski, *supra* note 20, at 190.
149. *See, e.g.*, Branzburg v. Hayes, 408 U.S. 665, 691 (1972).
150. 532 U.S. 514 (2001).
151. *See id.* at 517, 526–27.
152. *Id.* at 527.
153. *Id.* at 532 n.19.
154. *See id.* at 525.

with its earlier statement that the "right to speak and publish does not carry with it the unrestrained right to gather information."[155] Scholars have reached similar conclusions. For example, Professor Cohen has argued that the First Amendment does not guarantee general social practices of pervasive data collecting, as distinct from the practice of publishing information.[156] Professor Jane Bambauer, too, acknowledges that there are limits to the information-gatherer's ability to investigate.[157] So if the right to gather information may be restrained, the question is then, do prohibitions on the collection of faceprints fall within that acceptable boundary?

Some limitations on information-gathering are clearly defensible and don't raise any First Amendment concern—for example, laws prohibiting trespass onto private property or assaulting mail delivery workers.[158] These regulations are uncontroversial in light of the First Amendment because they clearly seek to address harms that occur irrespective of whether the defendant is engaging in the conduct to gain access to information.[159] Take the tort of trespass: in terms of whether one could be held liable for the tort, liability applies evenly to the defendant who breaks into a home to steal jewelry and the defendant who does so in order to plant a recording device. Few would suggest that a reporter would be shielded from liability for trespass even if they did so for the purpose of writing a news story, though whether the reporter can then be held liable for subsequent publication of the information obtained during the trespass is a different question.[160]

By contrast, laws that impose disproportionate penalties on people who engage in protected speech pose First Amendment problems. For example, in *Western Watersheds Project v. Michael*,[161] the Tenth Circuit distinguished between the State of Wyoming's ordinary trespass law and its statute imposing heightened civil and criminal liability

155. Zemel v. Rusk, 381 U.S. 1, 17 (1965).

156. Cohen, *Examined Lives*, *supra* note 52, at 1429–30.

157. *See* Bambauer, *supra* note 16, at 78–79.

158. *Id.*

159. *But see* Eric B. Easton, *Two Wrongs Mock a Right: Overcoming the* Cohen *Maledicta that Bar First Amendment Protection for Newsgathering*, 58 OHIO ST. L.J. 1135 (1997) (arguing that even laws of general applicability should require a balancing of First Amendment values against countervailing state interests and endorsing an "actual malice" standard for imposing tort liability that arises from acts of newsgathering).

160. Moreover, under *Bartnicki*, a third-party recipient of the information gathered via an act of trespass would not be liable so long as the information constituted a matter of public concern. *See* Bartnicki v. Vopper, 532 U.S. 514, 533–34 (2001).

161. 869 F.3d 1189 (10th Cir. 2017).

on individuals who trespassed for the purpose of collecting resource data.[162] In doing so, the court emphasized that the case concerned not the constitutionality of punishing trespass, but rather the differential treatment of trespassing when the person does so to collect resource data.[163] That is, the First Amendment was implicated where the statute treated people differently because they created speech.[164] The court in *Western Watersheds* was eminently correct to impose First Amendment scrutiny on the law at issue; not only did the law forbid trespassing for the purpose of engaging in speech, but it did so to suppress a certain kind of speech—resource data. In fact, the law was purportedly designed to prevent environmental activists from proving that the cattle industry was polluting waterways with fecal bacteria.[165] Thus, the law appears to have been designed to suppress particular viewpoints as well.

By contrast, laws regulating the collection of faceprints are content- and viewpoint-neutral and should therefore receive some level of intermediate scrutiny. They impose liability regardless of the specific information captured by the sensors and instead impose liability on the conduct of surveillance.[166] As detailed above, the harms from widespread FRT have nothing to do with the content of what is surveilled; instead, these harms flow from the act of continuous watching and the corresponding behavioral effects on the data subjects. To be sure, one of the concerns is that FRT may catch and expose a person engaged in embarrassing behavior that they might prefer others not to know. But other risks created by FRT—chilling effects, inability to control one's overall degree of exposure to the world, and data breach harms—do not depend at all on the speech that results from use of the technology (if any).

To address a potential counterargument, it may be appealing to argue that one can have no interest in privacy beyond one's own home. Those who may be tempted to argue as such would be correct, of course, to observe that the home represents a sacrosanct and uncontroversial zone of privacy. Moreover, this argument has received some

162. *Id.* at 1192.

163. *Id.* at 1197.

164. *Id.*

165. Jeff Guo, *Wyoming Doesn't Want You to Know How Much Cow Poop Is in Its Water*, WASH. POST (May 20, 2015), https://www.washingtonpost.com/blogs/govbeat/wp/2015/05/20/wyoming-doesnt-want-you-to-know-how-much-cow-manure-is-in-its-water/ [https://perma.cc/LKH7-4LD4].

166. *See, e.g.*, 740 ILL. COMP. STAT. 14/15 (2021).

degree of acceptance from courts; in deciding Fourth Amendment cases, the Supreme Court has often centered much of its analysis on whether the activities at issue occurred in the home.[167] Indeed, the Court has gone as far as to say that "the Fourth Amendment draws 'a firm line at the entrance to the house.'"[168] Thus, in Fourth Amendment as well as tort privacy jurisprudence, categorizing information as "public" has historically had somewhat of a talismanic power in privacy disputes, seemingly necessitating a conclusion that, if the information has been revealed in public, it can no longer fall subject to privacy claims.[169]

However, privacy scholars have pushed back on the tendency of courts to give conclusive weight to whether information is accessible in public.[170] Professor Woodrow Hartzog has highlighted the problem that what it means to be "public" is actually highly amorphous[171]—a legal standard about as clear as saying, "We'll know it when we see it."[172] Most often, the word is used descriptively to refer to anything that is hypothetically accessible to others.[173] This definition has proved useful to those seeking to surveil in publicly accessible places.[174] Under this construction, almost every piece of information must be deemed public and therefore non-regulable, from one's

167. *See* Kyllo v. United States, 533 U.S. 27 (2001); *see also* Solove, *supra* note 65, at 496 (noting that in *Kyllo*, "[t]he Court's holding relied heavily on the fact that, though conducted outside the petitioner's home, the surveillance was capturing information about activities within it").

168. *Kyllo*, 533 U.S. at 40 (quoting Payton v. New York, 445 U.S. 573, 590 (1980)).

169. Woodrow Hartzog, *The Public Information Fallacy*, 99 B.U. L. REV. 459, 467 (2019); *see also* Solove, *supra* note 65, at 496–97 (summarizing cases where the Court refused to recognize a "reasonable expectation of privacy" when conduct occurred in a public place); Eugene Volokh, *Tort Law vs. Privacy*, 114 COLUM. L. REV. 879, 904 (2014) ("The intrusion-upon-seclusion tort generally does not preclude surveillance in places open to large numbers of people."). *But see* Nader v. Gen. Motors Corp., 255 N.E.2d 765, 771 (N.Y. 1970) (holding the defendant liable for intrusion upon seclusion based on aggressive following of the plaintiff even where the relevant acts occurred entirely in public).

170. Kaminski, *supra* note 87, at 1114–15; *see* Hartzog, *supra* note 169, at 469.

171. Hartzog, *supra* note 169, at 469. For a particularly disturbing application of this doctrine, consider the case of *McNamara v. Freedom Newspapers, Inc.*, 802 S.W.2d 901, 903, 905 (Tex. App. 1991), in which a high school soccer player was denied relief after a newspaper published a photo of him where his genitalia were accidentally exposed during a soccer game. There, the court relied heavily on the fact that McNamara was photographed in a public place. *Id.* at 905. *See also* Solove, *supra* note 65, at 538–39 (discussing the *McNamara* case).

172. Hartzog, *supra* note 169, at 469. Professor Hartzog borrows this language from *Jacobellis v. Ohio*, 378 U.S. 184, 197 (1964) (Stewart, J., concurring), in which Justice Stewart criticized the highly amorphous standard used to identify obscenity in First Amendment cases.

173. Hartzog, *supra* note 169, at 498.

174. *Id.*

conversation in a restaurant with friends, to one's conduct in a hotel room with an unobscured window, to upskirt photos.[175]

Yet, as a practical matter, limiting this zone of privacy to one's own private property fails to comport with the expectations that shape people's behavior. Most of us do not believe that once something has occurred outside of the home, it will be broadcast on television or slapped on a billboard. Considering the normative and legal power that results from calling information "public," Professor Hartzog argues that such labelling should more accurately reflect the practical reality that people's conduct is guided by their expectations of obscurity.[176] As he explains, making "occurring in public" a sufficient condition for any and all disseminations of information derived from those public activities dramatically underplays the environmental constraints that generally make activities that occur in public more obscure than reflected by a rigid public-private divide.[177] While theoretically accessible to anyone who may view the activity, most people do not expect that anything and everything they do outside of their home is fair game for public discussion in any context imaginable.[178] In reality, people generally make decisions about how to conduct their lives in part based on the level of obscurity that they can reasonably expect in that circumstance.[179] For example, a person might choose to attend an Alcoholics Anonymous meeting in a location far away from their workplace, reasonably anticipating that doing so would decrease the likelihood of their being recognized by a co-worker. Of course, one would not consider it a privacy harm for that person to then unexpectedly run into a co-worker at the meeting. Yet, there is a significant difference between that and what companies like Clearview are doing. There is a great deal more harm involved in a company's practice of collecting faceprints in a way that allows it to surveil individuals through the real-time capture of data from cameras and similar devices, or through aggregations of data "scraped" from the internet. Widespread FRT would potentially eviscerate any possibility for the person to make these kinds of informed decisions. This would then result in the chilling effects discussed above—perhaps this person who wished to

175. *See id.* at 461–62.

176. *Id.* at 518.

177. *Id.* at 502.

178. *See* Kirsten Martin & Helen Nissenbaum, *Privacy Interests in Public Records: An Empirical Investigation*, 31 HARV. J. L. & TECH. 111, 113 (2017).

179. *See* Kaminski, *supra* note 20, at 171–72; Kaminski, *supra* note 87, at 1136.

attend an Alcoholics Anonymous meeting will not seek out the therapeutic treatment she needs at all. All this is to say that in reality, people's privacy expectations are far from binary, and a precise analysis of what constitutes an actionable privacy harm requires meaningfully addressing that FRT severely restricts people's ability to control their own exposure to the world.

In Fourth Amendment cases, members of the Supreme Court have begun to address precisely this issue. Justice Sotomayor stated the problem astutely in her concurrence in *United States v. Jones*,[180] in which the Court held that the Government violated the Fourth Amendment when it installed a GPS on a suspected narcotics trafficker's car and tracked its movements for four weeks without a valid warrant.[181] There, the Court relied heavily on the fact that law enforcement officers had committed a physical trespass when they initially installed the GPS on the car.[182] The Court declined to address the question of whether the Government would have violated Jones' Fourth Amendment rights had the GPS tracking been unaccompanied by any initial physical invasion.[183] However, in her concurrence, Justice Sotomayor went a step further and observed that technological developments have, in many cases, rendered physical intrusion unnecessary in order to surveil people.[184] Even without any physical contact with the data subject or their property, surveillance systems such as location monitoring make it possible to collect a profusion of personal information.[185] As Justice Sotomayor explained, this kind of technology has the power to make visible "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[186]

While the Fourth Amendment obviously does not apply to the use of FRT by private actors (at least not directly), Justice Sotomayor's reasoning makes clear the problem of relying on physical trespass as a proxy for invasion of privacy. Instead, whether a person has exceeded the bounds of acceptable information-gathering practices must

180. 565 U.S. 400 (2012); *see also* Reidenberg *supra* note 52, at 150, 157 (discussing *Jones*).
181. *Jones*, 565 U.S. at 403–04.
182. *Id.* at 404–05.
183. *Id.* at 412.
184. *Id.* at 414–15 (Sotomayor, J., concurring).
185. *Id.*
186. *Id.* at 415 (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)).

take into account the subject's expectations of obscurity. It must also contemplate the uniquely invasive capabilities of various modern technologies.

Thus, in the same way that laws imposing liability for intruding upon the seclusion of the home or for wiretapping protect against observations, punishing individuals for the collection of FRT data protects against practices that chill socially desirable activities, deprive individuals of the ability to choose when to expose themselves, infringe on the "breathing room" necessary for self-development,[187] and deter people from engaging in activities that require a level of anonymity. And, ultimately, because the First Amendment does not protect information-gatherers when they go beyond neutral zones of seclusion (and the collection of faceprints belongs within this zone), the First Amendment should not bar regulations on the collection of faceprints.

B. Use

As discussed above, legislatures should be able to regulate the capture of faceprints without running afoul of the First Amendment. Many laws go further, restricting the use of personal data—as distinguished from restrictions on disclosure to third parties. For example, similar restrictions appear in the Fair Credit Reporting Act, which limits credit reporting agencies' use of consumer data to specifically delineated purposes.[188] Similarly, California has restricted the use of faceprints once already captured; with the passage of the CPRA, California consumers may instruct businesses to limit their use of faceprints to uses that are "necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services."[189] Businesses are then obligated to use the consumers' faceprints only for those purposes unless consumers later provide consent.[190] Thus, if a person requests that Apple only use their faceprint to open their phone, does the Constitution permit Apple to disregard that request? Does Apple have a First Amendment defense

187. *See* Cohen, *supra* note 74, at 1906; *see also* Jane Yakowitz Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205, 252 (2012) ("Seclusion gives people the breathing space to be and to act without having to worry about social or economic consequences.").

188. 15 U.S.C. § 1681b(a)(3) (2018); Richards, *supra* note 20, at 1191; *see also id.* at 1190–92 (providing other examples of use restrictions).

189. CAL. CIV. CODE § 1798.121(a) (West Supp. 2021); *id.* § 1798.140(v)(1)(E) (defining "personal information" for purposes of the CPRA to include "biometric information" like faceprints).

190. *Id.* § 1798.121(b).

to use their faceprint to, for example, send targeted ads? This raises the question of whether use restrictions are compatible with the First Amendment.

In *Bartnicki v. Vopper*, the Court briefly addressed the constitutionality of use restrictions.[191] The wiretap law at issue in that case contained a provision prohibiting individuals from using the contents of an intercepted phone call.[192] The provision broadly prohibited all uses, including using the communications of a business rival to create a competing product, or using the information to discipline a subordinate.[193] Ultimately, the Court held that the use prohibition was a regulation of conduct, not speech.[194]

Some courts have analyzed various data usage laws as commercial speech. For example, in *U.S. West, Inc. v. Federal Communications Commission*,[195] the Tenth Circuit held that a law was a restriction on commercial speech where it restricted telecommunications carriers from using customer information to market additional services to their customers.[196] In that case, the court focused on the customers' right to receive information about these services rather than U.S. West's interests in communicating that information for its own benefit as an autonomous speaker.[197] It then held that the law did not survive *Central Hudson* review, in part because the state had not articulated a concrete privacy interest beyond consumers' general unease, and because an opt-out framework seemed sufficient to protect whatever privacy interest may have been at stake.[198]

The issue of use restrictions also came up in *Sorrell*. The statute at issue forbid pharmaceutical marketers from using prescriber-identifying information to market or promote a prescription drug without the physician's consent.[199] The Court reasoned that the use restriction was content based because it burdened only speech with a particular

191. *See* Bartnicki v. Vopper, 532 U.S. 514, 526–27, 527 n.10 (2001).

192. *Id.* at 523–24.

193. *Id.* at 527 n.10.

194. *Id.* at 526–27; *see also* Richards, *supra* note 20, at 1192 (summarizing the *Bartnicki* holding).

195. 182 F.3d 1224 (10th Cir. 1999).

196. *Id.* at 1230, 1232.

197. *Id.* at 1232. *But see* Alexander Tsesis, *Marketplace of Ideas, Privacy, and the Digital Audience*, 94 NOTRE DAME L. REV. 1585, 1597 (2019) (explaining that "[t]he commercial speech doctrine is predicated on the audience's right to know" and that this justification does not hold true in much of today's online marketing where consumers are not permitted to make informed decisions between advertised products).

198. *U.S. West*, 182 F.3d at 1235, 1238–1239.

199. Sorrell v. IMS Health Inc., 564 U.S. 552, 558–59 (2011).

content: pharmaceutical marketing by detailers.[200] The Court was concerned that the Vermont Legislature was using speech restrictions to achieve the otherwise permissible policy goal of lowering drug prices by foreclosing large pharmaceutical companies from marketing their drugs to physicians.[201] These concerns were further supported by the legislative history, which illustrated that the purpose of the statute was to lower the costs of medical services by making it more difficult to promote expensive and less safe brand-name drugs—but not their competitors'.[202] Thus, the government was regulating the use of data "in order to tilt public debate in a preferred direction," rather than merely restricting commercial speech.[203] Further, the Court ultimately applied *Central Hudson*'s test for commercial speech for argument's sake, and therefore it did not resolve the question of whether restricting the use of prescriber-identifying information for marketing purposes was a restriction on commercial speech.[204] It also did not reveal whether a general prohibition on commercial use would be impermissible absent the fact that the government used speech to favor some products over others. Consequently, while dicta in the majority opinion casts some doubt on the continued viability of the commercial speech doctrine, *Sorrell* does not stand for the proposition that any and all regulation of data use (even if limited to advertising purposes) presumptively violates free speech.

Unlike the statutes at issue in *Sorrell* and *U.S. West*, and like the prohibition in *Bartnicki*, restrictions on the use of faceprints need not target specific uses such as "marketing purposes." Nor, for that matter, should they target specific actors such as pharmaceutical marketers, allaying concerns that use restrictions are inherently viewpoint-discriminatory. Instead, by restricting businesses' use of faceprints to those that consumers reasonably expect, legislatures hold businesses liable for acting in a way that violates consumer expectations—not for producing speech with a particular content or representing a particular viewpoint.

200. *Id.* at 565.
201. *See id.* at 576–78.
202. *See id.* at 560–61; *see also* Richards, *supra* note 16, at 1506.
203. *See Sorrell*, 564 U.S. at 578–79.
204. *Id.* at 571–72.

C. Disclosure

Unlike the collection and use of faceprints, disclosure presents a much clearer case of a potential incursion on free speech. In this context, it seems like there is always a speaker (the disseminator of the information), a listener (the recipient of the information), and information (the faceprints). This would meet the definition for "speech" that the Court articulated in *Spence v. Washington*[205]: an intent to convey a message that would be understood by those who viewed it.[206] However, not all communications of information warrant First Amendment protection,[207] including those that formally meet *Spence*'s definition.[208] More importantly, even when they do, courts have applied a much more nuanced approach than the two tiers of strict and intermediate scrutiny would seem to suggest.[209]

Instead, recall that the law generally recognizes communications as requiring heightened First Amendment review when they fulfill the theoretical purpose of the First Amendment: furthering public discourse, contributing to the marketplace of ideas, or promoting human self-expression.[210] Additionally, a communication might receive the full protection of the First Amendment when it appears in a recognized medium of expression, such as photographs.[211] Patently, faceprints are not a socially recognized medium of expression akin to photography or art. Further, when faceprints are sold by commercial entities for commercial purposes, disclosures of faceprints cannot reasonably be said to further any of the above; data is generally then used for wholly internal purposes. While faceprints could theoretically be sold to research institutions to produce socially beneficial research, such an instance should be treated as an exception rather than the rule. Instead, there are two primary ways we might treat the sale of data between commercial entities: as commercial speech or "purely private speech." I discuss each in turn, ultimately concluding that the latter would be the proper approach.

---

205. 418 U.S. 405 (1974).

206. *Id.* at 410–11; Hurley v. Irish-Am. Gay, Lesbian & Bisexual Grp. of Bos., Inc., 515 U.S. 557, 569 (1995) (broadening the "particularized message" requirement from *Spence*).

207. *See* Post, *supra* note 110, at 1252; Bhagwat, *supra* note 22, at 843; Wu, *supra* note 110, at 1506.

208. Post, *supra* note 110, at 1252.

209. *See* Post & Rothman, *supra* note 99, at 134–35.

210. *See supra* notes 113–140 and accompanying text.

211. *See* Kreimer, *supra* note 140, at 373; *cf.* Post, *supra* note 110, at 1253–54.

1. Treating Disclosure Restrictions as Commercial Speech Restrictions

Because commercial speech is subject to a less strict level of review, some have argued that regulating data as a form of commercial speech is appropriate when the data will ultimately be used in something that qualifies as a form of commercial speech, or if the data will be generated or sold as a product (as is done by data brokers, for example).

For example, Katherine Peyton has argued[212] that restrictions on the sale and use of consumer data for marketing purposes regulate commercial speech of the kind described in *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.*[213]: speech that merely proposes a commercial transaction.[214] The prototypical example of such speech is a commercial advertisement. Per Peyton, because the data mining industry sells data to third parties or directly uses it for advertising purposes, and these companies make profits off of the data, regulating uses and sales of data are a form of commercial speech.[215]

This argument has some force as it pertains to some restrictions on data use, but not disclosure. It is true that data is generally processed and sold to be used as part of the advertising industry.[216] However, the fact that a company profits off of a disclosure of information (i.e., sells it) cannot be, in and of itself, sufficient to transform a law prohibiting that disclosure into a prohibition on commercial speech.[217] Otherwise, a government could treat prohibitions on newspaper, book, or movie sales under the more lenient commercial speech standard by reasoning that the company profits from such sales. Thus, this cannot be the sole basis for calling data disclosure laws regulations on commercial speech. Nor does the fact that the recipient of the information intends to use the information for commercial purposes constitute a regulation on commercial speech. As Professor Bhagwat has argued,

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

213. 425 U.S. 748 (1976).

214. *Id.* at 762.

215. Peyton, *supra* note 212, at 75–76.

216. *See* Rebecca Harris, Note, *Forging A Path Towards Meaningful Digital Privacy: Data Monetization and the CCPA*, 54 LOY. L.A. L. REV. 197, 204 (2020).

217. *See* Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 67 (1983); IMDb.com Inc. v. Becerra, 962 F.3d 1111, 1122 (9th Cir. 2020); Bhagwat, *supra* note 22, at 866; Balkin, *supra* note 20, at 1198.

the commercial nature of speech turns on the content of the information—not the purpose for which the recipient may or may not use the information in the future.[218] While a buyer of faceprints might want the information to generate advertising or other forms of commercial speech, the sale of faceprints themselves clearly does not propose a commercial transaction.

Further, considering the reasons why the Court granted First Amendment protection to commercial speech illustrates the flaw of the proposition that selling (or otherwise disclosing) faceprints should be regulated as commercial speech. The First Amendment protects commercial speech out of concern for the interest of consumers—the listeners.[219] Specifically, commercial speech is meant to serve listeners' interests by providing them with useful information that can shape their purchasing choices.[220] The sale of a database does not aid its recipient (the buyer) in making any such choices about what product to purchase; the data itself is the product.

2. Treating Disclosure Restrictions as "Matters of Purely Private Concern"

Even though the sale of FRT cannot be categorized as commercial speech, there remains another way to analyze restrictions on these disclosures. In *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*,[221] the Court's plurality opinion held that courts could award presumed and punitive damages in defamation cases where the plaintiff was not a public figure or official, nor was the publication on a matter of public concern.[222] The case involved a credit report that erroneously stated that the plaintiff, a construction contractor, had filed for bankruptcy.[223] After the plaintiff sued the defendant credit reporting agency for defamation, the plaintiff prevailed at trial, and the jury awarded it both compensatory and punitive damages.[224] The defendant moved for a new trial, arguing that a showing of actual malice was required for a defamation plaintiff to recover punitive damages.[225] In doing so, the

218. Bhagwat, *supra* note 22, at 866–67.
219. *Va. State Bd. of Pharmacy*, 425 U.S. at 763–64.
220. *See id.*
221. 472 U.S. 749 (1985) (plurality opinion).
222. *Id.* at 761.
223. *Id.* at 751.
224. *Id.* at 752.
225. *Id.* at 752–54.

defendant relied on cases like *New York Times Co. v. Sullivan*,[226] which required a showing of "actual malice" (defined as "knowledge that it was false or with reckless disregard of whether it was false or not") in order for a public figure plaintiff to prevail in a defamation suit.[227]

After granting certiorari, the *Dun & Bradstreet* plurality held that no such showing was required.[228] In reaching that conclusion, the Court considered the theoretical purposes of the First Amendment, and concluded that the particular credit report at issue in that case furthered none of them.[229] In fact, the Court was highly skeptical of such an argument, observing that "[t]here is simply no credible argument that this type of credit reporting requires special protection to ensure that 'debate on public issues [will] be uninhibited, robust, and wide-open.'"[230] This did not mean that the reports merited no protection—rather that they merited a lower level of protection consistent with the lower constitutional value of the speech.[231]

Since *Dun & Bradstreet*, lower courts have reached similar conclusions in cases involving the disclosure of credit header information[232] and the identity of individuals who purchase videos.[233] Courts also employ a similar distinction in the area of speech by government employees.[234] In those cases, speech is only accorded significant First Amendment protection if it concerns a matter of public importance.[235] Scholars have argued for courts to conduct a similar analysis in other areas of the law, such as nonconsensual pornography.[236]

Regulations on the commercial use of faceprints should be analyzed much the same way. Like the credit reports at issue in *Dun &*

226. 376 U.S. 254 (1964).

227. *Id.* at 279–80.

228. *Dun & Bradstreet*, 472 U.S. at 761.

229. *Id.* at 759–61.

230. *Id.* at 762 (second alteration in original) (quoting Sullivan, 376 U.S. at 270); *see also* Bhagwat, *supra* note 20, at 876 ("The disclosure of large amounts of data, especially personal data, generally has no real connection to self-governance, no matter how broadly that concept is defined.").

231. *Dun & Bradstreet*, 472 U.S. at 760 ("While such speech is not totally unprotected by the First Amendment, . . . its protections are less stringent.").

232. Individual Reference Servs. Grp., Inc. v. Fed. Trade Comm'n, 145 F. Supp. 2d 6, 40–41 (D.D.C. 2001).

233. *E.g.*, Boelter v. Hearst Commc'ns, Inc., 192 F. Supp. 3d 427, 445–46 (S.D.N.Y. 2016).

234. *See, e.g.*, Connick v. Myers, 461 U.S. 138 (1983).

235. *See id.* at 146–47.

236. *See* Citron & Franks, *supra* note 111, at 383.

Bradstreet, the sale of faceprints generally does not enrich public discourse in any meaningful way. Considering the "content, form, and context" of these disclosures,[237] the average sale of commercial information from one entity to another does not enhance the discussion of any issue. For example, when companies sell facial recognition data to data brokers, no individual person has gained any knowledge. In fact, most people would not even know when such a transaction has occurred. Though the Court was presented squarely with this question in *Sorrell*, the Court declined to resolve the case on these grounds, suggesting that it may be disinclined to make a sweeping proclamation that the sale of a database is speech fully protected by the First Amendment. The better way to resolve this issue would be to analyze faceprint sales as the type of purely private speech covered by *Dun & Bradstreet* and subject to intermediate scrutiny—an approach that would allow courts to realistically address both potential risks posed by FRT and their low contributions to free speech.

One might argue that the distinction between purely private speech and speech on matters of public interest produces line drawing problems. This criticism is not without merit, as current jurisprudence on whether something is a matter of purely private concern is not exceptionally well delineated.[238] However, a similar problem existed when the Court first opted to make such a distinction in defamation law.[239] Developments in these areas of jurisprudence should provide helpful guideposts for courts to conduct similar analyses with the sale of faceprints and other consumer data. More crucially, I am sensitive to the criticisms that delineating between speech on "matters of public concern" and "matters of private concern" presents the risk of courts becoming the arbiters of what is fit for public discussion.[240] Thus, in determining that faceprint disclosures constitute private speech, courts should pay particular attention to the absence of a human speaker (or listener) and the fact that the information gleaned from most data disclosures does not even reach the general public. Such communications should not be subject to lower scrutiny because they concern a topic that people have no legitimate right to speak about, but rather because they generally do not help people say anything at all.

237. Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 761 (1985) (quoting *Connick*, 461 U.S. at 147–48).

238. *See* Post & Rothman, *supra* note 99, at 167–68.

239. New York Times Co. v. Sullivan, 376 U.S. 254, 270 (1964).

240. *See* Volokh, *supra* note 16, at 1089.

3. Limitations on Data Disclosure Laws

Even if regulations of commercial FRT use can be considered a regulation on speech that is only of private concern, there are two limitations on information disclosures that any privacy statute most confront. First, the government cannot punish an entity for publishing information on matters of public concern when it has received the information lawfully.[241] In the context of FRT, this rule would apply in instances where a party has published information derived from faceprints. Returning to the *Bartnicki* case, the Court was confronted with the question of whether an innocent recipient of an unlawfully recorded communication could be punished for airing the recording on a radio show.[242] Plaintiffs Bartnicki and Kane were members of a teachers' union engaged in contentious collective-bargaining negotiations with a school board.[243] While Bartnicki and Kane were discussing the negotiations over the phone, Kane spoke some rather unflattering words about the board: "If they're not gonna move for three percent, we're gonna have to go to their, their homes . . . . To blow off their front porches, we'll have to do some work on some of those guys."[244] Unbeknownst to the plaintiffs, an unidentified third party had intercepted and recorded their conversation.[245] That third party then deposited the tape into the mailbox of Yocum (the head of a local taxpayers' organization) who then delivered it to Vopper, a radio commentator.[246] Vopper played the tape on his talk show, and other media outlets republished the text of the conversation.[247] Bartnicki and Kane filed suit against all of the media representatives as well as Yocum.[248] In their complaint, the plaintiffs alleged that they had violated both the federal and Pennsylvania state wiretapping statutes, which prohibited a person from willfully disclosing the contents of a phone call if the person knew the information was obtained through an illegal interception.[249]

Because the wiretap laws were content- and viewpoint-neutral, the Court did not apply strict scrutiny—in fact, it barely engaged with

241. *See infra* notes 243–259 and accompanying text.
242. Bartnicki v. Vopper, 532 U.S. 514, 517, 526–27 (2001).
243. *Id.* at 518.
244. *Id.* at 518–19 (omission in original).
245. *Id.* at 518.
246. *Id.* at 519.
247. *Id.*
248. *Id.*
249. *Id.* at 520 & n.3, 525.

any level of scrutiny at all.[250] However, the statute's disclosure prohibition still failed. The government identified two interests purportedly served by the provision: first, the interest in removing incentives for those who wanted to engage in wiretapping; and second, the interest in minimizing harm to the individuals' whose conversation was intercepted.[251] The Court quickly dismissed the first asserted interest, reasoning that the proper way to de-incentivize wrongful conduct was to prohibit the *unlawful* actor from disclosing the unlawfully acquired information.[252] However, prohibiting its disclosure by an innocent third party did not permissibly serve that interest, particularly given how unlikely it would be for someone to intercept a communication in order to hand it over to a third party without some reward (though that was precisely what happened in *Bartnicki*).[253]

While the Court did not have much difficulty in rejecting the first asserted interest, the Court was considerably more receptive to the second—minimizing harm.[254] Yet, despite the admittedly serious value in protecting people's private communications,[255] they yielded in the face of the strong First Amendment concerns in that case.[256] Specifically, the Court focused on the fact that the airing of the recording was a "publication of truthful information of public concern."[257] It expressly reserved the question of whether the First Amendment would impose similar requirements on "information of purely private concern."[258] This is consistent with the Court's narrow approach to other privacy-versus-speech cases[259]—an approach that indicates the Court's reluctance to restrict privacy laws across the board.

Thus, *Bartnicki* makes clear that innocent recipients of FRT data cannot be held liable for using the data to speak on issues of public concern, even when the information was initially procured unlawfully. For example, if a company were to surreptitiously provide FRT data that revealed valuable insights about whether people were wearing

250. *See id.* at 526.
251. *Id.* at 529.
252. *Id.* at 529–30.
253. *Id.* at 530–31.
254. *See id.* at 532.
255. *Id.* at 532–33.
256. *See id.* at 535.
257. *Id.* at 533–34.
258. *Id.* at 533.
259. *See* Fla. Star v. B.J.F., 491 U.S. 524, 533 (1989); Cox Broad. Corp. v. Cohn, 420 U.S. 469, 491 (1975); *see also* Sorrell v. IMS Health Inc., 564 U.S. 552, 571 (2011) (declining to address the question of whether all data is speech and instead resolving the case on narrower grounds).

face masks, a recipient could not be held liable for later writing a story based on that information.

However, consistent with dicta in *Bartnicki*, the government can impose liability on a corporation for selling (or otherwise disclosing) that information when it has obtained the faceprints unlawfully in the first place. This reflects the fact that the disclosure of private information can cause further invasions of privacy from continued use of the sensitive information. It also serves to disincentivize parties from the initial privacy invasion. At first blush, this might seem to contravene the First Amendment—how can dignitary harms outweigh the significant weight we place on freedom of speech? But, recall that unrestrained FRT can cause damage far beyond revealing tidbits of embarrassing information.[260] Limits on further disclosure are necessary to avoid the chilling effects that occur when people know their sensitive information could be disclosed not only to the original interceptor but also to further recipients of the information.[261] From a more practical standpoint, having some degree of control over the sale of one's faceprint is essential to addressing data breaches and deterring identity theft.

Apart from the concerns at issue in *Bartnicki*, the government also may not punish disclosures of information where the government originally published the information itself. This principle developed in two cases, *Cox Broadcasting Corp. v. Cohn*[262] and *Florida Star v. B.J.F.*,[263] both of which involved statutes forbidding the publication of rape victims' identities.[264] In *Cox*, the television station had obtained the name of the victims from courthouse records.[265] Similarly, in *Florida Star*, the newspaper discovered the victim's identity from a police report.[266] In both cases, much of the Court's reasoning revolved around the fact that the government itself had originally published the information.[267] For example, in *Florida Star*, the Court highlighted the fact that the government could have chosen ample means to protect victims' identities aside from punishing the press: it could have redacted the information in the first place, punished government

260. *See supra* notes 66–91 and accompanying text.
261. *See Bartnicki*, 532 U.S. at 533.
262. 420 U.S. 469 (1975).
263. 491 U.S. 524 (1989).
264. *Cox*, 420 U.S. at 471–72; *Fla. Star*, 491 U.S. at 526.
265. *Cox*, 420 U.S. at 472–73.
266. *Fla. Star*, 491 U.S. at 526.
267. *Cox*, 420 U.S. at 491; *Fla. Star*, 491 U.S. at 534.

employees for wrongfully disclosing it, or wholly abstained from publishing it.[268] Yet, in both cases, the Court was careful to limit its holding to the facts before it, clearly wary of the harmful effects that a broad holding could have on privacy rights.[269]

IV. RECOMMENDATIONS

Above, I have argued that the First Amendment analysis depends on the activity at issue, as well as the ultimate purpose of the data usage. At the collection stage, FRT is best analyzed under an information-gathering framework under which regulation would be permissible subject to intermediate scrutiny. The First Amendment by no means disappears in such an inquiry, but, much like the law at issue in *Bartnicki*, laws governing collection of information will be permissible so long as the government has a substantial interest. Once the data is collected, an unlawful collector can be held liable for continued use of the data. Further, even a lawful possessor can constitutionally be held liable for violating generic use restrictions. As for disclosures, legislatures should be able to prohibit the disclosure of the information by an unlawful possessor, regardless of whether the matter concerns public discourse. However, a lawful actor who has been provided with facial recognition data cannot be held liable for using that data in public discourse. Finally, in the unlikely chance that the government has already publicized faceprints, the government could not then punish parties who use that data.

A. California Privacy Law: The CCPA and CPRA

The CCPA and CPRA are the first consumer privacy laws in the country to approximate the comprehensive data privacy laws already found in Europe,[270] and California's first large-scale regulation of FRT. These laws regulate businesses that either meet a revenue threshold or collect a minimum amount of personal information.[271] Unlike sectoral privacy regulations that have tended to dominate the American legislative landscape, the CCPA and CPRA mark a shift towards

268. *Fla. Star*, 491 U.S. at 534.

269. *See id.* at 532; *Cox*, 420 U.S. at 491.

270. *See* Anupam Chander et al., *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1771, 1776 (2021).

271. CAL. CIV. CODE § 1798.140(c) (West Supp. 2021).

the more broadly applicable regulatory approach taken in the European Union's General Data Protection Regulation (GDPR).[272]

In terms of the laws' coverage, the CCPA and CPRA define "personal information" (PI) to cover "biometric information," which includes "imagery of the . . . face . . . from which an identifier template, such as a faceprint . . . can be extracted."[273] Going further, the CPRA covers more than just imagery of the face; it includes faceprints themselves in its definition of "sensitive personal information" (SPI).[274] While the statute generally exempts publicly available information from its coverage, this does not include faceprints collected without the consumer's knowledge.[275]

As it relates to both PI and SPI, the CCPA has four main features: (1) it requires companies to make disclosures regarding the categories of information being collected, the purposes for which information is being used, and the categories of third parties with whom the business shares the information;[276] (2) it provides individuals with a right to request that businesses disclose which categories and specific pieces of information the business has collected;[277] (3) it grants individuals the right to opt out of the sale of their data[278] and institutes a duty of nondiscrimination[279] (though it allows businesses to alter their pricing or services if directly related to a consumer's abstention from providing personal information[280]); and (4) it empowers consumers to request that a business delete any personal information about them,[281] although this is limited to businesses that directly collect information from consumers rather than those that acquire the information later on.[282] The deletion right also does not apply if the information is

272. *See* Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

273. *See* CAL. CIV. CODE § 1798.140(b), (o)(1)(E).

274. *See id.* § 1798.140(b), (ae)(2)(A) (together, defining "sensitive personal information" as referring to the "processing of [imagery of the face from which an identifier template, such as a faceprint, can be extracted] for the purpose of uniquely identifying a consumer").

275. *See id.* § 1798.140(v)(2).

276. *Id.* § 1798.110(a).

277. *Id.* § 1798.100(a).

278. *Id.* § 1798.120(a).

279. *Id.* § 1798.125(a)(1).

280. *Id.* § 1798.125(b)(1).

281. *Id.* § 1798.105(a).

282. Chander, *supra* note 270, at 1754 (describing the CCPA's right to deletion and contrasting it with the GDPR's more expansive right); Margot Kaminski et al., *Symposium: The California Consumer Privacy Act*, 54 LOY. L.A. L. REV. 157, 192 (2020).

necessary to "enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business and compatible with the context in which the consumer provided the information."[283]

Further, the passage of the CPRA created additional duties relating to SPI[284]: (1) it requires businesses that collect SPI to disclose to the consumer which categories it will collect, the purposes for its collection and use;[285] (2) it allows consumers to direct businesses to limit their uses of SPI to those that are "necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services,"[286] and (3) it prohibits businesses who have received such directions from using or disclosing SPI for any other purpose unless the consumer later provides consent.[287] Notably, the last two duties do not apply to SPI that is "collected or processed without the purpose of inferring characteristics about a consumer."[288]

Applying all of the above to facial recognition data, the CCPA and CPRA give consumers access to information on whether their faceprints are being collected and used and for what purposes. If the faceprints are collected or processed with the purpose of inferring characteristics about consumers, they may also opt out of the use and disclosure of their faceprints, except to the extent reasonably necessary to perform requested services or provide requested goods. The CCPA and CPRA also let consumers request that their faceprints be

283. CAL. CIV. CODE § 1798.105(d)(7).

284. *See generally* Mary T. Costigan, *CPRA Series: Sensitive Personal Information*, JACKSONLEWIS: WORKPLACE PRIVACY, DATA MANAGEMENT & SECURITY REPORT (Dec. 14, 2020), https://www.workplaceprivacyreport.com/2020/12/articles/california-consumer-privacy-act/cpra-series-sensitive-personal-information [https://perma.cc/TW72-5PSR] (explaining how the CPRA has expanded upon the CCPA, such as by adding a category called "Sensitive Personal Information").

285. CAL. CIV. CODE § 1798.100(b). While the statute originally required businesses to disclose whether the SPI would be sold or shared and the length of time it intends to retain each category of SPI, the statute was amended by ballot initiative in late 2020 to omit these requirements. However, that version of the statute is operative only until January 1, 2023, at which point California law will again impose these requirements.

While I do not focus on notice provisions in this Note, it is worth mentioning that they do relate to the First Amendment as a form of compelled speech. However, in the context of commercial speech, such disclosures are subject to a lenient standard of review. They have not proven controversial in biometric litigation.

286. *Id.* § 1798.121(a).

287. *Id.* § 1798.121(b).

288. *Id.* § 1798.121(d).

deleted. Significantly, the law does not mandate that businesses first get permission from consumers, instead operating on an opt-out basis.

Because of the opt-out framework, the law departs significantly from Illinois's biometric privacy law, BIPA, which requires companies to obtain consent before collecting a faceprint.[289] Based on this shortcoming alone, some would argue that the law will fail to meaningfully impact individuals' control over their personal information.[290] Others have argued that a notice-and-choice framework is wholly inadequate.[291] Further, many privacy advocates have argued that the statute is unlikely to be strongly enforced, as it creates a private right of action that applies only in the event of a data breach; otherwise, enforcement is left to the discretion of the newly-established California Privacy Protection Agency.[292] However, with its coverage of facial recognition data and restrictions on use and disclosure, it is a step towards greater control over California consumers' privacy—if the First Amendment will so permit.

B. Evaluating the CCPA's Biometric Provisions Against the First Amendment

Likely anticipating a First Amendment challenge to the law, drafters of the CCPA/CPRA have expressly created various exceptions with a view towards free speech concerns. First, it contains an exception to the deletion right: businesses need not delete faceprints if they require that information in order to exercise free speech rights.[293] While this exception might save the statute, it is not entirely helpful, either for the enforcement agency or for the businesses who must comply—and if regulation of personal data were to be held unconstitutional in most circumstances, it would become the exception that

289. 740 ILL. COMP. STAT. 14/15 (2021).

290. *See* Felix T. Wu, *The Constitutionality of Consumer Privacy Regulation*, 2013 U. CHI. LEGAL F. 69, 75–76 (outlining various suggestions to improve notice in a notice-and-consent framework).

291. *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1660–62 (1999); Cohen, *Examined Lives*, *supra* note 52, at 1399.

292. CAL. CIV. CODE § 1798.155(a); *see also* Carla Llaneza, Comment, *An Analysis on Biometric Privacy Data Regulation: A Pivot Towards Legislation Which Supports the Individual Consumer's Privacy Rights in Spite of Corporate Protections*, 32 ST. THOMAS L. REV. 177, 196 (2020) (arguing that a private right of action is necessary in biometric privacy statutes for meaningful enforcement). For a criticism of the tendency to focus on the efficacy of public enforcement and on enforcement litigation altogether as a means to alleviate privacy concerns, see Julie E. Cohen, *How (Not) to Write a Privacy Law*, *supra* note 52.

293. CAL. CIV. CODE § 1798.105(d)(4).

swallows the rule. Additionally, without further articulation of when the statute does not apply, it would also run the risk of being void for vagueness.

However, the statute does contain additional such exceptions. Businesses need not respect a deletion request when (1) the business requires the information to engage in scientific, historical, or statistical research, and (2) the consumer has given informed consent—oddly, the only instance in which use of a consumer's faceprint requires affirmative consent.[294] While one might argue that creating an exception for scientific researchers runs the risk of making the statute underinclusive—the fatal flaw of the statute in *Sorrell*[295]—the statute explicitly requires informed consent from data subjects.[296] However, this higher consent requirement for research purposes may ultimately be struck down because it places a higher burden on parties engaging in research than those using it for other purposes. Thus, the legislature should revise the statute to provide for a uniform consent requirement.

Apart from scientific research, the law also does not apply at all to lawfully obtained, truthful information that is a matter of public concern.[297] This exception moves the statute outside of *Bartnicki* territory. Additionally, as for data usage, the CPRA restricts faceprint usage based on consumers' expectations rather than targeting a particular purpose,[298] distinguishing the statute from those at issue in *Sorrell* and *U.S. West*. Finally, the law does not apply to information that the government has already made available.[299] Interestingly, a prior version of the law had a narrower exception to the use of government-provided information; it foreclosed such uses only where they were "not compatible with the purpose for which the data is maintained and made available."[300] However, the final version of the law broadly exempts businesses from liability where the government first provided the information.[301] The law thereby avoids the problems that arose with the rape shield laws in *Cox* and *Florida Star*.[302]

294. *Id.* § 1798.105(d)(6).
295. Sorrell v. IMS Health Inc., 564 U.S. 552, 572–73 (2011).
296. CAL. CIV. CODE § 1798.105(d)(6).
297. *Id.* § 1798.140(v)(2).
298. *Id.* § 1798.121(a).
299. *See id.* § 1798.140(v)(2).
300. Memorandum from Andrew J. Pincus et al., Mayer Brown LLP, to Christopher Mohr et al., (Jan. 24, 2019) [https://perma.cc/YJ4E-WPUY].
301. *See* CAL. CIV. CODE § 1798.140(v)(2).
302. *Id.*

While these exceptions might address the most obvious First Amendment arguments, the most troublesome problem for the statute lies in its failure to meaningfully address the privacy harms of FRT. Even when the Court analyzed the Vermont statute in *Sorrell* as a restriction on commercial speech, it failed intermediate scrutiny because the law could not be said to actually further the privacy interests proffered by the government; it permitted disclosure of the prescriber-identifying information for a wide variety of other purposes, including health care research and journalism.[303] In this way, perhaps the most problematic outcome of the case was that it has put legislatures in the double-bind of taking an all-or-nothing approach to privacy laws: either they must protect privacy to the detriment of socially valuable uses of the information, or they cannot regulate the information at all. From a more optimistic perspective, the main outcome of *Sorrell* is that legislatures must carefully consider how a statute will actually protect against given privacy harms and only create exceptions when they would not endanger the statute's objectives.

With *Sorrell*'s lesson in mind, I suggest that the statute be modified to require affirmative consent before a business may collect faceprints for any purpose; given the ease with which faceprints can be captured without a consumer's knowledge, it is difficult to explain how an opt-out framework would provide the level of notice and control necessary to alleviate chilling effects that stem from the possibility that one is being watched. Even if one could install software to make their privacy preferences known to apps and websites,[304] it would be wholly unrealistic to assume that a person could communicate a deletion or opt-out request to all businesses that the person passes by when walking on the street. Further, as the CCPA/CPRA currently stand, those requests would be ineffective if the data has already been sold; the deletion right applies only to businesses with a direct relationship to the consumer and does not apply to downstream possessors.[305] Instead, giving consumers control at the moment their faceprints are captured would allow them to choose which businesses they would like to entrust with their sensitive data.

303. Sorrell v. IMS Health Inc., 564 U.S. 552, 572–73 (2011).
304. For a discussion of global opt-outs, see Kaminski et al., *supra* note 282, at 170, 193–94.
305. *See* CAL. CIV. CODE § 1798.105(a); Kaminski et al., *supra* note 282, at 192–93.

V. CONCLUSION

In a brief filed in support of Clearview's motion to dismiss, various amici criticize the plaintiffs for "convert[ing] a descriptive account into a prescriptive one."[306] In other words, just because we have grown accustomed to a certain level of obscurity does not mean that it is the most desirable level.[307] Time may prove them correct; maybe the level of obscurity in which we currently live is truly undesirable.

But maybe it isn't. And if privacy expectations continue playing a role in determining whether one has experienced a legally cognizable privacy harm that might outweigh undoubtedly important First Amendment interests, the problem is that sitting back and waiting for harms to reveal themselves will come too late. It would be extremely difficult for a person to be able to convincingly argue they have a reasonable expectation that a corporation will not collect their faceprint when corporations have been doing so for years. Moreover, if legislatures are not able to control the collection and dissemination of faceprints, it will be impossible for consumers to claw back that data years after it has already been in circulation. In other words, failing to regulate FRT now may well make it impossible to regulate at all.

These concerns about facial recognition technology go beyond the "offensiveness" of speech that drives other speech restrictions. FRT does not merely offend a person's sense of propriety the way the word "fuck" on a t-shirt might. Nor does it merely seek to redress individual senses of embarrassment. It presents real risks that threaten our ability to navigate the world with some degree of control over who we expose ourselves to. Further, it serves as yet another powerful tool for Big Data to tighten its grip on consumers.

I conclude by reiterating that determining that states *can* regulate FRT does not mean that they must. Perhaps, as has been suggested with HIPAA, compliance with biometric rules will be too costly for our society.[308] Or, as some suggest, we may ultimately choose that the benefits of widespread FRT outweigh the costs.[309] To draw from an oft-used metaphor in privacy literature, sunshine might well be the

306. Brief of Amici First Amendment Clinic at Duke Law and Professors of Law Eugene Volokh and Jane Bambauer in Support of Defendant's Motion to Dismiss at 11–12, ACLU v. Clearview AI, Inc., No. 2020CH04353 (Ill. Cir. Ct. Dec. 3, 2020) [hereinafter Brief of Amici First Amendment Clinic].

307. *See id.*

308. Bambauer, *supra* note 187, at 264.

309. *See* Brief of Amici First Amendment Clinic, *supra* note 306, at 18–19.

best disinfectant. But the First Amendment does not require us to relegate ourselves to our homes to avoid its blinding light.