RESISTING FACE SURVEILLANCE WITH COPYRIGHT LAW*

AMANDA LEVENDOWSKI**

Face surveillance is animated by deep-rooted demographic and deployment biases that endanger marginalized communities and threaten the privacy of all. But current approaches have not prevented its adoption by law enforcement. Some companies have offered voluntary moratoria on selling the technology, leaving many others to fill in the gaps. Legislators have enacted regulatory oversight at the state and city levels, but a federal ban remains elusive. Both approaches require vast shifts in practical and political will, each with drawbacks. While we wait, face surveillance persists. This Article suggests a new possibility: face surveillance is fueled by unauthorized copies and reproductions of photographs, and resisting face surveillance compels us to consider countering it with copyright law.

So why haven't face surveillance companies been overwhelmed with copyright infringement litigation? Fair use. This Article lays out the litigation landscape before analyzing the recent Supreme Court decision in Google v. Oracle*, alongside other key fair use cases, to examine why this complex doctrine may permit many uses of machine learning without allowing face surveillance to copy and reproduce online profile pictures. Some face surveillance companies claim to be transformative search engines, but their business models are more like private subscription services that are rarely found to be fair use. And scraping profile pictures harms the unique licensing market for these photographs, which grows as companies and researchers increasingly reject scraped photos as sources of face analysis training data. This Article concludes that copyright law could curtail*

** Associate Professor of Law at Georgetown University Law Center. Thanks to Kendra Albert, Lindsey Barrett, Alvaro Bedoya, Barton Beebe, Erin Carroll, Anupam Chander, Julie Cohen, Karin Dryhurst, Dan Ernst, Megan Graham, Gautam Hans, Woody Hartzog, Meg Leta Jones, Brett Max Kaufman, Harry Levin, Christy Lopez, Chris Morten, Laura Moy, Paul Ohm, Blake Reid, Em Richardson, Matthew Sag, Abbe Smith, Gerry Spann, Erik Stallman, Madhavi Sunder, Kristen Tiscione, Carrie Toole, Rebecca Wexler, and Cameron Tepski for their thoughtful and generous comments. Dan Bateyko, Eve Maynard, Taylor Pigram, and Shadé Oladetimi provided brilliant research assistance. This Article benefitted from presentation to the Junior Law and Tech* Scholars, Georgetown Faculty Workshop, the Southeastern Association of Law Schools Conference, Intellectual Property Law Scholars Conference, the Clinical Law Review Writers' Workshop, the Legal Scholars Roundtable on Artificial Intelligence, and the University of Virginia Faculty Workshop. I am deeply grateful to the Georgetown Gender+ Justice Initiative for a grant that supported this research.

face surveillance without waiting for companies or Congress to catch up—and we ought to use it.

INTRODUCTION

In January 2020, Robert Julian-Borchak Williams was arrested on his front lawn while his wife and two daughters watched.[1] He had no idea why he was being arrested. Officers declined to say why or much else, even telling his wife to "Google it" when she asked where they were taking him.[2] Williams found himself at the Detroit Detention Center, where he spent the night in jail before the officers let him take a good look at the blurry surveillance photograph behind his arrest.[3] "I hope you guys don't think that all [B]lack men look alike," Williams said, holding the surveillance video still next to own face.[4] It was

1. Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/28ZL-W6DW (dark archive)] (Aug. 3, 2020) [hereinafter Hill, *Wrongfully Accused*].

2. Bobby Allyn, *'The Computer Got It Wrong': How Facial Recognition Led to False Arrest of Black Man*, NPR, https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig [https://perma.cc/WQ8M-K4V2] (June 24, 2020, 9:05 PM).

3. Hill, *Wrongfully Accused*, *supra* note 1.

4. Robert Williams, Opinion, *I Was Wrongfully Arrested Because of Facial Recognition. Why Are Police Allowed To Use It?*, WASH. POST (June 24, 2020), https://www.washingtonpost.com/opinions/2020/06/24/i-was-wrongfully-arrested-because-facial-recognition-why-are-police-allowed-use-this-technology/ [https://perma.cc/PE6R-JCJV (dark archive)].

obviously not him. A detective explained the problem: "[T]he computer must have gotten it wrong."[5]

Williams was misidentified by a face recognition algorithm developed by a company called DataWorks Plus,[6] which is one of many companies in the business of selling face recognition technology to law enforcement.[7] The same month that Williams was arrested, journalist Kashmir Hill revealed that a startup called Clearview AI was snapping up selfies and profile pictures to create a massive face recognition database for law enforcement.[8] In less than three years, Clearview AI systemically copied three billion photographs to create face recognition tools for six hundred police departments, all without the consent of individuals, authorization of social media companies, or knowledge of the public.[9] Backlash was swift. Within days, the largest social media companies alleged that Clearview AI's unauthorized scraping of their websites violated their terms of service—at that time an arguable violation of the

5. *Id.* Williams continued to be held until that evening, totaling thirty hours in detention. *Id.* In response, the American Civil Liberties Union of Michigan filed a letter with the Detroit Police Department. Letter from Phil Mayor, Senior Staff Att'y, ACLU Fund of Michigan, to Off. of the Chief Investigator, Detroit Pub. Safety (June 24, 2020), https://www.aclu.org/letter/aclu-michigan-complaint-re-use-facial-recognition [https://perma.cc/S3CA-PZCL].

6. Hill, *Wrongfully Accused*, *supra* note 1. The company got its start offering mugshot-management software. *Id.*

7. Other providers include NEC, Ayonix Corporation, and Clearview AI. Jared Council, *Facial Recognition Companies Commit To Police Market After Amazon, Microsoft Exit*, WALL ST. J. (June 12, 2020, 5:28 PM), https://www.wsj.com/articles/facial-recognition-companies-commit-to-police-market-after-amazon-microsoft-exit-11591997320 [https://perma.cc/FH6K-UNDD (dark archive)].

8. Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/QF3A-L55Z (dark archive)] (Nov. 2, 2021) [hereinafter Hill, *The Secretive Company*]. Private customers, including those experimenting with the technology on an unpaid trial basis, included banks, retail stores, and sports franchises. Ryan Mac, Caroline Haskins & Logan McDonald, *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA*, BUZZFEED NEWS, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement [https://perma.cc/8A9X-JRES] (Feb. 27, 2020, 11:37 PM). Clearview AI was not the only company using scraped photographs to power its face surveillance technology. Olivia Solon, *Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped Without Consent*, NBC NEWS, https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n98192 [https://perma.cc/6GXV-PY5Q] (Mar. 17, 2019, 11:25 AM).

9. Hill, *The Secretive Company*, *supra* note 8. That number has since skyrocketed to ten billion. Will Knight, *Clearview AI Has New Tools To Identify You in Photos*, WIRED (Oct. 4, 2021, 7:00 AM), https://www.wired.com/story/clearview-ai-new-tools-identify-you-photos/ [https://perma.cc/3KKK-GZ9V (dark archive)]. For an accounting of why the public is so rarely part of the surveillance technology procurement process, see generally the illuminating work of Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. L. REV. 1595 (2016) and Ira S. Rubinstein, *Privacy Localism*, 93 WASH. L. REV. 1961 (2018). *See also* Amanda Levendowski, *Trademarks as Surveillance Transparency*, 36 BERKELEY TECH. L.J. (forthcoming 2022) (manuscript at 4–5) (on file with Berkeley Technology Law Journal) (recommending the use of the federal trademark register to investigate new, secret surveillance technologies).

Computer Fraud and Abuse Act.[10] The public balked at the violation and began strategizing about how to resist it.[11]

Face surveillance is a broad term that embraces multiple biometric systems that use algorithms to analyze faces, such as face detection, face classification, and, as emphasized here, face recognition.[12] Concerns over face surveillance are far from new. Legal scholars have expressed wariness over the use of face recognition technology in classrooms,[13] by corporations,[14] or during carceral investigations.[15] Julie Cohen's vision of the biopolitical domain warned of the

10. Alfred Ng & Steven Musil, *Clearview AI Hit with Cease-and-Desist from Google, Facebook over Facial Recognition Collection*, CNET (Feb. 5, 2020, 6:10 PM), https://www.cnet.com/news/clearview-ai-hit-with-cease-and-desist-from-google-over-facial-recognition-collection/ [https://perma.cc/MR8L-Z7U2]; *see also* 18 U.S.C. § 1030; Van Buren v. United States, 141 S. Ct. 1648, 1659 n.8 (2021) ("For present purposes, we need not address whether this inquiry turns only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies.").

11. *See infra* Part II.

12. *See Face Surveillance*, LAW INSIDER (Jan. 17, 2022, 12:50 PM), https://www.lawinsider.com/dictionary/face-surveillance [https://perma.cc/K9KY-MW2T] (defining "face surveillance"); *see also Face Recognition Technology*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology [https://perma.cc/49K2-WY98] ("Facial recognition systems are built on computer programs that analyze images of human faces for the purpose of identifying them.").

13. *See, e.g.*, Nila Bala, *The Danger of Facial Recognition in Our Children's Classrooms*, 18 DUKE L. & TECH. REV. 249 (2020) (discussing the implications of facial recognition on children's privacy, development, and existing inequities); Lindsey Barrett, *Ban Facial Recognition Technologies for Children—and for Everyone Else*, 26 B.U. J. SCI. & TECH. L. 223 (2020) (discussing how young people have less say over where they go and what they do, making them exceptionally vulnerable to facial recognition technologies). *See generally* Lindsey Barrett, *Rejecting Test Surveillance in Higher Education*, 2023 MICH. ST. L. REV. (forthcoming 2023) (discussing the prevalence of facial recognition and adjacent technology in remote-proctoring software).

14. *See generally, e.g.*, Yana Welinder, *A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks*, 26 HARV. J.L. & TECH. 165 (2012) (discussing proposed privacy requirements of social network companies); Elizabeth A. Rowe, *Regulating Facial Recognition Technology in the Private Sector*, 24 STAN. TECH. L. REV. 1 (2020) (posing guided questions to outline potential facial recognition regulation); Kerri A. Thompson, *Countenancing Employment Discrimination: Facial Recognition in Background Checks*, 8 TEX. A&M L. REV. 63 (2020) (positing that the technology that made facial recognition viable also has discriminatory implications in the employment context).

15. *See generally, e.g.*, Sabrina A. Lochner, *Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans*, 55 ARIZ. L. REV. 201 (2013) (discussing law enforcement's use of the Mobile Offender Recognition and Information System and associated privacy and policy concerns); Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105 (2021) (revealing limitations of the Fourth Amendment in constraining the increasing use of facial surveillance and artificial intelligence by law enforcement); Matthew Doktor, *Facial Recognition and the Fourth Amendment in the Wake of* Carpenter v. United States, 89 U. CIN. L. REV. 552 (2021) (discussing the Court's extension of Fourth Amendment privacy rights to modern law enforcement technology). Civil society also raised alarm bells over the corporate use of face recognition to surveil Black tenants in rent-controlled buildings. *See* Tranae' Moran, Fabian Rogers & Mona Patel, *Tenants Against Facial Recognition: AI Now 2019 Symposium*, YOUTUBE (Oct. 15, 2019), https://youtu.be/7VUAdVrkFuw [https://perma.cc/FUA7-SERF]; Tranae' Moran, *Atlantic Plaza Towers Tenants Won a Halt to Facial Recognition in Their Building: Now They're Calling on a Moratorium on All Residential Use*, MEDIUM (Jan. 9, 2020), https://medium.com/@AINowInstitute/atlantic-plaza-towers-tenants-won-a-halt-to-facial-recognition-in-their-building-now-theyre-274289a6d8eb [https://perma.cc/A6Z6-WURK]; *see also* Ginia Bellafante, *The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why?*, N.Y.

rise of business models premised on turning publicly available information into corporate assets.[16] Helen Nissenbaum urged that definitions of privacy could not discount protecting "vast stores of information—even so-called 'public' information" used to surveil people, and Joel Reidenberg predicted that face recognition would create confusion about the "appropriate treatment of publicly available personal information."[17] Evan Selinger and Woodrow Hartzog concluded that the confusion is settled, putting the current calculus bluntly: "[F]acial recognition technology is the most uniquely dangerous surveillance mechanism ever invented."[18] Other scholars—including legal scholars Danielle Citron, Clare Garvie, Alvaro Bedoya, Margaret Hu, Ari Waldman, Rashida Richardson, Laura Moy, and Vincent Southerland and sociotechnical scholars Safia Umoja Noble, Virginia Eubanks, and Ruha Benjamin—have long established that the burdens of biased algorithms are borne by marginalized people.[19]

TIMES (Mar. 28, 2019), https://www.nytimes.com/2019/03/28/nyregion/rent-stabilized-buildings-facial-recognition.html [https://perma.cc/Z723-XP6C (dark archive)]. Thanks to Megan Graham for highlighting the residential use of face surveillance.

16. *See* Julie E. Cohen, *The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy*, 31 PHIL. & TECH. 213, 213 (2018); *see also* Julie E. Cohen, *What Privacy Is for*, 126 HARV. L. REV. 1904, 1921–27 (2013).

17. Helen Nissenbaum, *Toward an Approach to Privacy in Public: Challenges of Information Technology*, 7 ETHICS & BEHAV. 207, 208 (1997); Joel R. Reidenberg, *Privacy in Public*, 69 U. MIA. L. REV. 141, 142 (2014).

18. Woodrow Hartzog & Evan Selinger, *Facial Recognition Is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66 [https://perma.cc/75PM-XMJ7 (dark archive)]; *see also* Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOY. L. REV. 33 (2020). Luke Stark has compared the technology to plutonium, explaining that "[i]t's dangerous, racializing, and has few legitimate uses" requiring "regulation and control on par with nuclear waste." Luke Stark, *Facial Recognition Is the Plutonium of AI*, 25 XRDS, Spring 2019, at 50, 50.

19. *See, e.g.*, Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1256 (2008) (providing an example of how biased algorithms disproportionately affect poor people); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014) (marginalized people); Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *Unregulated Police Face Recognition in America*, PERPETUAL LINE-UP (Oct. 18, 2016), https://www.perpetuallineup.org/findings/racial-bias [https://perma.cc/8HJX-UYDF] (women of color); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016) (protected classes under Title VII); ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017) (people of color); Margaret Hu, *Algorithmic Jim Crow*, 86 FORDHAM L. REV. 633 (2017) (people of color); Amanda Levendowski, *How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem*, 93 WASH. L. REV. 579 (2018) [hereinafter Levendowski, *Copyright Law*] (women, people of color, and queer people); Ari Ezra Waldman, *Power, Process, and Automated Decision-Making*, 88 FORDHAM L. REV. 613, 622 (2019) (people of color, women, and poor people); Rashida Richardson, Jason M. Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. REV. ONLINE 15 (2019) (people of color); Sandra G. Mayson, *Bias In, Bias Out*, 128 YALE L.J. 2218 (2019) (people of color); Ifeoma Ajunwa, *The Paradox of Automation as Anti-Bias Intervention*, 41 CARDOZO L. REV. 1671 (2020) (women and people of color); Laura M. Moy, *A Taxonomy of Police Technology's Racial Inequity Problems*, U. ILL. L. REV. 139 (2021) (people of color);

Nearly a decade of scholarship rooted in lived experiences reveals an urgent need for a federal law banning the use of face surveillance by law enforcement.[20] To be truly effective, a federal ban on face surveillance must include a ban of private face recognition technologies that directly or indirectly support law enforcement investigations—which, at some level, may be all of them.[21] But waiting for such legislation is a luxury few can afford.[22] This Article argues that there is previously unexplored law that could be used to resist invasive face surveillance in the meantime: copyright law. Photographs used as profile pictures, both on social media networks and other websites, are protectable by copyright, and the unauthorized copies created and reproduced by some face recognition companies constitute copyright infringement barring an exception.[23]

This Article seeks to answer Jeanne Fromer's thoughtful question of whether we should care why intellectual property rights are asserted.[24] Part I

Vincent M. Southerland, *The Intersection of Race and Algorithmic Tools in the Criminal Legal System*, 80 MD. L. REV. 487 (2021) (people of color); Ngozi Okidegbe, *Discredited Data*, 107 CORNELL L. REV. (forthcoming 2022) (poor people and people of color). For sociotechnical explorations of algorithmic bias, see CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016) (women, people of color, and poor people); Kristian Lum & William Isaac, *To Predict and Serve?*, SIGNIFICANCE, Oct. 2016, at 14 (people of color); SAFIA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM (2018) (women and people of color); MEREDITH BROUSSARD, ARTIFICIAL UNINTELLIGENCE: HOW COMPUTERS MISUNDERSTAND THE WORLD (2018) (poor people and people of color); VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR (2018) (poor people); RUHA BENJAMIN, RACE AFTER TECHNOLOGY: ABOLITIONIST TOOLS FOR THE NEW JIM CODE (2019) (people of color); Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACHINE LEARNING RES. 77 (2018) (women and people of color); Inioluwa Deborah Raji & Joy Buolamwini, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products*, 2019 CONF. ON A.I. ETHICS & SOC. 429 (women and people of color). Algorithmic bias in face recognition technology is also central in the documentary film CODED BIAS (7th Empire Media 2020).

20. This echoes the ask to the Biden administration made by thirty social justice organizations in December 2020. Dean DeChiaro, *Advocates To Press Biden, Congress on Facial Recognition Curbs*, ROLL CALL (Dec. 8, 2020, 6:30 AM), https://www.rollcall.com/2020/12/08/advocates-to-press-biden-congress-on-facial-recognition-curbs/ [https://perma.cc/H67E-YVDS]. The urgent need for a federal bill is not news to Congress. *See infra* Section II.B.

21. For an in-depth discussion of how private surveillance technologies can prove just as problematic as law enforcement surveillance technologies, see generally Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 91 N.Y.U. L. REV. ONLINE 19 (2017).

22. More than 117 million adults are believed to be in face recognition databases. Garvie et al., *supra* note 19.

23. 17 U.S.C. § 102(a), (a)(5) ("Copyright protection subsists . . . in original works of authorship fixed in any tangible medium of expression . . . . Works of authorship include . . . pictorial, graphic, and sculptural works . . . ."); *id.* § 106 ("[T]he owner of copyright under this title has the exclusive rights to do and to authorize any of the following . . . to reproduce the copyrighted work in copies or phonorecords . . . .").

24. Jeanne C. Fromer, *Should the Law Care Why Intellectual Property Rights Have Been Asserted?*, 32 HOUS. L. REV. 549, 549 (2015).

traces the injustices of face surveillance through two of its baked-in biases—demographic biases affecting the accuracy of face analysis technology and deployment biases driving its use against marginalized communities—to establish the urgency of thinking creatively about combatting face surveillance. As Part II explains, existing approaches to resisting face recognition, including awaiting corporations to stop selling face surveillance technology to law enforcement or pursuing local legislation banning or regulating the technology, require vast shifts in practical or political will, each with its own drawbacks.[25] While we wait, face surveillance becomes more entrenched in society, which is why Part III explores how existing copyright law could provide a desperately necessary fix. Part III outlines the contours of copyright infringement litigation and analyzes why fair use—the key infringement exception—may not apply to face surveillance companies' practice of copying profile pictures to use as face surveillance training data and reproducing those photographs in face match reports used by law enforcement. Lawsuits over machine learning ("ML"), like face surveillance, will draw out the full complexities of the fair use doctrine, and many uses of copyrighted works as training data will be fair use.[26] But face surveillance may be the exception to the rule that ML is fair use.

This Article should not need to exist. Not all privacy issues are copyright ones—and they should not be.[27] But decades of lobbying created a Congress that cares more about conserving copyrights than protecting privacy,[28] and the

25. Others have pursued creative litigation. The Vermont Attorney General is suing Clearview AI for violation of its unfair and deceptive acts or practices act. Complaint at 1, State v. Clearview AI, Inc., No. 226-3-20 (Vt. Super. Ct. Mar. 10, 2020) [hereinafter Vermont Clearview AI Complaint]; Ruling on Defendant's Motion to Dismiss at 38, *Clearview AI*, No. 226-3-20 (Vt. Super. Ct. Sept. 10, 2020) (order granting Clearview AI's motion to dismiss on two counts and denying motion to dismiss on all other counts). Additionally, Mijente, NorCal Resist, and four individual plaintiffs are suing Clearview AI and alleging misappropriation of likeness under California law. Complaint, Renderos v. Clearview AI, Inc., No. 21-cv-05286 (N.D. Ill. filed Mar. 9, 2021, in Cal. Super. Ct. as No. RG21091138) [hereinafter Renderos Complaint].

26. *See* Levendowski, *Copyright Law*, *supra* note 19, at 619–30; Mark A. Lemley & Bryan Casey, *Fair Learning*, 99 TEX. L. REV. 743, 748–49 (2021). *But see* Benjamin L.W. Sobel, *Artificial Intelligence's Fair Use Crisis*, 41 COLUM. J.L. & ARTS 45, 45–46 (2017) (observing that invoking fair use for fairer ML may have costs, such as shifting valuable innovation elsewhere or diverting earnings away from authors).

27. *Compare* Garcia v. Google, Inc., 786 F.3d 733 (9th Cir. 2015) (attempting to distort copyright law to shield actor from displaying her performance in a public film), *with* Complaint, Jane Doe v. Elam, No. 14-cv-09788 (C.D. Cal. Dec. 22, 2014) (invoking existing copyright law to sue persistent distributor of nonconsensual pornography). Jane Doe was awarded $450,000 for copyright infringement, part of the largest judgment in any nonconsensual pornography case to date. Christine Hauser, *$6.4 Million Judgment in Revenge Porn Case Is Among Largest Ever*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/us/revenge-porn-california.html [https://perma.cc/QU8L-JC2W (dark archive)].

28. *See* JESSICA LITMAN, DIGITAL COPYRIGHT 19, 61–65 (2017) (detailing lobbying efforts surrounding copyright term extension); Christopher Buccafusco & Paul J. Heald, *Do Bad Things Happen When Works Enter the Public Domain?: Empirical Tests of Copyright Term Extension*, 28 BERKELEY TECH. L.J. 1, 6–10 (2013) (same).

suggestion that copyright is our best short-term hope at resisting face recognition technology reveals deep flaws in our legal system that should be critiqued, not celebrated.[29] Ultimately, face recognition by law enforcement should be eliminated because it poses an existential threat to privacy and dignity, not because the technology appears to depend on copyright infringement.[30] Yet it does. Until the federal government bans face recognition software, copyright law may be able to shield us from the most insidious forms of face surveillance by holding corporate creators civilly liable.[31] This Article concludes that we should care when copyright is weaponized for censorship or harassment. But if copyright law can curtail face surveillance without waiting for action from companies or Congress, then we should use it.

I. IDENTIFYING INJUSTICES OF FACE SURVEILLANCE

The algorithms used in every ML system are subject to biases, and the ones underpinning face surveillance complicate any quest for justice. Multiple factors play into the biases of algorithms like those behind face surveillance technology, from homogenous communities of creators and flawed algorithms to incomplete or mislabeled datasets.[32] These problems are so pernicious that tracks of academic conferences, even entire conferences themselves, are dedicated to the development of "fairer" artificial intelligence ("AI").[33] And when it comes to face surveillance, these problems are impossible to ignore. The biases embodied by face surveillance ensure that justice will remain elusive.

29. Indeed, some scholars oppose such an invocation of copyright law. *See infra* Part III.

30. A similar dynamic was observed with Reddit's decision to remove the subreddits trafficking in hacked nonconsensual pornography of celebrity women in response to copyright takedown notices rather than doing so out of respect for the victims' privacy and dignity. Sarah Jeong, *Reddit as a Government*, FORBES (Sept. 8, 2014, 3:12 PM), https://www.forbes.com/sites/sarahjeong/2014/09/08/reddit-as-a-government/?sh=6fd7c8d1856d [https://perma.cc/RG63-GJYL (dark archive)].

31. *See* 17 U.S.C. § 504(c)(2) (providing statutory damages for infringement). It is no surprise that copyright law is, in the words of Cathay Smith, a tool "par excellence." Cathay Y.N. Smith, *Weaponizing Copyright*, 35 HARV. J.L. & TECH. (forthcoming 2022) (manuscript at 34) [hereinafter Smith, *Weaponizing Copyright*], https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3806015 [https://perma.cc/6WC4-3U5Q].

32. *See* Levendowski, *Copyright Law*, *supra* note 19, at 583–85. For a foundational discussion of bias in computer systems, see generally Batya Friedman & Helen Nissenbaum, *Bias in Computer Systems*, 14 ACM TRANSACTIONS ON INFO. SYS. 330 (1996).

33. *See, e.g.*, ACM CONF. ON FAIRNESS ACCOUNTABILITY & TRANSPARENCY (ACM FAccT), https://facctconference.org/ [https://perma.cc/9SEU-G7EY]. "Fairness" also occupies an outsized focus in scholarship. *See, e.g.*, KIMMO KÄRKKÄINEN & JUNGSEOCK JOO, FAIRFACE: FACE ATTRIBUTE DATASET FOR BALANCED RACE, GENDER, AND AGE FOR BIAS MEASUREMENT AND MITIGATION 2–3 (2019), https://arxiv.org/pdf/1908.04913.pdf [https://perma.cc/6WZ3-BV8P] (creating a "fair" dataset treating "Latino [as] a race, which can be judged from the facial appearance" and including only binary genders). Crucially, no one can quite agree on what "fairness" means. Arvind Narayanan, *Tutorial: 21 Fairness Definitions and Their Politics*, YOUTUBE (2018), https://www.youtube.com/watch?v=jIXIuYdnyyk [https://perma.cc/U9SR-2M3Q] (describing definitions of fairness at the 2018 ACM FAT* Conference). FAT* is the predecessor of FAccT.

The literal lens through which we view faces has always been biased. When photography became popularized in the 1950s, Black parents found that the photographs reduced their children to "ink blots."[34] Erasing the visibility of Black subjects was done by design. At Kodak Eastman, a model on staff named Shirley became the metric for calibrating the printed color stock used by cameras.[35] Kodak photographed Shirley against bland backgrounds with bright lighting to determine how skin would look in high-contrast environments.[36] Of course, Shirley was white.[37] Kodak only began correcting its cameras' biases after receiving complaints—not from Black parents, but from chocolate and furniture companies saying they "weren't getting the right brown tones" on product photographs.[38]

Today, photographers still struggle to capture Black skin accurately.[39] As Simone Browne details, face scan technology fails "'very dark-skinned users,'

34. Ainissa Ramirez, *How 20th Century Camera Film Captured a Snapshot of American Bias*, TIME (July 24, 2020, 4:44 PM), https://time.com/5871502/film-race-history/ [https://perma.cc/DYE3-P4Z9 (staff-uploaded, dark archive)]. The medium itself betrays systemic biases: the earliest known photograph of African Americans in the United States depicts enslaved people picking cotton on a plantation. Brigit Katz, *This May Be the Earliest Known Image of Enslaved Individuals with Cotton*, SMITHSONIAN MAG. (Dec. 6, 2019), https://www.smithsonianmag.com/smart-news/may-be-earliest-known-image-slaves-cotton-180973705/ [https://perma.cc/86WH-PPVJ].

35. Code Switch, *Light and Dark: The Racial Biases That Remain in Photography*, NPR (Apr. 16, 2014, 3:35 PM), https://www.npr.org/sections/codeswitch/2014/04/16/303721251/light-and-dark-the-racial-biases-that-remain-in-photography [https://perma.cc/AX53-45ZE].

36. *Id.*

37. These cards were known as Shirley Cards, and a multiracial Shirley Card featuring a Black woman, a white woman, and an Asian woman was not introduced until the mid-1990s. Sarah Lewis, *The Racial Bias Built into Photography*, N.Y. TIMES (Apr. 25, 2019), https://www.nytimes.com/2019/04/25/lens/sarah-lewis-racial-bias-photography.html [https://perma.cc/5AJF-9GHZ (dark archive)].

38. *Id.* (quoting Lorna Roth, *Looking at Shirley, the Ultimate Norm: Colour Balance, Image Technologies, and Cognitive Equity*, 34 CANADIAN J. COMM. 111, 119 (2009)).

39. Famed photographer Annie Leibovitz and *Vogue* magazine were criticized for failing to accurately capture Simone Biles's skin tone in a recent cover story. *See* Abby Aguirre, *Simone Biles on Overcoming Abuse, Postponed Olympics, and Training During a Pandemic*, VOGUE (July 9, 2020), https://www.vogue.com/article/simone-biles-cover-august-2020 [https://perma.cc/R2SB-MD7A (dark archive)]; DL Cade, *Vogue Slammed for Hiring Annie Leibovitz for Simone Biles Cover Instead of Black Photographer*, PETAPIXEL (July 13, 2020), https://petapixel.com/2020/07/13/vogue-slammed-for-hiring-annie-leibovitz-for-simone-biles-cover-instead-of-black-photographer/ [https://perma.cc/DF5H-4K2G] (sharing critiques from prominent photographers, photo editors, and Black Women Photographers founder Polly Irungu); Anete Lusina, *Vogue and Annie Leibovitz Under Criticism for Badly Lit Photos of Gymnast Simone Biles, Raising Another Discussion About Lack of Diversity*, FSTOPPERS (July 19, 2020), https://fstoppers.com/news/vogue-and-annie-leibovitz-under-criticism-badly-lit-photos-gymnast-simone-biles-499513 [https://perma.cc/D3VA-P4DC]. If an artist like Leibovitz cannot get the lighting right, imagine the challenges with analyzing grainy CCTV footage. But the failure is just as likely to be user error, as demonstrated by gorgeous cover shoots of Michaela Coel or Viola Davis by Black photographers. *See* E. Alex Jung, *Michaela the Destroyer*, VULTURE (July 6, 2020), https://www.vulture.com/article/michaela-coel-i-may-destroy-you.html#_ga=2.207146203.992060006.1618513076-1250292094.1606755378 [https://perma.cc/3HZF-7AAA (staff-uploaded, dark archive)] (featuring photography by Nigerian photographer Ruth Ossai); Sonia Saraiya, *Viola Davis: "My Entire Life Has Been a Protest*," VANITY FAIR (July 14, 2020), https://www.vanityfair.com/hollywood/2020/07/

not due to 'lack of distinctive features, of course, but to the quality of the images provided to the facial-scan system by video cameras optimized for lighter-skinned users.'"[40] Similarly, face detection systems built into cameras struggle to recognize Black skin at all. Less than five years ago, Hewlett-Packard was taken to task for developing a face detection algorithm that worked seamlessly for white people but failed to track Black people entirely.[41] Today, face surveillance renders people of color invisible when they benefit from it but hypervisible when law enforcement can.[42]

As Laura Moy has thoughtfully taxonomized, police technology—like face surveillance—is developed and deployed against a backdrop of biases that can replicate, mask, transfer, and exacerbate inequity in policing, as well as compromise oversight of that inequity.[43] Historically, two white men working for law enforcement pioneered face recognition by relying on photographs of arrested men—commonly known as mugshots—to develop their methodologies.[44] Arrested men became training data without their consent, an

cover-story-viola-davis [https://perma.cc/YCJ5-LMDR (dark archive)] (featuring photography by African American photographer Dario Calmese, the first Black photographer to shoot a cover for *Vanity Fair*). In the television realm, Issa Rae's series *Insecure* has won awards for its lighting of Black skin. *How 'Insecure' Lights Its Actors So Well*, MIC (Sept. 11, 2017), https://www.facebook.com/micmedia/videos/1644358292253621 [https://perma.cc/VM2P-AV6D]; *see also* Nadia Latif, *It's Lit! How Film Finally Learned To Light Black Skin*, GUARDIAN (Sept. 21, 2017, 12:26 PM), https://www.theguardian.com/film/2017/sep/21/its-lit-how-film-finally-learned-how-to-light-black-skin [https://perma.cc/ASC7-E6WT (staff-uploaded, dark archive)]. For a first-person account of cameras' bias, see Syreeta McFadden, *Teaching the Camera To See My Skin*, BUZZFEED (Apr. 2, 2014, 8:01 PM), https://www.buzzfeednews.com/article/syreetamcfadden/teaching-the-camera-to-see-my-skin [https://perma.cc/ZU8A-V3UA].

40. SIMONE BROWNE, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS 113 (2015) (quoting SAMIR NANAVATI, MICHAEL THIEME & RAJ NANAVATI, BIOMETRICS: IDENTITY VERIFICATION IN A NETWORKED WORLD 37 (2002)).

41. wzamen01, *HP Computers Are Racist*, YOUTUBE (Dec. 10, 2009), https://www.youtube.com/watch?v=t4DT3tQqgRM&feature=youtu.be [https://perma.cc/U8P9-VBPU]. This same sort of algorithmic invisibility inspired Joy Buolamwini to pioneer the Algorithmic Justice League. CODED BIAS (7th Empire Media 2020).

42. For a discussion of the relationship between photography and Blackness, see Ainissa G. Ramirez, *Black Images Matter: How Cameras Helped—and Sometimes Harmed—Black People*, SCI. AM. (July 8, 2020), https://www.scientificamerican.com/article/black-images-matter-how-cameras-helped-mdash-and-sometimes-harmed-mdash-black-people/ [https://perma.cc/XCF5-2KYG (staff-uploaded, dark archive)]. Cameras have failed people of color as an accountability mechanism for law enforcement, as evidenced by the ways that body-worn camera footage and videos of police brutality fail to translate into meaningful accountability. *See id.*

43. Moy, *supra* note 19, at 143–44.

44. The men were Alphonse Bertillon, a Parisian police officer who invented mugshots in the nineteenth century, and Woody Bledsoe, a Ph.D. graduate working in Silicon Valley who pioneered computerized face recognition on behalf of law enforcement in the 1960s. *See* Hansi Lo Wang, *Meet Alphonse Bertillon, the Man Behind the Modern Mug Shot*, NPR (Mar. 8, 2016, 6:21 PM), https://www.npr.org/2016/03/08/469174753/meet-alphonse-bertillon-the-man-behind-the-modern-mug-shot [http://perma.cc/NS6B-QBBD]; Sahil Chinov, *The Racist History Behind Facial Recognition*, N.Y. TIMES (July 10, 2019), https://www.nytimes.com/2019/07/10/opinion/facial-recognition-race.html [https://perma.cc/5LED-DB6B (dark archive)] (describing Bertillon as a "facial analysis pioneer"). For a

objection levied against some of the most prolific datasets in face recognition today.[45] As a result, face recognition is inextricably coupled with lack of consent and perceived criminality.[46]

This part explores two of the contemporary biases that animate face recognition: demographic and deployment biases. Demographically, face recognition reflects and amplifies the biases of the camera itself. Study after study across different forms of face surveillance—including face characterization and face recognition—demonstrate empirically that face surveillance performs poorly for people of color, women, and young people, and it often excludes or misgenders transgender and nonbinary people.[47] But fixing demographic biases cannot fix face recognition. Even if face recognition was accurate, past and present practices show us that face surveillance will be deployed disproportionately against marginalized people.[48] Even when face recognition is sometimes turned on the powerful,[49] people of color, immigrants, and sex workers remain persistent targets of the technology.[50]

Technology that creates a more efficient carceral system should be resisted. The imbalanced power dynamics inherent in face surveillance's demographic and deployment biases suggest that the technology can solve

history of how these men's work contributed to face surveillance's flaws, see Amanda Levendowski, *Face Surveillance Was Always Flawed*, PUB. BOOKS (Nov. 30, 2021), https://www.publicbooks.org/face-surveillance-was-always-flawed/ [https://perma.cc/7HWM-TTY4] [hereinafter Levendowski, *Face Surveillance Was Always Flawed*].

45. For deeper discussion, see *infra* Part III. *See also* Levendowski, *Face Surveillance Was Always Flawed*, *supra* note 44.

46. *See* Okidegbe, *supra* note 19, at 1–8.

47. *See, e.g.*, PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, NAT'L INST. OF STANDARDS & TECH., FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 2–3 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf [https://perma.cc/6S4R-WUWZ]; Buolamwini & Gebru, *supra* note 19, at 88. For an explanation of intersectionality, see Kimberlé Crenshaw, *Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics*, 1989 U. CHI. LEGAL F. 139. *See also* PATRICIA HILL COLLINS, BLACK FEMINIST THOUGHT: KNOWLEDGE, CONSCIOUSNESS, AND THE POLITICS OF EMPOWERMENT 225 (1990) ("Replacing additive models of oppression with interlocking ones creates possibilities for new paradigms. The significance of seeing race, class, and gender as interlocking systems of oppression is that such an approach fosters a paradigmatic shift of thinking inclusively about other oppressions, such as age, sexual orientation, religion, and ethnicity.").

48. *See generally* Damien Patrick Williams, *Fitting the Description: Historical and Sociotechnical Elements of Facial Recognition and Anti-Black Surveillance*, 7 J. RESPONSIBLE INNOVATION 74 (2020) (explaining how surveillance tools are "inextricably bound up with a history of racialized inequality").

49. Kashmir Hill, *Activists Turn Facial Recognition Tools Against the Police*, N.Y. TIMES, https://www.nytimes.com/2020/10/21/technology/facial-recognition-police.html [https://perma.cc/YFV7-8KFQ (dark archive)] (Aug. 1, 2021) [hereinafter Hill, *Activists Turn Facial Recognition*]; Joan Donovan & Chris Gilliard, *Facial Recognition Technology Isn't Good Just Because It's Used To Arrest Neo-Nazis*, SLATE (Jan. 12, 2021, 12:54 PM), https://slate.com/technology/2021/01/facial-recognition-technology-capitol-siege.html [https://perma.cc/J46C-JVXA].

50. *See infra* Section I.B.

crimes without necessarily promoting justice. These injustices inherent in face surveillance reveal why we should think creatively about countering its use.

A. *Demographic Biases*

A year before Williams' arrest in Detroit, Nijeer Parks spent ten days in a New Jersey jail after he was wrongly accused based on a flawed face recognition match.[51] When presented with the fake driver's license that generated the match, Parks said, "I don't think he looks like me. . . . The only thing we have in common is the beard."[52] That same year, back in Detroit, Michael Oliver was also wrongly arrested.[53] To date, all three of the publicly disclosed victims of mistaken law enforcement face recognition matches are Black men.[54]

The men wrongfully identified as criminals by face recognition algorithms are not the only examples of the automated facial analysis technology betraying people of color.[55] The landmark "Gender Shades" study conducted by Joy Buolamwini and Timnit Gebru shed light on the vastness of intersectional, automated face analysis biases.[56] Rather than use an existing dataset, the researchers developed the Pilot Parliaments Benchmark, a new dataset comprised of photographs of male and female politicians from six countries to measure the performance of Microsoft, Face++, and IBM face recognition algorithms.[57] The politicians were identified in four intersectional categories: darker-skinned males, lighter-skinned males, darker-skinned females, and

51. Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Face Recognition Match*, N.Y. TIMES, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html [https://perma.cc/2XCN-JC6K (dark archive)] (Jan. 6, 2021) [hereinafter Hill, *Another Arrest*]; Anthony G. Attrino, *He Spent 10 Days in Jail After Facial Recognition Software Led to the Arrest of the Wrong Man, Lawsuit Says*, NJ.COM, https://www.nj.com/middlesex/2020/12/he-spent-10-days-in-jail-after-facial-recognition-software-led-to-the-arrest-of-the-wrong-man-lawsuit-says.html [http://perma.cc/MK73-M66W (dark archive)] (Dec. 29, 2020, 1:40 PM). Parks is currently suing the mayor, director of the police department, several officers, and the acting prosecutor of Middlesex County, New Jersey. Complaint, Parks v. McCormack, No. 21-cv-04021 (D.N.J. filed Nov. 25, 2020, in N.J. Super. Ct. as No. L-003672-20).

52. Hill, *Another Arrest*, *supra* note 51.

53. Elisha Anderson, *Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn't Commit*, DETROIT FREE PRESS, https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/ [https://perma.cc/VC7Z-RHSV (dark archive)] (July 11, 2020, 11:03 PM). Oliver is also suing the City of Detroit over his wrongful arrest. Oliver v. Bussa, No. 20-011495-NO (Mich. Cir. Ct. Sept. 4, 2020).

54. Hill, *Another Arrest*, *supra* note 51.

55. *See supra* Introduction.

56. Buolamwini & Gebru, *supra* note 19. In 2012, the Federal Bureau of Investigation found that multiple face recognition algorithms struggled to identify Black faces, young faces, and women's faces. Brendan F. Klare, Mark J. Burge, Joshua C. Klontz, Richard W. Vorder Bruegge & Anil K. Jain, *Face Recognition Performance: Role of Demographic Information*, 7 IEEE TRANSACTIONS ON INFO. FORENSICS & SEC. 1789, 1800 (2012).

57. Buolamwini & Gebru, *supra* note 19, at 81, 85 tbl.4. Notably, these features were chosen because it ensured that the subjects were "public figures with known identities and photos available under non-restrictive licenses posted on government websites." *Id.* at 81.

lighter-skinned females.[58] Consistently, the algorithms performed worst on darker-skinned females, with error rates approaching nearly thirty-five percent higher than those for lighter-skinned males.[59] Inioluwa Deborah Raji and Buolamwini performed a reaudit of the first batch of companies and added new algorithms.[60] Their research found that the initially targeted companies all reduced accuracy disparities, but the newly studied companies persisted in performing poorly for darker-skinned females.[61]

The National Institute of Standards and Technology ("NIST") confirmed the Gender Shades findings in a follow-up study. NIST tested 189 algorithms from 99 developers, including commercial developers like Microsoft and law enforcement contractors like Vigilant Solutions.[62] As one of the researchers put it, "[I]t is usually incorrect to make statements across algorithms, [but] we found empirical evidence for the existence of demographic differentials in the majority of the face recognition algorithms we studied . . . ."[63] Those differentials were stark. For 1:N matching, which compares features from a search image with all other possibilities in the gallery and is used in most face recognition systems, false positives were elevated for West African, East African, and East Asian people, alongside—though at a slightly lower rate—South Asian and Central

58. *Id.* at 83 tbl.2. The researchers used a skin tone classification methodology developed by a dermatologist. *Id.* at 82.

59. Steve Lohr, *Facial Recognition Is Accurate, If You're a White Guy*, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html [https://perma.cc/5G9W-7CJW (dark archive)]. Microsoft and IBM responded by tweaking their algorithms. *See* John Roach, *Microsoft Improves Facial Recognition Technology To Perform Well Across All Skin Tones, Genders*, MICROSOFT: A.I. BLOG (June 26, 2018), https://blogs.microsoft.com/ai/gender-skin-tone-facial-recognition-improvement/ [https://perma.cc/A6A2-TQCS]; IBM, IBM RESPONSE TO "GENDER SHADES: INTERSECTIONAL ACCURACY DISPARITIES IN COMMERCIAL GENDER CLASSIFICATION" (2018), http://gendershades.org/docs/ibm.pdf [https://perma.cc/H7GU-RFHS].

60. Raji & Buolamwini, *supra* note 19.

61. *Id.* In *AI, Ain't I a Woman*, Buolamwini shows that commercial face recognition misgenders former First Lady Michelle Obama as a man. Joy Buolamwini, *AI, Ain't I a Woman*, YOUTUBE (June 28, 2018), https://www.youtube.com/watch?v=QxuyfWoVV98 [https://perma.cc/Z9KR-E3YF].

62. GROTHER ET AL., *supra* note 47, at 1, 26 tbl.5, 27 tbl.6. NIST was urged to conduct such a study by researchers at the Center for Privacy and Technology at Georgetown Law. *See* Garvie et al., *supra* note 19, at 6. The results echoed an earlier study, which found that face recognition systems demonstrated bias against women, Black people, and younger people. *See* Klare et al., *supra* note 56, at 1789.

63. *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, NAT'L INST. STANDARDS & TECH. (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software [https://perma.cc/48ME-F3WC]. Note that the NIST study used race rather than skin color. *Id.*

American people.[64] The lowest rate of false positives was for East European people.[65]

While the Gender Shades and NIST studies both revealed intersectional biases most affecting dark-skinned women, neither fully captured the extent of face analysis biases because both suffered from a shared shortcoming: use of binary gender. Gender Shades acknowledged expressly that "[t]his reductionist view of gender does not adequately capture the complexities of gender or address transgender identities," nor nonbinary ones.[66] Face recognition technology was not developed with trans and nonbinary faces in mind. In decades of research in the field, only a few leading scholarly papers acknowledge the existence of trans people and none mention nonbinary people.[67] Face recognition technology—including from major commercial developers such as IBM, Microsoft, and Amazon—misgenders trans people and simply cannot identify nonbinary people more than one-third of the time.[68]

When people cannot trust the accuracy of technology, these biases have practical effects. A Utah DMV employee forced a trans woman to remove her makeup out of concern that her appearance would create problems for face recognition.[69] Attempting to verify its drivers, Uber used Microsoft face recognition technology that failed to identify trans drivers and effectively

64. *Id.* The higher false positive rates for people of color were among algorithms developed in the United States, with American Indians (identified as a subset of Native faces) reflecting the highest rate of false positives. *Id.* A Federal Bureau of Investigation study likewise found that face recognition algorithms are least accurate for people of color, women, and young people. Klare et al., *supra* note 56, at 1800. Much face surveillance research, including the NIST study, also assumes and reifies the existence of "race" without interrogating its social construction. Alex Hanna, Emily Denton, Andrew Smart & Jamila Smith-Loud, *Towards a Critical Race Methodology in Algorithmic Fairness*, 2020 CONF. ON FAIRNESS ACCOUNTABILITY & TRANSPARENCY 501, 501.

65. GROTHER ET AL., *supra* note 47, at 2. It is worth noting that several developers' systems had virtually undetectable false-positive differentials, including Idemia and NEC-3, among several others. *Id.* at 8.

66. Buolamwini & Gebru, *supra* note 19, at 82; *see also* SARAH MYERS WEST, MEREDITH WHITTAKER & KATE CRAWFORD, AI NOW INST. DISCRIMINATING SYSTEMS: GENDER, RACE, AND POWER IN AI 17 (2019), https://ainowinstitute.org/discriminatingsystems.pdf [https://perma.cc/UJ8J-L3LJ] (explaining that the gender classification in the Gender Shades study presented several problems, one of which was the study's assumption that gender can be detected automatically).

67. *See, e.g.*, Ari Schlesinger, W. Keith Edwards & Rebecca E. Grinter, *Intersectional HCI: Engaging Identity Through Gender, Race, and Class*, PROC. 2017 CONF. ON HUM. FACTORS IN COMPUTING SYS. 5412; Os Keyes, *The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition*, 2 PROC. ACM ON HUM.-COMPUT. INTERACTION 88:1 (2018).

68. The study also looked at Clarifai. Morgan Klaus Scheuerman, Jacob M. Paul & Jed R. Brubaker, *How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis and Image Labeling Services*, 3 PROC. ACM HUM.-COMPUT. INTERACTION 144:1, 144:8 (2019).

69. Sonia K. Katyal & Jessica Y. Jung, *The Gender Panopticon: Artificial Intelligence, Gender, and Design Justice*, 68 UCLA L. REV. 692, 715 (2021). The concept of the "panopticon" is rooted in racist surveillance—Jeremy Bentham was inspired by the construction of a slave ship when conceptualizing it. *See* BROWNE, *supra* note 40, at 31–32.

locked them out of their accounts.[70] Other uses of gender-identifying face recognition technology include "real-time security, targeted marketing, and personalized human-robot interaction."[71] But even expanding face surveillance data labeling beyond binary gender may not be enough. Morgan Klaus Scheuerman's work examining issues of incorporating binary gender into face recognition technology curated a dataset of seven genders, including "genderless 'genders.'"[72] That work acknowledged that "there is boundless opportunity to include other genders in computer vision research" and recognized that these technologies still "require[] assumptions to be made about gender identity and pronouns" based on images alone.[73] And those assumptions are likely to be flawed.

Perversely, developers', researchers', and even auditors' attempts at correcting face recognition bias against trans and nonbinary people can perpetuate harm against the people they are trying to protect.[74] One researcher notoriously sought to develop a face recognition system using transition videos scraped from YouTube, a privacy invasion to which many scholars and subjects objected.[75] Anna Lauren Hoffman puts it plainly: inclusion can work to normalize oppression.[76] If the answer to correcting demographic bias in face surveillance requires strategic, expanded inclusion of people of color, women, trans, and nonbinary people in face recognition databases, then we must ask a different question.

B. *Deployment Biases*

Some people may believe that the use of face recognition by law enforcement would be acceptable if the technology were less demographically biased. But law enforcement would still deploy face recognition technology

70. John Riley, *Transgender Uber Drivers Say App's New Security Features Are Getting Them Suspended*, METROWEEKLY (Aug. 10, 2018), https://www.metroweekly.com/2018/08/transgender-uber-drivers-app-security-features-get-suspended/ [https://perma.cc/SG29-M6DG].

71. Scheuerman et al., *supra* note 68, at 144:6.

72. *Id.* at 144:26.

73. *Id.*

74. Inioluwa Deborah Raji, Timnit Gebru, Margaret Mitchell, Joy Buolamwini, Joonseok Lee & Emily Denton, *Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing*, 2020 AAAI/ACM A.I. ETHICS & SOC'Y CONF. 145, 147 (noting these attempts "can promote gender stereotypes, [be] . . . exclusionary of transgender, non-binary, and gender non-conforming individuals, and threaten[] further harm against already marginalized individuals" (internal citations omitted)). For a critical discussion of transgender politics and surveillance practices, see generally TOBY BEAUCHAMP, GOING STEALTH (2019).

75. *See* James Vincent, *Transgender YouTubers Had Their Videos Grabbed To Train Facial Recognition Software*, VERGE (Aug. 22, 2017, 10:44 AM), https://www.theverge.com/2017/8/22/16180080/transgender-youtubers-ai-facial-recognition-dataset [https://perma.cc/DAF7-HZCK].

76. *See* Anna Lauren Hoffman, *Terms of Inclusion: Data, Discourse, Violence*, 23 NEW MEDIA & SOC'Y 3539, 3539 (2021). *But see* Lemley & Casey, *supra* note 26, at 771 ("The solution is to build bigger databases overall or to 'oversample' members of smaller groups.").

against marginalized people with minimal oversight and limited means of recourse. Weaponizing surveillance technologies, such as face surveillance, against marginalized communities renders their movements hypervisible to law enforcement.[77] This has been the case for centuries. Simone Browne has detailed disparate surveillance dating to when states enforced so-called lantern laws that required Black and Native people to carry lit candles at night, illuminating themselves to the white gaze.[78] "Black luminosity," she says, worked as a "form of boundary maintenance occurring at the site of the black body, whether by candlelight, flaming torch, or the camera flashbulb that documents the ritualized terror of a lynch mob."[79] Little has changed. As the Fourth Circuit recently observed, "[T]echnology 'allow[s] government watchers to remain unobtrusive,' [but] the impact of surveillance '[is] conspicuous in the lives of those least empowered to object.'"[80] The court continued, "Because those communities are over-surveilled, they tend to be over-policed, resulting in inflated arrest rates and increased exposure to incidents of police violence."[81] People of color remain up to two-and-a-half times more likely to be targets of police surveillance.[82] And face recognition is deployed strategically against marginalized people, including people of color, immigrants, and sex workers, with minimal regulation, oversight, or accountability.[83] As poet and activist Malkia Devich-Cyril warned, "[F]acial-recognition . . . [will] be used to supercharge police abuses of power and worsen racial discrimination."[84]

77. *See, e.g.*, *Color of Surveillance*, GEO. L. CTR. ON PRIV. & TECH. (2019), https://www.law.georgetown.edu/privacy-technology-center/events/color-of-surveillance-2019/ [https://perma.cc/N5F7-5WKN] (documenting the past, present, and future of surveillance against marginalized communities, including Black people, immigrants, religious minorities, and poor people); Richardson et al., *supra* note 19, at 45.

78. *See* BROWNE, *supra* note 40, at 76–80.

79. *Id.* at 67; *see also* Brandi Thompson Summers, *Black Lives Under Surveillance*, PUB. BOOKS (Dec. 1, 2016), https://www.publicbooks.org/black-lives-under-surveillance/ [https://perma.cc/YYV8-2EKD] ("Today, poor communities of color are under constant surveillance and on the receiving end of brutal market forces.").

80. Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 347 (4th Cir. 2021) (en banc) (quoting BARTON GELLMAN & SAM ADLER-BELL, CENTURY FOUND., THE DISPARATE IMPACT OF SURVEILLANCE 2 (2017), https://production-tcf.imgix.net/app/uploads/2017/12/03151009/the-disparate-impact-of-surveillance.pdf [https://perma.cc/2869-QUAC]).

81. *Id.*

82. Clare Garvie & Jonathan Frankle, *Facial-Recognition Software Might Have Racial Bias Problem*, ATLANTIC (Apr. 7, 2016), https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/ [https://perma.cc/QW9G-DBL7 (dark archive)]. This overrepresentation plays out in mugshot databases used by face recognition technology. *Id.*

83. Williams, *supra* note 48, at 77–80.

84. Malkia Devich-Cyril, *Defund Facial Recognition*, ATLANTIC (July 5, 2020), https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/ [https://perma.cc/8L9U-UFA9 (dark archive)].

The New York Police Department ("NYPD") provides one example of law enforcement's history with face surveillance deployment biases.[85] After 9/11, the NYPD dusted downtown Manhattan with thousands of surveillance cameras and later consolidated video surveillance operations into a centralized command center.[86] In 2012, the NYPD began working with IBM to take surveillance footage from across the city and transform it into an effective face recognition system, integrating its system with more than five hundred cameras.[87] IBM developed new search features for the NYPD that allowed it to search by features like hair color, facial hair—and, most notably, skin tone.[88] Perhaps, then, it is no surprise that the NYPD also has a record of misusing face recognition technology against people of color.[89] Last summer, the NYPD admitted to using face recognition to surveil Black Lives Matter activist Derrick Ingram, despite public representations that the department "does not use facial recognition technology to monitor and identify people in crowds or political rallies."[90] Even if the technology were less demographically biased, history suggests that it would still be disproportionately focused on people of color.

The arrests of Williams and Oliver put these practices into stark relief beyond New York. Both Black men were arrested in Detroit, a city that is seventy-eight percent Black.[91] In the wake of their arrests, the Detroit Police Chief admitted that the department's face recognition technology misidentified suspects "about 96 percent of the time."[92] Yet despite known demographic biases, particularly for people of color, the department has not retired face recognition technology. Instead, Detroit doubled down and invested in a million-dollar system called Project Green Light that empowers police to scan

85. The public has little say in the acquisition and deployment of surveillance systems in most jurisdictions, as documented by Crump, *supra* note 9, at 1655, and Joh, *supra* note 21, at 20, 22, 37.

86. *See* James Vincent, *IBM Secretly Used New York's CCTV Cameras To Train Its Surveillance Software*, VERGE (Sept. 6, 2018, 10:24 AM), https://www.theverge.com/2018/9/6/17826446/ibm-video-surveillance-nypd-cctv-cameras-search-skin-tone [https://perma.cc/2NWM-3C9M].

87. *See id.*

88. Despite developing the skin tone feature and providing officers with the skin tone search tool, an NYPD spokesperson claimed the NYPD declined an offer to use the feature. *See id.*

89. *See* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEO. L. CTR. ON PRIV. & TECH. (May 16, 2019), https://www.flawedfacedata.com [https://perma.cc/74X3-FV3G] (detailing NYPD use of a photograph of actor Woody Harrelson, famed for his role in *Cheers* and more recently the dystopian series *The Hunger Games*, as a substitute for a suspect's image).

90. Sidney Fussell, *The Next Target for a Facial Recognition Ban? New York*, WIRED (Jan. 28, 2021, 8:00 AM), https://www.wired.com/story/next-target-facial-recognition-ban-new-york/ [http://perma.cc/R6EM-2SHA (dark archive)].

91. *Detroit City, Michigan; Michigan*, U.S. CENSUS BUREAU, https://www.census.gov/quickfacts/fact/table/detroitcitymichigan,MI/PST045219 [https://perma.cc/W7GM-62Y7].

92. Timothy B. Lee, *Detroit Police Chief Cops to 96-Percent Facial Recognition Error Rate*, ARS TECHNICA (June 30, 2020, 12:12 PM), https://arstechnica.com/tech-policy/2020/06/detroit-police-chief-admits-facial-recognition-is-wrong-96-of-the-time/ [https://perma.cc/NAG9-49GU].

live surveillance video from cameras across the city, from businesses and schools to hospitals and apartment buildings.[93]

Law enforcement also deploys face recognition technology to target immigrants. In 2019, Georgetown Law's Center on Privacy & Technology revealed through disclosed documents that the Federal Bureau of Investigation ("FBI") and Immigration and Customs Enforcement ("ICE") transformed state driver's license databases into routine immigration investigative tools.[94] More than a dozen states, including Utah, Vermont, and Washington, offer driver's licenses or driving privilege cards to undocumented immigrants.[95] According to records requests, ICE agents worked with state officials to run face recognition searches using those databases.[96] Searches were rarely accompanied by warrants or subpoenas, with some searches run using nothing more than an email attaching an investigative photograph, or "probe photo," of the target.[97] The revelation marked the first known instance of ICE deploying face recognition technology on state driver's license databases.[98] Alvaro Bedoya, the former director of Georgetown Law's Center on Privacy and Technology, explained that "this is a scandal, and a huge betrayal of undocumented people . . . . [ICE agents are] actually taking advantage of that [licensure] to secretly find and deport those people using face recognition technology . . . ."[99] In Maryland, another state that offers driver's licenses to undocumented immigrants, ICE ran face recognition searches on millions of photos without state or court approval.[100] Unlike prior cases, in which ICE requested state officials to run searches, ICE officials nationwide searched Maryland driver's license databases

93. Clare Garvie & Laura M. Moy, *America Under Watch: Face Surveillance in the United States*, GEO. L. CTR. ON PRIV. & TECH. (May 16, 2019), https://www.americaunderwatch.com/ [https://perma.cc/L3DY-5NRK]. Detroit's surveillance expansion has been resisted vehemently by local activists. *See* Tawana Petty, *Defending Black Lives Means Banning Facial Recognition*, WIRED (July 10, 2020, 8:00 AM), https://www.wired.com/story/defending-black-lives-means-banning-facial-recognition/ [https://perma.cc/9BFA-Z577 (dark archive)].

94. 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/77A7-8E4V (dark archive)].

95. *Id.*

96. *Id.*

97. *Id.*

98. *See* Catie Edmondson, *ICE Used Facial Recognition To Mine State Driver's License Databases*, N.Y. TIMES (July 7, 2019), https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html [https://perma.cc/R3B2-AADD (dark archive)].

99. Bill Chappell, *ICE Uses Facial Recognition To Sift State Driver's License Records, Researchers Say*, NPR (July 8, 2019, 4:23 PM), https://www.npr.org/2019/07/08/739491857/ice-uses-facial-recognition-to-sift-state-drivers-license-records-researchers-sa [https://perma.cc/588L-QHZD].

100. *See* Drew Harwell & Erin Cox, *ICE Has Run Facial-Recognition Searches on Millions of Maryland Drivers*, WASH. POST (Feb. 26, 2020), https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers/ [https://perma.cc/N734-BZGN (dark archive)].

independently without approval or oversight.[101] With state legislation on the horizon banning the practice,[102] ICE has opted to contract with a private subscription service for face recognition "mission support"—Clearview AI.[103]

Face recognition technology is also turned against sex workers, who have played an active role in resisting the technology and long occupied the frontiers of the internet through their communities and work.[104] The prominence of sex workers' online presence through advertisements, social media, and other content contributes to their vulnerabilities to surveillance. Their images are easily accessible which, as activist Danielle Blunt and her coauthors explain, means that "[s]ex workers are disproportionately . . . used as test subjects for facial recognition databases."[105] It is easy to run commercial face recognition technology on videos or photographs of sex workers,[106] and it is just as simple to scrape photos of sex workers and share them with law enforcement.[107]

101. *See id.*

102. Kevin Rector, *ICE Has Access to Maryland's Driver's License Records. State Lawmakers Want To Limit It.*, BALT. SUN (Feb. 26, 2020, 6:45 PM), https://www.baltimoresun.com/politics/bs-md-pol-ice-mva-bill-20200227-rsgqqajmwne4hollsz4svgpa6m-story.html [https://perma.cc/S5QM-7NMP (dark archive)].

103. Kim Lyons, *ICE Just Signed a Contract with Facial Recognition Company Clearview AI*, VERGE, https://www.theverge.com/2020/8/14/21368930/clearview-ai-ice-contract-privacy-immigration [https://perma.cc/E7TU-4P4V] (Aug. 14, 2020, 3:19 PM).

104. Private face recognition app FindFace was immediately turned against sex workers in Russia. Jason Abbruzzese, *Facial Recognition App Used To Shame Sex Workers in Russia*, MASHABLE (May 3, 2016), https://mashable.com/2016/05/03/facial-recognition-russia-shame-sex-workers/ [https://perma.cc/BF96-666L]. Sex workers successfully advocated for the New Orleans ban of face recognition technology. *See* Caroline Sinders, *How Musicians and Sex Workers Beat Facial Recognition in New Orleans*, VICE (Mar. 26, 2021, 9:00 AM), https://www.vice.com/en/article/xgznka/meet-the-musicians-and-strippers-who-beat-facial-recognition-in-new-orleans [https://perma.cc/LH2E-JEE8]; *see also Sexual Gentrification: An Internet Sex Workers Built*, HACKING//HUSTLING (Apr. 6, 2021), https://hackinghustling.org/sexual-gentrification-an-internet-sex-workers-built/ [https://perma.cc/Y84Y-TPNY] (situating sex workers at the forefront of the internet's innovations).

105. DANIELLE BLUNT, EMILY COOMBES, SHANELLE MULLIN & ARIEL WOLF, HACKING//HUSTLING, POSTING INTO THE VOID 7 (2020), https://hackinghustling.org/wp-content/uploads/2020/09/Posting-Into-the-Void.pdf [https://perma.cc/WJ45-F6KL].

106. *See, e.g.*, Abbruzzese, *supra* note 104 (explaining how running commercial face recognition technology played out in Russia); Bruce Schneier, *Technology To Out Sex Workers*, SCHNEIER ON SEC. (Oct. 13, 2017, 6:57 AM), https://www.schneier.com/blog/archives/2017/10/technology_to_o.html [https://perma.cc/75QA-NMBF] (describing a controversial PornHub feature that uses face recognition algorithms to identify performers); Samantha Cole, *DIY Facial Recognition for Porn Is a Dystopian Disaster*, VICE (May 29, 2019, 10:11 AM), https://www.vice.com/en/article/9kxny7/diy-facial-recognition-for-porn-weibo [https://perma.cc/DW29-TQTW] (reporting an unverified claim that a German user identified "more than 100,000 young ladies").

107. Sex Workers Outreach Project Chicago is among the plaintiffs in the ACLU lawsuit challenging Clearview AI. Complaint at 1, ACLU v. Clearview AI, Inc., No. 2020-CH-04353 (Ill. Cir. Ct. May 28, 2020). This may have happened to Amina du Jean, a sex worker who was approached by Metropolitan Police for a "welfare check." *See* Rivkah Brown, *How Facial Recognition Is Being Used To Target Sex Workers*, NEW STATESMAN, https://www.newstatesman.com/science-tech/privacy/2019/05/how-facial-recognition-being-used-target-sex-workers [https://perma.cc/7VUP-K3E5 (dark archive)] (Sept. 9, 2021, 3:10 PM).

Indeed, using sex workers as face recognition test subjects may be the byproduct of anti-sex-trafficking work by a nonprofit called Thorn.[108] Thorn provides limited details about the operation of its Spotlight tool, which law enforcement uses.[109] But Kate Zen, a community organizer and cofounder of grassroots sex-worker coalition Red Canary Song, describes the Spotlight tool as taking "escort ads from various different advertising sites" and providing Thorn's partners with copies of the advertisements.[110] Thorn uses Amazon Rekognition, the company's former face recognition tool, to identify individuals in the advertisements and work alongside law enforcement to track down hits.[111] But Thorn's approach to collecting advertisements may bundle ads trafficking children with ads for consensual, adult sex work.[112] As a result, sex workers may be subject to criminal investigation or harassment by law enforcement.[113]

Even perfect accuracy and procedure cannot salvage the technology.[114] The intractable power biases that animate face surveillance enables invasive privacy

108. *See Spotlight*, THORN, https://www.thorn.org/spotlight/ [https://perma.cc/XZN2-NJED].

109. *See id.* The trademark application for the SPOTLIGHT mark describes the tool as "providing temporary use of non-downloadable software for use in human trafficking investigations; providing temporary use of non-downloadable software for use in analyzing pattern data in online activity to detect criminal activity." SPOTLIGHT, Registration No. 4783591.

110. Erin Taylor, *Sex Workers Are at the Forefront of the Fight Against Mass Surveillance and Big Tech*, OBSERVER (Nov. 12, 2019, 10:43 AM), https://observer.com/2019/11/sex-workers-mass-surveillance-big-tech/ [https://perma.cc/H6DB-5RMS]. A former Thorn partner was the controversial surveillance company and law enforcement contractor Palantir. *Id.*

111. Amazon, *Thorn Uses AWS To Help Law Enforcement Identify Child-Trafficking Victims Faster*, AWS, https://aws.amazon.com/solutions/case-studies/thorn/ [https://perma.cc/9G26-WHG2].

112. *Id.* ("One way for law enforcement agents to catch traffickers and rescue kids would be to identify and investigate escort ads that *seem* to feature minors . . . ." (emphasis added)). Thorn has avoided discussing whether such bundling occurs, but the organization has not denied it. Taylor, *supra* note 110.

113. Police and other government officials have a history of abusing access to databases for misogynistic purposes. *See, e.g.*, United States v. Rodriguez, 628 F.3d 1258, 1261–62 (11th Cir. 2010) (dealing with a Social Security Administration employee who used a department database to access ex-girlfriend's personal information sixty-two times, a female ex-coworker's child's personal information twenty-two times, a female restaurant worker's personal information twenty times, a female church study group colleague's personal information sixty-five times, another female church study group colleague's personal information forty-five times, as well as multiple other women from the church study group's personal information totaling over eighty times, to variously stalk and alarm the targeted women); United States v. Valle, 807 F.3d 508, 512 (2d Cir. 2015) (ruling on a police officer using department database to investigate women he fantasized about cannibalizing); Van Buren v. United States, 141 S. Ct. 1648 (2021) (handling a police sergeant taking $5,000 cash to use a state database to investigate whether woman was undercover officer).

114. As Ben Green and Salomé Viljoen explain, computer scientists should ask other questions about the social impacts of their code, including:

> Who are the relevant social actors? What are their interests and relative amounts of power? Which people need to approve this algorithm? What are their goals? On whose use of the algorithmic system does success depend? What are their interests and capabilities? How might this algorithmic affect existing scientific, social, and political discourses or introduce new discourses?

intrusions by law enforcement. These inherent intrusions ensure the technology can never be just.

II. WHAT COULD PREVENT FACE SURVEILLANCE?

The demographic and deployment biases of face recognition technology are no secret. That is why legislators introduced the first piece of federal legislation regulating face recognition in February 2020.[115] The proposed law acknowledged the technology's demographic biases, stating that "[f]acial recognition has a history of being inaccurate, particularly for women, young people, African Americans, and other ethnic groups."[116] The proposed law also recognized the technology's deployment biases, stating that "[f]acial recognition has been shown to disproportionately impact communities of color, activists, immigrants, and other groups that are already unjustly targeted."[117] Given the baked-in biases of face surveillance, the bill imposed a temporary moratorium on its use by federal law enforcement.[118] However, congressional representatives failed to enact it as law. They likewise failed to pass bills introduced afterward, though a new version remains before Congress.[119]

Absent enactment of a federal law, other attempts at face surveillance accountability emerged. In response to the murder of George Floyd and calls to defund the police, IBM, Amazon, and Microsoft announced corporate moratoria pledging not to sell face recognition technology to law enforcement.[120] And across the country, states and cities enacted legislative face recognition bans, moratoria, and regulations of their own.[121] This part examines both paths and unpacks why the prosecutorial, practical, and political shifts necessary to realize them fall short as means of resisting face surveillance.

A. *Encouraging Corporate Moratoria*

The summer of 2020 saw renewed protests calling to protect Black lives, defund the police, and divest corporate development of surveillance tools for

Ben Green & Salomé Viljoen, *Algorithmic Realism: Expanding the Boundaries of Algorithmic Thought*, 2020 CONF. ON FAIRNESS ACCOUNTABILITY & TRANSPARENCY 19, 27 (proposing a new model of "algorithmic realism" "to account for realities of social life and algorithmic impacts").

115. Khari Johnson, *U.S. Senators Propose Facial Recognition Moratorium for Federal Government*, VENTURE BEAT (Feb. 12, 2020, 3:24 PM), https://venturebeat.com/2020/02/12/u-s-senators-propose-facial-recognition-moratorium-for-federal-government/ [https://perma.cc/FV5M-J29L].

116. Ethical Use of Facial Recognition Act, S. 3284, 116th Cong. § 2(3) (2020).

117. *Id.* § 2(2).

118. *See id.* § 4.

119. *See* Facial Recognition and Biometric Technology Moratorium Act of 2020, S. 4084, 116th Cong. (2020); Facial Recognition and Biometric Technology Moratorium Act of 2021, S. 2052, 117th Cong. (2021).

120. *See infra* Section II.A.

121. *See infra* Section II.B.

law enforcement.[122] Within weeks of George Floyd's murder, the biggest names in commercial face recognition—IBM,[123] Amazon,[124] and Microsoft[125]—declared they would not sell their face surveillance technology to law enforcement. For all three, the announcement was unexpected, given the opportunities for profit created by selling the technology to police.

After scraping a million photographs to fuel its own face recognition algorithms,[126] IBM was the first mover, sunsetting its general-purpose face recognition technology entirely and proclaiming:

> IBM firmly opposes and will not condone uses of any technology, including facial recognition technology offered by other vendors, for mass surveillance, racial profiling, violations of basic human rights and freedoms . . . . [N]ow is the time to begin a national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies.[127]

In the only statement among IBM, Microsoft, and Amazon that does not mention support for human rights, Amazon announced that it would be "implementing a one-year moratorium on police use of Amazon's facial

122. *See, e.g.*, Amna A. Akbar, *An Abolitionist Horizon for (Police) Reform*, 108 CALIF. L. REV. 1781 (2020) (arguing that a structural critique on policing requires an abolitionist perspective); Matthew Clair & Amanda Woog, *Courts and the Abolition Movement*, 110 CALIF. L. REV. (forthcoming 2022) (arguing that criminal trial courts function as an unjust social institution and should be replaced with other institutions that do not inherently legitimate police, rely on jails and prisons, or themselves operate as tools of racial and economic oppression); Anthony O'Rourke, Rick Su & Guvora Binder, *Disbanding Police Agencies*, 121 COLUM. L. REV. 1327 (2021) (assessing the disbanding of police forces as a reform strategy from a democratic and institutionalist perspective).

123. *See* Arvind Krishna, *IBM CEO's Letter to Congress on Racial Justice Reform*, IBM: THINKPOLICY BLOG (June 8, 2020), https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/ [https://perma.cc/QG97-2D7C].

124. *See* Amazon Staff, *We Are Implementing a One-Year Moratorium on Police Use of Rekognition*, AMAZON (June 10, 2020), https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition [https://perma.cc/6S3A-4YCV].

125. *See* Jay Greene, *Microsoft Won't Sell Police Its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM*, WASH. POST (June 11, 2020), https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/ [https://perma.cc/KV4T-TSFR (dark archive)]. Months earlier, Microsoft President Brad Smith said the company did not want a moratorium, claiming that "the only way to continue developing [face recognition] actually is to have more people using it." Bill Radke & Alison Bruzek, *Microsoft President Brad Smith on Consumer Privacy*, NPR (Jan. 16, 2020, 2:23 PM), https://www.kuow.org/stories/microsoft-president-brad-smith-on-consumer-privacy [https://perma.cc/XP9G-HGDA].

126. Ironically, IBM used the nonconsensually collected images for a dataset targeted to debiasing face recognition algorithms. *See* John R. Smith, *IBM Research Releases 'Diversity in Faces' Dataset To Advance Study of Fairness in Facial Recognition Systems*, IBM (Jan. 29, 2019), https://web.archive.org/web/20190201133121/https://www.ibm.com/blogs/research/2019/01/diversity-in-faces/ [http://perma.cc/8KB4-VSSD (staff-uploaded archive)].

127. Krishna, *supra* note 123. Perhaps the company learned its lesson from collaborating with Nazis during World War II. *See* EDWIN BLACK, IBM AND THE HOLOCAUST 7–17 (2001). *But see* Vincent, *supra* note 86 (developing an IBM tool to search surveillance footage by skin tone).

recognition technology" in hopes that one year "might give Congress enough time to implement appropriate rules."[128] Microsoft reiterated its decision not to sell face recognition technology to law enforcement[129] "until we have a national law in place, grounded in human rights, that will govern this technology."[130]

A trio of corporate moratoria is a triumph for researchers and advocates who sounded the alarm about the dangers of supplying law enforcement with face recognition technology. But that victory is compromised by loopholes. Corporate moratoria are voluntary and, in some cases, temporary.[131] There is no means of public recourse if one of these companies decides that the just choice fails to maximize shareholder value or advance leadership agendas.[132] Nothing in the moratoria prevents the selling of face recognition technology to entities that collaborate with law enforcement.[133] It is unclear from the moratoria whether these companies are also refusing to work with government agencies like ICE or the U.S. Department of Defense.[134] But crucially, law enforcement was never these companies' biggest customer—and these companies were never police departments' biggest suppliers. IBM, Amazon, and Microsoft sell consumer-facing products and have an interest in maintaining their public reputations, a concern not shared by many other vendors in the space whose customer base is law enforcement. DataWorks Plus, the company behind the flawed face recognition algorithm that misidentified Williams, did not announce a moratorium. Neither did many of the larger companies, like NEC, nor the smaller, largely unknown companies—like LACRIS, Rank One, Cognitec, and Ayonix Corporation—that supply law enforcement with face recognition technology.[135] When major corporations withdrew from the face

128. Amazon Staff, *supra* note 124.

129. However, the company contracted to sell other surveillance services to law enforcement. *See* Michael Kwet, *The Microsoft Police State: Surveillance, Facial Recognition, and the Azure Cloud*, INTERCEPT (July 14, 2020, 3:42 PM), https://theintercept.com/2020/07/14/microsoft-police-state-mass-surveillance-facial-recognition/ [https://perma.cc/Q7DT-KVCR].

130. Greene, *supra* note 125.

131. However, Amazon recently announced an extension of its initial moratorium—indefinitely. Karen Weise, *Amazon Indefinitely Extends a Moratorium on the Police Use of Its Facial Recognition Software*, N.Y. TIMES, https://www.nytimes.com/2021/05/18/business/amazon-police-facial-recognition.html [https://perma.cc/ATQ4-JCEJ (dark archive)] (Aug. 1, 2021).

132. Indeed, Amazon previously defeated shareholder efforts to prevent selling face recognition technology to government customers. Zach Whittaker, *Amazon Defeated Shareholder's Vote on Facial Recognition by a Wide Margin*, TECHCRUNCH (May 28, 2019, 9:27 AM), https://techcrunch.com/2019/05/28/amazon-facial-recognition-vote/ [https://perma.cc/E24W-VCFG].

133. Amazon expressly mentioned continuing to allow Thorn, which works closely with law enforcement, to use Amazon Rekognition. *See* Amazon Staff, *supra* note 124.

134. Amazon previously pitched its Amazon Rekognition face recognition technology to ICE. Russell Brandom, *Amazon Pitched Its Facial Recognition System to ICE*, VERGE (Oct. 23, 2018, 10:35 AM), https://www.theverge.com/2018/10/23/18013376/amazon-ice-facial-recognition-aws-rekognition [https://perma.cc/9E84-X8LU].

135. Council, *supra* note 7; Kevin Rector & Richard Winton, *Despite Past Denials, LAPD Has Used Facial Recognition Software 30,000 Times in the Last Decade, Records Show*, L.A. TIMES (Sept. 21,

recognition supply chain, they left the least accountable companies in control of developing face surveillance for law enforcement.

Corporate moratoria on face surveillance still bear a final flaw. Despite acknowledging the harms of pervasive and persistent surveillance, none of these companies committed to cease doing business with police departments. To the contrary, the limited scope of these moratoria mean that IBM, Amazon, and Microsoft can continue supplying other surveillance technologies, such as predictive policing tools,[136] smart doorbells,[137] and cloud computing capabilities[138] to police departments across the country.[139] As a practical matter, these companies helped normalize face surveillance and continue working in partnership with police departments—they cannot be trusted to dismantle a system they helped develop.

B. *Enacting Local Legislative Oversight*

World-renowned corporations are not the only ones creating face surveillance technology—and relying on moratoria is not the only means of recourse. Months after the revelation that Clearview AI amassed a database of scraped photographs to fuel its face surveillance technology, the American Civil Liberties Union ("ACLU") jumped into action, suing the company under an increasingly invoked Illinois law called the Biometric Information Privacy Act

2020, 12:43 PM), https://www.latimes.com/california/story/2020-09-21/lapd-controversial-facial-recognition-software [https://perma.cc/PG5N-NEDQ (staff-uploaded, dark archive)]; *see also* Julia Horowitz, *Tech Companies Are Still Helping Police Scan Your Face*, CNN BUS., https://www.cnn.com/2020/07/03/tech/facial-recognition-police/index.html [https://perma.cc/S8DK-DTGF] (July 3, 2020, 8:36 AM).

136. IBM sold "near-instant intelligence" applications to police departments, which was not discussed in the moratorium. Kate Kaye, *IBM, Microsoft, and Amazon's Face Recognition Bans Don't Go Far Enough*, FAST CO. (June 13, 2020), https://www.fastcompany.com/90516450/ibm-microsoft-and-amazons-face-recognition-bans-dont-go-far-enough [https://perma.cc/4487-HLUD (staff-uploaded, dark archive)].

137. Amazon continues selling Amazon Ring technology in cooperation with hundreds of police forces. *See* Sidney Fussell, *How Surveillance Has Always Reinforced Racism*, WIRED (June 19, 2020, 7:00 AM), https://www.wired.com/story/how-surveillance-reinforced-racism/ [https://perma.cc/JKZ6-9CFX (dark archive)]; Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/ [https://perma.cc/E7XC-89XS (dark archive)]. Amazon Ring doorbells appropriate technology developed by Black inventor Marie Van Brittan Brown, who patented the technology for the first home security system. *See* Claudia Garcia-Rojas, *The Surveillance of Blackness: From the Trans-Atlantic Slave Trade to Contemporary Surveillance Technologies*, TRUTHOUT (Mar. 3, 2016), https://truthout.org/articles/the-surveillance-of-blackness-from-the-slave-trade-to-the-police/ [https://perma.cc/T8U4-74BJ].

138. *See* Kwet, *supra* note 129. Drones and robotic devices are also on the menu. *Id.*

139. This hypocrisy has not gone unnoticed by employees. *See, e.g.*, Dave Gershgorn, *250 Microsoft Employees Call on CEO To Cancel Police Contracts and Support Defunding Seattle PD*, ONEZERO (June 9, 2020), https://onezero.medium.com/250-microsoft-employees-call-on-ceo-to-cancel-police-contracts-and-support-defunding-seattle-pd-e89fa5d9e843 [https://perma.cc/AP2W-LVZV (dark archive)].

("BIPA").[140] BIPA makes it illegal for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's . . . biometric identifier or biometric information, unless it first" informs the subject and "receives a written release executed by the subject of the biometric identifier or biometric information."[141] As the ACLU alleged in its complaint, Clearview AI did neither—the company failed to inform millions of people before scraping their photographs, and it certainly did not receive written consent.[142] The law proved powerful in the past, forcing Facebook into a $650 million settlement over its own flawed face recognition ambitions.[143] Indeed, Woodrow Hartzog suggests that BIPA is potentially the most important biometric privacy law in the United States.[144] But there is a significant problem with BIPA as a means of tackling face surveillance: it only protects residents of Illinois.[145]

140. Complaint at 3, ACLU v. Clearview AI, Inc., No. 2020-CH-04353 (Ill. Cir. Ct. May 28, 2020).

141. Biometric Information Privacy Act, 2008 Ill. Laws 3693, 3695 (codified at 740 ILL. COMP. STAT. ANN. 14/15(b)(3) (2022)). In 2008, the Illinois legislature enacted the law after Pay By Touch, a biometrics company that provided retailers across Illinois with fingerprint scanners, filed for bankruptcy and opened up the possibility that biometric information could be sold or shared through bankruptcy proceedings. *See* Charles N. Insler, *Understanding the Biometric Privacy Act Litigation Explosion*, 106 ILL. BAR J. 34, 35 (2018); *see also* 2008 Ill. Laws at 3693 ("The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.").

142. *See* Complaint, *supra* note 140, at 3. Ryan Mac, a journalist for Buzzfeed News, broke the story on Twitter. *See* Ryan Mac (@RMac18), TWITTER (Feb. 13, 2020, 6:22 PM), https://twitter.com/RMac18/status/1228097214578225153 [https://perma.cc/G5CX-HM6M]. Clearview AI faces at least nine other lawsuits. *See* Adam Schwartz & Andrew Crocker, *Clearview's Faceprinting Is Not Sheltered from Biometric Privacy Litigation by the First Amendment*, ELEC. FRONTIER FOUND. (Nov. 5, 2020), https://www.eff.org/deeplinks/2020/11/clearviews-faceprinting-not-sheltered-biometric-privacy-litigation-first-amendment [https://perma.cc/4CEZ-PBXB]. The company claims its business practices are protected by the First Amendment. *But see* Brief for Electronic Frontier Foundation as Amici Curiae in Opposition to Defendant's Motion to Dismiss at 6–7, ACLU v. Clearview AI, Inc., No. 2020-CH-04353 (Ill. Cir. Ct. Nov. 5, 2020) (arguing that the First Amendment does not allow Clearview AI to ignore BIPA and urging the court to apply intermediate scrutiny on any First Amendment issues).

143. Order Granting Preliminary Approval of Class Action Settlement at 1–2, *In re* Facebook Biometric Info. Priv. Litig., No. 15-cv-03747-JD (N.D. Cal. Aug. 19, 2020). The law has been invoked against face recognition technology elsewhere. *See, e.g.*, Rivera v. Google, Inc., 238 F. Supp. 3d 1088, 1102 (N.D. Ill. 2017) (holding that Google violated BIPA for using photographs to create face scans); Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1204 (Ill. 2019) (holding that Six Flags violated BIPA for using fingerprint scanners to obtain season passes).

144. *See* Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, *in* REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS 96, 96 (Amba Kak ed., 2020), https://ainowinstitute.org/regulatingbiometrics.pdf [https://perma.cc/DRD4-HFT2].

145. *See* Dave Gershgorn, *A Simple Way To Measure Whether Your Privacy Law Is Worth a Damn*, ONEZERO (Mar. 12, 2021), https://onezero.medium.com/a-simple-way-to-measure-whether-your-privacy-law-is-worth-a-damn-2d591f0ac13 [https://perma.cc/7M7W-69C5 (staff-uploaded, dark archive)].

Illinois is not alone in its regulation of face recognition technology.[146] Absent federal legislation, some states, like Oregon, New Hampshire, and California, prohibit use of face recognition in body-worn cameras.[147] Others, like Washington and Massachusetts, regulate its use by law enforcement.[148] New York paused the use of face recognition technology in schools through recent legislation.[149] And in 2020, Vermont became the first state, now joined by Maine and Virginia, to ban the use of face recognition technology by law enforcement.[150] In total, only ten states have taken action against face surveillance.[151] On the other hand, far more than ten cities have pursued legislation, sometimes in direct response to police misuse.

Take San Francisco, for example. The city's police department said that it did not currently use face recognition but admitted to testing the technology on mugshots from 2013 to 2017.[152] To prevent the revival of those tests, the San Francisco Board of Supervisors overwhelmingly voted to ban law enforcement

146. Texas and Washington also have biometric privacy laws, which are less litigated—unlike Illinois's BIPA, neither includes a private cause of action. *See* TEX. BUS. & COM. CODE ANN. § 503.001 (Westlaw through the end of the 2021 Reg. and Called Sesss. of the 87th Leg.); *see also* WASH. REV. CODE ANN. § 19.375.020 (Westlaw with effective legislation through chapter 185 of the 2022 Reg. Sess. of the Wash. Leg.).

147. *See* OR. REV. STAT. ANN. § 133.741 (Westlaw through Ch. 1 enacted in the 2022 Reg. Sess. of the 81st Legis. Assemb.); CAL. PENAL CODE § 832.19 (Westlaw with urgency legislation through Ch. 14. of 2022 Reg. Sess.); N.H. REV. STAT. ANN. § 105-D:2 (Westlaw through Ch. 29 of the 2022 Reg. Sess.); *see also* Fahmida Y. Rashid, *Washington Is First State To Regulate Facial Recognition*, DUO: DECIPHER (Apr. 1, 2020), https://duo.com/decipher/washington-is-first-state-to-regulate-facial-recognition [https://perma.cc/SM7Z-EZ8C].

148. *See* WASH. REV. CODE ANN. § 43.386.080 (Westlaw with effective legislation through Ch. 185 of the 2022 Reg. Sess. of the Wash. Leg.); MASS. GEN. LAWS ANN. ch. 6, § 220 (Westlaw through Ch. 41 of the 2022 2d Ann. Sess.); Kashmir Hill, *How One State Managed To Actually Write Rules on Facial Recognition*, N.Y. TIMES, https://www.nytimes.com/2021/02/27/technology/ Massachusetts-facial-recognition-rules.html [https://perma.cc/JH5A-SMPU (dark archive)] (Mar. 5, 2021) [hereinafter Hill, *How One State Managed*].

149. Act of Dec. 22, 2020, 2020 N.Y. Laws 1142 (codified as amended at N.Y. STATE TECH. LAW § 106-b (2022)).

150. Act of Oct. 7, 2020, 2020 Vt. Acts & Resolves 951, 957 (codified as amended at VT. STAT. ANN. tit. 20, § 2369 note (2022)); Act of July 1, 2021, ch. 394, 2021 Me. Legis. Serv. (West) (codified at ME. REV. STAT. ANN. tit. 25, § 6001 (2022)); Act of Apr. 7, 2021, ch. 537, 2021 Va. Adv. Legis. Serv. (LexisNexis); *see also ACLU of Vermont Statement on the Enactment of S. 124, the Nation's Strongest Statewide Ban on Law Enforcement Use of Facial Recognition Technology*, ACLU VT. (Oct. 8, 2020, 2:15 PM), http://www.acluvt.org/en/news/aclu-vermont-statement-enactment-s124-nations-strongest-statewide-ban-law-enforcement-use [https://perma.cc/7R8P-GY2M]; Igor Bonifacic, *Maine Bans Facial Recognition Technology from Schools and Most Police Work*, YAHOO! FIN. (June 30, 2021), https://finance.yahoo.com/news/maine-facial-recognition-law-19125274.html [http://perma.cc/5HP5-SB2B] .

151. Illinois, Oregon, New Hampshire, California, Washington, Massachusetts, New York, Vermont, Maine, and Virginia. *See supra* text accompanying notes 146–50. As shown through this list, not a single state in the Southwest has banned face surveillance. *See supra* text accompanying notes 146–50.

152. Gregory Barber, *San Francisco Bans Agency Use of Facial-Recognition Tech*, WIRED (May 14, 2019, 6:17 AM), https://www.wired.com/story/san-francisco-bans-use-facial-recognition-tech/ [http://perma.cc/2PNP-HVM2 (dark archive)].

and other agencies from using face recognition technology.[153] The following month, Somerville, Massachusetts, became the first East Coast city to ban government use of face recognition technology.[154] Kade Crockford, director of the Technology for Liberty Project at the ACLU of Massachusetts, commented that Somerville was "joining a nationwide movement to bring the technology under democratic control."[155] In some ways, they are right: more than a dozen cities enacted bans, moratoria, or regulations of face recognition technology in the last several years.[156] Many more have adopted community control over police surveillance ("CCOPS") regulations—which, in part, create oversight mechanisms prior to law enforcement acquisition of invasive surveillance technologies—that may have the effect of regulating face surveillance.[157] But these statutes do not always accomplish what the public expects.

Several cities' statutory language suffers from the same shortcomings as corporate moratoria: loopholes. Some laws—such as those in Pittsburgh, Boston, Alameda, Madison, Northampton, and East Hampton—permit police to continue relying on face recognition technology indirectly through state and federal agencies, private companies, and even other police departments.[158] Other laws do not preclude government agencies, such as airport and seaport agents, from using face recognition technology.[159] Law enforcement simply flouts some laws. Despite explicit bans, the San Francisco Police Department used a match from another government agency to investigate a gun-related

153. Kate Conger, Richard Fausset & Serge F. Kovaleski, *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html [https://perma.cc/32TQ-VVF6 (dark archive)].

154. Katie Lannan, *Somerville Bans Government Use of Facial Recognition Tech*, WBUR (June 28, 2019), https://www.wbur.org/bostonomix/2019/06/28/somerville-bans-government-use-of-facial-recognition-tech [https://perma.cc/W3PY-KV3P].

155. Crockford is a lawyer for the ACLU of Massachusetts who advocated for city bans. *Somerville Becomes First East Coast City To Ban Government Use of Face Recognition Technology*, ACLU (June 28, 2019), https://www.aclu.org/press-releases/somerville-becomes-first-east-coast-city-ban-government-use-face-recognition [https://perma.cc/66L9-S6UM].

156. Those cities include Alameda, Baltimore, Berkeley, Boston, Brookline, Cambridge, Jackson, Madison, New York, Minneapolis, New Orleans, Northampton, Oakland, Pittsburgh, both Portlands (Maine and Oregon), Seattle (via King County), and Springfield, with others being added regularly. *See Ban Facial Recognition: Interactive Map*, FIGHT FOR FUTURE, https://www.banfacialrecognition.com/map/ [https://perma.cc/GQ6X-PQSF].

157. *Community Control over Police Surveillance*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance [https://perma.cc/LBY6-6TQ3].

158. Alfred Ng, *Police Say They Can Use Facial Recognition Despite Bans*, MARKUP (Jan. 28, 2021, 8:00 AM), https://themarkup.org/news/2021/01/28/police-say-they-can-use-facial-recognition-despite-bans [https://perma.cc/Q4FY-J23Y].

159. *See* Barber, *supra* note 152.

crime last year,[160] and the Pittsburgh Police Department continued using Clearview AI during Black Lives Matter protests.[161]

Further, stricter face recognition regulations remain unevenly distributed. Most jurisdictions, including the entire Southwest region, have no laws regulating the use of face surveillance technology by law enforcement. Detroit, where law enforcement misidentified Williams and Oliver, responded to pressure from activist Tawana Petty and other advocates by enacting guidelines limiting police use of face recognition technology to investigate violent crimes and home invasions.[162] Despite the poor performance of Datawork Plus's face recognition technology, the city recently voted to extend its contract with the company.[163] Two cities, Miami and Washington, D.C., admitted to surveilling Black Lives Matter protesters with face recognition technology, and neither city responded by enacting laws governing the use of the technology.[164] States and cities must continue legislating the oversight of face surveillance, but relying on localities leaves the technology to thrive where there is less political investment in protecting people's privacy—perhaps even where police desire less of it. When we are all subject to face surveillance, we all need protection.

160. Megan Cassidy, *Facial Recognition Tech Used To Build SFPD Gun Case, Despite Ban*, S.F. CHRON., https://www.sfchronicle.com/bayarea/article/Facial-recognition-tech-used-to-build-SFPD-gun-15595796.php [https://perma.cc/AXR6-W9SU (dark archive)] (Sept. 24, 2020, 9:35 PM).

161. Juliette Rihl, *Emails Show Pittsburgh Police Officers Accessed Clearview Facial Recognition After BLM Protests*, PUBLICSOURCE (May 20, 2021), https://www.publicsource.org/pittsburgh-police-facial-recognition-blm-protests-clearview/ [https://perma.cc/E9H9-MW56].

162. *See* DETROIT POLICE DEP'T, MANUAL DIRECTIVE 307.5 (Sept. 12, 2019), https://detroitmi.gov/sites/detroitmi.localhost/files/2019-09/Revised%20facial%20recognition%20directive%20transmitted%20to%20Board%209-12-2019.pdf [https://perma.cc/2693-FXB4]; *Thank You, Tawana!*, DETROIT CMTY. TECH. PROJECT, https://detroitcommunitytech.org/?q=content/thank-you-tawana [https://perma.cc/SQY9-S7LG]. Williams and Oliver were wrongfully accused of larceny, which falls into neither category. Hill, *Wrongfully Accused*, *supra* note 1 (discussing Williams' charges); Anderson, *supra* note 53 (discussing Oliver's charges); *see also* Susan Crawford, *Facial Recognition Laws Are (Literally) All Over the Map*, WIRED (Dec. 16, 2019, 8:00 AM), https://www.wired.com/story/facial-recognition-laws-are-literally-all-over-the-map/ [https://perma.cc/9YR4-DV5Y (dark archive)] (discussing limited adoption of local laws prohibiting face recognition by law enforcement).

163. Miriam Marini, *Detroit City Council Votes To Extend Facial Recognition Contract, Despite Controversy*, DETROIT FREE PRESS (Sept. 29, 2020, 5:18 PM), https://www.freep.com/story/news/local/michigan/detroit/2020/09/29/facial-recognition-software-contract-extended/3578348001/ [https://perma.cc/Q3XW-K4W2 (dark archive)].

164. Tate Ryan-Mosley, *Why 2020 Was a Pivotal, Contradictory Year for Facial Recognition*, MIT TECH. REV. (Dec. 29, 2020), https://www.technologyreview.com/2020/12/29/1015563/why-2020-was-a-pivotal-contradictory-year-for-facial-recognition/ [https://perma.cc/5W84-HA7N (dark archive)]. However, Washington, D.C., recently stopped using the face recognition technology under pressure from advocates. Justin Jouvenal, *Facial Recognition System Used To Identify Lafayette Square Protester To Be Halted*, WASH. POST (May 18, 2021, 4:28 PM), https://www.washingtonpost.com/local/public-safety/facial-recognition-system-halted/2021/05/18/af2d19e2-b737-11eb-a6b1-81296da0339b_story.html [https://perma.cc/CNF9-888K (dark archive)].

III. INVOKING COPYRIGHT AND ENVISIONING AN (UN)FAIR USE ANALYSIS

Protection from face surveillance may come in an unusual form: copyright law. Thanks to Oscar Wilde, copyright law protects photographs. In 1882, a photographer named Napoleon Sarony created an image of the dapper author leaning his head on his hand, apparently deep in thought.[165] The Burrow-Giles Lithographic Company began making and selling copied lithographs of the photograph; Sarony sued. The Supreme Court found itself weighing whether photographs were merely mechanical reproductions or works of authorship, such as "writing, printing, engraving, etching, [etc.]," protected by copyright law.[166] The Supreme Court affirmed the lower court's conclusion that:

> [Sarony] pos[ed] the said Oscar Wilde in front of the camera, selecting and arranging the costume, draperies, and other various accessories in said photograph, arranging the subject so as to present graceful outlines, arranging and disposing the light and shade, suggesting and evoking the desired expression, and from such disposition, arrangement, or representation, made entirely by plaintiff, he produced the picture in suit.[167]

In unanimously concurring with the lower court, the Supreme Court determined that the photograph was "an original work of art" with an "author" and of "a class of inventions for which the Constitution intended that Congress should secure" copyright.[168] One cannot own a copyright in one's physical features, such as a nose or mouth—the "facts" of one's face—but copyright law continues to protect rights in photographs that depict those physical features, including the exclusive rights to create or reproduce copies of those photos.[169]

While facts are not protected by copyright, face surveillance generally peddles protectable photographs.[170] Different face surveillance companies take different approaches to developing their datasets and algorithms. Some use third-party datasets. Others use secretive, proprietary datasets of their own.

165. Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53, 54–55 (1884).

166. *Id.* at 58.

167. *Id.* at 60.

168. *Id.*

169. 17 U.S.C. § 106.

170. Some scholars have speculated that Clearview AI only scraped "factual information" from social media photographs, which would not be protectable by copyright law. *See, e.g.*, Benjamin L.W. Sobel, *A New Common Law of Web Scraping*, 25 LEWIS & CLARK L. REV. 147, 171–72 (2021); Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S 340, 360 (1991) (holding that copyright law does not protect facts). Derek Bambauer previously opined that providing copyright in face prints or facial features, rather than photographs of faces, would be "stupid," akin to "fixing alcoholism with heroin." Derek Bambauer, *Copyright and Your Face*, PRAWFSBLAWG (Dec. 10, 2011), https://prawfsblawg.blogs.com/prawfsblawg/2011/12/copyright-and-your-face.html [https://perma.cc/KC7S-2FYU]. As discussed in Part III, however, at least some face surveillance companies copy and reproduce photographs of faces, not merely factual information derived from those photographs.

And still others rely on customers to upload photographs as matching datasets.[171] But we do know how at least one company operates. And because we know the most about it, it is used as an example through this part.

Clearview AI scraped photographs—including those used as profile pictures—from sites like Facebook, YouTube, LinkedIn, Venmo, Twitter, and many others, creating copies along the way.[172] That is what journalist Thomas Smith discovered when he requested his file from Clearview AI.[173] He submitted a candid photograph of himself making latkes.[174] In return, Clearview AI provided his "Face Search Results," which reproduced nine other images that the company identified as Smith.[175] The face search results included an "[i]mage [i]ndex" with links to the photographs' source sites. Smith's file reveals that the company makes, stores, and reproduces copies of the photographs it scrapes.[176] Each copy is intrusive.[177] Each copy is unauthorized. And each copy is infringing.[178] Which is why Tim Wu proclaimed that the company "should be the target of a . . . copyright lawsuit."[179]

171. It is likely that some of these companies would attempt to shield their datasets behind trade secrecy in litigation.

172. Hill, *The Secretive Company*, *supra* note 8.

173. Thomas Smith, *I Got My File from Clearview AI and It Freaked Me Out*, ONEZERO (Mar. 24, 2020), https://onezero.medium.com/i-got-my-file-from-clearview-ai-and-it-freaked-me-out-33ca28b5d6d4 [https://perma.cc/K3PT-3JRR (staff-uploaded, dark archive)] [hereinafter Smith, *I Got My File*].

174. *Id.*

175. *Id.*

176. *Id.* This is consistent with journalist Anna Merlan's experience obtaining her own Clearview AI file. Anna Merlan, *Here's the File Clearview AI Has Been Keeping on Me, and Probably on You Too*, VICE (Feb. 28, 2020, 3:17 PM), https://www.vice.com/en/article/5dmkyq/heres-the-file-clearview-ai-has-been-keeping-on-me-and-probably-on-you-too [https://perma.cc/ZZ3J-7KU5]. DataWorks Plus structures its search results similarly. *Face Plus*, DATAWORKS PLUS, https://www.dataworksplus.com/faceplus.html [https://perma.cc/WZ4X-2QUD] ("If there is a possible match, you can choose to view all linked images for a particular gallery image. This will display all linked images for that individual that are currently in your agency's database. This may provide you with images that are easier to match against your probe image.").

177. Just because a photograph is public does not mean its appropriation is not intrusive. *See generally* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004) (explaining how disclosure of information in one context ought to conserve privacy from disclosure in other contexts).

178. 17 U.S.C. § 106(1), (5) (reserving exclusive rights of reproduction and display to copyright owners).

179. Tim Wu (@superwuster), TWITTER (Jan. 18, 2020, 7:26 AM), https://twitter.com/superwuster/status/1218524978225741824?s=20 [https://perma.cc/ED8M-DERE (staff-uploaded archive)]. *But see* Tom Kulik, *In Your Face: How Facial Recognition Databases See Copyright Law but Not Your Privacy*, ABOVE L. (Apr. 1, 2019, 5:17 PM), https://abovethelaw.com/legal-innovation-center/2019/04/01/in-your-face-how-facial-recognition-databases-see-copyright-law-but-not-your-privacy/rf1 [http://perma.cc/SH7C-5JA7] (concluding that IBM's scraping of Creative Commons-licensed images was likely fair use); Jaren Butts, *A "Face-Off" Between Copyrights and Human Rights in the Battle of Facial Recognition Technology*, WAKE FOREST J. BUS. & INTELL. PROP. L. (Sept. 8, 2020), http://ipjournal.law.wfu.edu/2020/09/a-face-off-between-copyrights-and-human-rights-in-the-battle-of-facial-recognition-technology/ [https://perma.cc/6TDK-6MAH] (same).

In the past, researchers and companies seemed sensitive to how copyright law governs the photographs used to train face recognition algorithms. Raji and Genevieve Fried documented how developers of early face recognition datasets actually "pa[id] considerable attention to issues of copyright and the protection of image ownership rights in distribution practices" and avoided legal issues by creating photographs of subjects who consented to, and were occasionally compensated for, participation.[180] Facebook and other companies have used their business models as a means to license selfies and other sources of training data for proprietary AI systems.[181] The Pilot Parliaments Benchmarks dataset curated by Buolamwini and Gebru avoids copyright by using only public domain images.[182] And Microsoft and IBM scraped photographs from Flickr designated with Creative Commons licenses[183]—to which Creative Commons responded that "copyright is not a good tool to protect individual privacy, to address research ethics in AI development, or to regulate the use of surveillance tools employed online."[184] True enough. But even if copyright is not a *good* tool, there are several reasons it may still be the one to get the job done for now.

One common defense of scraping does not shield against copyright infringement: the First Amendment. In its motion to dismiss the ACLU's BIPA lawsuit, Clearview AI cited the Supreme Court's observation that "[t]he 'creation and dissemination of information are speech within the meaning of the First Amendment'" to support its claim that scraping photographs to fuel face surveillance constitutes protected First Amendment speech.[185] But as Julie

180. INIOLUWA DEBORAH RAJI & GENEVIEVE FRIED, ABOUT FACE: A SURVEY OF FACIAL RECOGNITION EVALUATION 6 (2021), https://arxiv.org/pdf/2102.00813.pdf [https://perma.cc/7J6N-GBSQ] (observing that scrupulous attention to copyright and consent faded with contemporary scraped datasets).

181. Levendowski, *Copyright Law*, *supra* note 19, at 606–07 (describing AI's "build-it model").

182. Buolamwini & Gebru, *supra* note 19, at 79.

183. Madhumita Murgia, *Microsoft Quietly Deletes Largest Public Face Recognition Data Set*, FIN. TIMES (June 6, 2019), https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2 [https://perma.cc/ZZH2-GZBT (dark archive)] (describing Microsoft's scraping of photographs from Flickr); Olivia Solon, *Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped Without Consent*, NBC NEWS (Mar. 12, 2020), https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921 [https://perma.cc/X4ZH-H57L] (Mar. 17, 2019, 11:25 AM) (describing IBM's scraping of photographs from Flickr). This approach may have sidestepped copyright issues, but it stumbled into ethical ones. To see whether your photographs are part of a dataset, see Cade Metz & Kashmir Hill, *Here's a Way To Learn if Facial Recognition Systems Used Your Photos*, N.Y. TIMES, https://www.nytimes.com/2021/01/31/technology/facial-recognition-photo-tool.html [https://perma.cc/K5EE-7VFS (dark archive)] (Feb. 1, 2021) (describing Exposing.AI investigation tool).

184. Ryan Merkley, *Use and Fair Use: Statement on Shared Images in Facial Recognition AI*, CREATIVE COMMONS: BLOG (Mar. 13, 2019), https://creativecommons.org/2019/03/13/statement-on-shared-images-in-facial-recognition-ai/ [https://perma.cc/84D9-2BKL].

185. Defendant's Memorandum of Law in Support of Its Motion to Dismiss at 16, ACLU v. Clearview AI, Inc., No. 2020-CH-04353 (Ill. Cir. Ct. Oct. 7, 2020) (quoting Sorrell v. IMS Health Inc., 564 U.S. 552, 570 (2011)); *see also* Kashmir Hill, *Facial Recognition Start-Up Mounts a First Amendment Defense*, N.Y. TIMES, https://www.nytimes.com/2020/08/11/technology/clearview-floyd-

Cohen wryly notes, "to be a copyright lawyer is always in some sense to be a First Amendment lawyer."[186] Copyright infringement is not protected by the First Amendment—indeed, the Supreme Court sees no conflict between the First Amendment and copyright law.[187] The Court has specifically observed that "copyright law contains built-in First Amendment accommodations" that "strike[] a definitional balance between the First Amendment and copyright law by permitting free communication of facts while still protecting an author's expression."[188]

Not only do the First Amendment and copyright laws coexist, but copyright can also serve as a significant deterrent to face surveillance. Copyright law provides hefty statutory damages to the tune of $150,000 per instance of willful infringement.[189] Clearview AI alone sits on a system backed by copies of billions of photographs, and that number likely grows each day.[190] And unlike many biometric and face surveillance statutes, copyright does not rely on action by state attorneys general.[191] As Woodrow Hartzog has concluded, "only private causes of action seem capable of meaningfully deterring companies from engaging in practices with biometrics based on business models that inevitably lead to unacceptable abuses."[192] Copyright law happens to provide one.[193]

Despite the alarming biases discussed in Part I, some scholars remain skeptical of using copyright to protect privacy.[194] After all, the constitutional

abrams.html [https://perma.cc/KXJ8-5QS8 (dark archive)] (Mar. 18, 2021) [hereinafter Hill, *Facial Recognition Start-Up*]. *But see* Brief of Law Professors as Amici Curiae in Opposition to Defendant's Motion to Dismiss at 2, *ACLU*, No. 2020-CH-04353 (amicus brief of First Amendment scholars). The court recently found that "Clearview's activities . . . are entitled to some First Amendment protection" but found that intermediate scrutiny was satisfied. *ACLU*, No. 2020-CH-4353, at 9–10, https://www.aclu.org/opinion-denying-clearview-ais-motion-dismiss [https://perma.cc/9BHB-R9DY].

186. Julie E. Cohen, *Intellectual Privacy and Censorship of the Internet*, 8 SETON HALL CONST. L.J. 693, 694 (1998).

187. Scholars are another story. *See, e.g.*, Joseph P. Bauer, *Copyright and the First Amendment: Comrades, Combatants, or Uneasy Allies?*, 67 WASH. & LEE L. REV. 831, 914 (2010) (suggesting that copyright law should bend to First Amendment speech).

188. Eldred v. Ashcroft, 537 U.S. 186, 190 (2003) (citing Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 556, 560 (1985)). *Eldred* is a real bummer of a case for other reasons, such as allowing the extension of copyright terms.

189. 17 U.S.C. § 504(c)(2). These damages are limited to infringement that takes place after the work is registered with the Copyright Office, however. *Id.* § 412.

190. Hill, *The Secretive Company*, *supra* note 8.

191. Michael A. Rivera, *Face Off: An Examination of State Biometric Privacy Statutes & Data Harm Remedies*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 571, 586 (2019).

192. Hartzog, *supra* note 144, at 96, 101.

193. 17 U.S.C. § 501(b).

194. *See, e.g.*, Pierre N. Leval, *Toward a Fair Use Standard*, 103 HARV. L. REV. 1105, 1129 (1990) ("The occasional attempt to read protection of privacy into the copyright is also mistaken."); Rebecca Tushnet, *How Many Wrongs Make a Copyright?*, 98 MINN. L. REV. 2346, 2348 (2014) (reviewing Derek E. Bambauer, *Exposed*, 98 MINN. L. REV. 2025 (2014), and rejecting the suggestion that copyright should be used to protect the privacy of nonconsensual pornography victims); Fromer, *supra* note 24, at 580 (referring to protection of privacy as an "ill-fitting motivation[]" for asserting copyright); M.

purpose of copyright is to "promote the progress of science and useful arts," not to save society from invasive face surveillance.[195] But the deep, damaging, and damning biases embedded in face surveillance technology suggests that it does not promote progress at all—and that copyright law is poised to prevent its attack on privacy.

Other scholars concur.[196] Shyamkrishna Balganesh has observed that copyright is fully capable of not only addressing economic harms but also ones that "emerge[] instead from the mere dissemination or use of the protected work without the creator's authorization, regardless of the objective utility or value of such actions."[197] And copyright is no stranger to privacy. In 1890, Samuel Warren and Louis Brandeis analogized privacy protection to copyright law in their famed article, *The Right to Privacy*, by illustrating the ways in which

Margaret McKeown, *Censorship in the Guise of Authorship: Harmonizing Copyright and the First Amendment*, 15 CHI.-KENT J. INTELL. PROP. 1, 8–9 (2016) ("[C]opyright is not the answer to your privacy prayers."); Edward Lee, *Suspect Assertions of Copyright*, 15 CHI.-KENT J. INTELL. PROP. 379, 385 (2016) ("If a work has already been published with the author's authorization, then the author has effectively renounced her First Amendment right not to speak and whatever privacy interest in the work copyright protects through the right of first publication is lost."); Christopher Buccafusco & David Fagundes, *The Moral Psychology of Copyright Infringement*, 100 MINN. L. REV. 2433, 2487–88 (2016) (outlining the adoption of an "incentive-relevant harm" standard, while acknowledging the interpretative challenge for judges); Eric Goldman & Jessica Silbey, *Copyright's Memory Hole*, 2019 BYU L. REV. 929, 996 ("Despite the legitimate and sometimes profound harms experienced by some privacy victims, copyright law should not be manipulated to fix privacy law's problems."); Sobel, *supra* note 170, at 170 ("Copyright is an economic right, not a privacy protection.").

195. The idea that contemporary copyright remains beholden to the Progress Clause is unmoored from reality. *See generally* U.S. CONST. art. I, § 9, cl. 2 (the Progress Clause); Eldred v. Ashcroft, 537 U.S. 186 (2003) (upholding copyright term extension absent any supporting empirical evidence justifying an extension).

196. Jon O. Newman, *Copyright Law and the Protection of Privacy*, 12 COLUM.-VLA J.L. & ARTS 459, 463, 479 (1988) ("There is a strong indication in the early cases that while the right being articulated was one of property, the interest being protected was one of privacy. . . . In shaping the contours of copyright law, we should acknowledge the privacy interest not just for the great writers but for each one of us."); Bambauer, *supra* note 194, at 2058 (recommending amending copyright law to grant subjects of nonconsensual pornography authorship rights); Amanda Levendowski, *Using Copyright To Combat Revenge Porn*, 3 N.Y.U. J. INTELL. PROP. & ENT. L. 422, 442–43 (2014) [hereinafter Levendowski, *Using Copyright To Combat Revenge Porn*] (suggesting using the Digital Millennium Copyright Act to remove nonconsensual pornography from the internet); Margaret Chon, *Copyright's Other Functions*, 15 CHI.-KENT J. INTELL. PROP. 364, 366 (2016) ("Privacy and other functions of copyright should not be categorically excluded as beyond the legitimate purview of copyright's concerns, and copyright will not be stretched beyond its breaking point by incorporating them."); Andrew Gilden, *Sex, Death, and Intellectual Property*, 32 HARV. J.L. & TECH. 67, 68 (2018) ("IP is doing work that it was not intended to do. And this is okay."); Shyamkrishna Balganesh, *Privative Copyright*, 73 VAND. L. REV. 1, 37–59 (2020) (tracing the longstanding history of using copyright law to protect privacy); Smith, *Weaponizing Copyright*, *supra* note 31, at 64 ("[T]here are strong arguments to allow copyright to not only protect economic interests in copyrighted works, but also allow it to be weaponized in limited circumstances to protect privacy.").

197. Balganesh, *supra* note 196, at 7.

copyright distinguished publicly permissible from disallowable disclosures.[198] Nearly a century later, the Supreme Court acknowledged that "common-law copyright was often enlisted in the service of personal privacy."[199] Today, victims of nonconsensual pornography effectively use copyright law to remove their images from the internet and seek remedies from infringers.[200] As Madhavi Sunder puts it, "the fact that intellectual property law might be established for instrumental reasons does not mean that other purposes should not be considered . . . ."[201] So why has there not been an avalanche of copyright infringement lawsuits against Clearview AI and companies like it? Fair use.

Beginning with fair use may feel like dropping into the middle of a copyright infringement lawsuit—there are certainly other hurdles before a court reaches fair use. A potential plaintiff, who may be the photographer rather than the subject of the image (or in the case of selfies, both), must register their work with the Copyright Office.[202] That plaintiff, along with their attorneys, must decide whether to proceed individually or as part of a class action.[203] Even if several plaintiffs proceed individually, their lawsuits may be consolidated and transferred for coordinated pretrial proceedings through opaque multidistrict litigation.[204] If plaintiffs proceed through a class action, they must wait to see whether their class is certified.[205] But as the Supreme Court recently confirmed in *Google v. Oracle*,[206] fair use is a mixed question of fact and law that "primarily

198. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 199–205 (1890). Warren and Brandeis pointed to letters, contents of a diary, and a series of paintings or etchings to illustrate how the flexible rules of copyright law might allow some uses (descriptions of the works) while disallowing others (verbatim reproduction of them). *Id.* at 201.

199. Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 554 (1985).

200. Levendowski, *Using Copyright To Combat Revenge Porn*, *supra* note 196, at 442–45 (detailing how to use the Digital Millennium Copyright Act to remove nonconsensual pornography and explaining that such infringement may be litigable with sizeable statutory damages); *Online Removal Guide*, CYBER C.R. INITIATIVE, https://www.cybercivilrights.org/online-removal/ [https://perma.cc/Y39E-LTCG] (explaining that victims of nonconsensual pornography may be able to rely on copyright); Hauser, *supra* note 27 (describing copyright infringement judgment with sizable statutory damages).

201. MADHAVI SUNDER, FROM GOODS TO A GOOD LIFE: INTELLECTUAL PROPERTY AND GLOBAL JUSTICE 102 (2012).

202. 17 U.S.C. § 412; Fourth Est. Pub. Benefit Corp. v. Wall-Street.com, LLC, 139 S. Ct. 881, 890 (2019) ("[I]t is the Register's action that triggers a copyright owner's entitlement to sue.").

203. *See generally* FED. R. CIV. P. 23 (detailing class action procedures and requirements).

204. 28 U.S.C. § 1407(a) ("When civil actions involving one or more common questions of fact are pending in different districts, such actions may be transferred to any district for coordinated or consolidated pretrial proceedings."). Proceedings may be transferred by the judicial panel on multidistrict litigation or a party's motion. *Id.* § 1407(c). For an illuminating discussion of how the mechanics of multidistrict consolidation and class-action certification operate in information privacy litigation, see Julie E. Cohen, *Information Privacy Litigation as a Bellwether for Institutional Change*, 66 DEPAUL L. REV. 535, 567–70 (2017).

205. *See* FED. R. CIV. P. 23.

206. Google LLC v. Oracle Am., Inc., 141 S. Ct. 1183 (2021).

involves legal work," making it litigable at the motion-to-dismiss stage, which may precede multidistrict consolidation or overlap with class certification.[207]

Addressing the question of fair use is crucial because making fair use of a copyrighted work is "not an infringement of copyright"[208]—it is also a key reason behind the Court's finding that copyright law contains "built-in First Amendment accommodations."[209] In 1841, a judicial decision about George Washington's correspondence gave us fair use.[210] An author copied 353 pages of an earlier book incorporating Washington's letters, "private and official," into his own tome.[211] Justice Story determined that copying the pages was an act of "piracy" and announced a test for evaluating whether a copier's use was fair by "look[ing] to the nature and objects of the selections made, the quantity and value of the materials used, and the degree in which the use may prejudice the sale, or diminish the profits, or supersede the objects, of the original work."[212] More than a century later, the Copyright Act of 1976 resulted in the codification of fair use.[213]

Fair use calls on courts to assess four factors:

(1) The purpose and character of the use . . . ;
(2) The nature of the copyrighted work;
(3) The amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
(4) The effect of the use upon the potential market for or value of the copyrighted work.[214]

As the Supreme Court recently observed in *Google*, "we have understood the provision to set forth general principles, the application of which requires judicial balancing, depending upon relevant circumstances, including

207. *Id.* at 1199–200. Timing for consolidation and certification are not statutorily defined. *See* § 1407(a) ("Such transfers shall be made by the judicial panel on multidistrict litigation authorized by this section upon its determination that transfers for such proceedings will be for the convenience of parties and witnesses and will promote the just and efficient conduct of such actions."); FED. R. CIV. P. 23(c)(1)(A) ("At an early practicable time after a person sues or is sued as a class representative, the court must determine by order whether to certify the action as a class action.").

208. 17 U.S.C. § 107.

209. Eldred v. Ashcroft, 537 U.S. 186, 190 (2003) (citing Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 560 (1985)).

210. Folsom v. Marsh, 9 F. Cas. 342, 345 (C.C.D. Mass. 1841) (No. 4901).

211. *Id.* at 345.

212. *Id.* at 348.

213. The Act was strongly influenced by Barbara Ringer. For more about the work and legacy of Barbara Ringer, see Amanda Levendowski, *The Lost and Found Legacy of Barbara Ringer*, ATLANTIC (July 11, 2014), https://www.theatlantic.com/technology/archive/2014/07/the-lost-and-found-legacy-of-a-copyright-hero/373948/ [https://perma.cc/82U6-YRGM (dark archive)] and *Advancing Inclusion in Copyright and Register Barbara Ringer's Legacy*, U.S. COPYRIGHT OFF. (Nov. 19, 2020, 5:00 PM), https://copyright.gov/events/barbara-ringer/ [https://perma.cc/2BRY-TG4F].

214. 17 U.S.C. § 107.

'significant changes in technology.'"[215] In that case, Oracle sued Google for copying a portion of the Sun Java application programming interface ("API"), which allows programmers to call up prewritten software that carries out specific tasks.[216] Google copied thirty-seven packages of Oracle's declaring code—copying that helped create the ubiquitous Android platform.[217] In its first decision to address fair use since 2 Live Crew was a chart-topper,[218] the Court applied the four fair use factors to determine whether Google's use promoted "creative 'progress' that is the basic constitutional objective of copyright itself," ultimately holding that Google's copying was fair use.[219]

As I have written in previous work, ML will challenge and potentially redefine fair use—many uses of copyrighted works to train AI systems, from algorithms that recognize images of cats to those that autocomplete emails, likely constitute fair use.[220] However, the underlying rationales justifying fair use in those instances may not hold in at least one sliver of the overall ecosystem: using profile pictures for face surveillance.

Put another way, not all uses of copyrighted works as AI training data will be fair use. This complexity is rooted in fair use's flexibility. While fair use is flexible, empirical and qualitative work by Pamela Samuelson,[221] Matthew Sag,[222] and Barton Beebe[223] demonstrates that fair use can also be surprisingly predictable. This part uses *Google v. Oracle*, alongside other key fair use cases, to assess each fair use factor as it applies to copying and reproducing profile pictures. Section III.A begins by establishing that some face surveillance companies copy photographs to fuel face surveillance algorithms for the same purpose as users who choose the photos as profile pictures: particularized identification. But even without a new purpose, such a use may still be

215. Google LLC v. Oracle Am., Inc., 141 S. Ct. 1183, 1197 (2021) (quoting Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 430 (1984)).

216. *Id.* at 1193.

217. *Id.* at 1191, 1193.

218. *See* Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569 (1994) (detailing the most recent Supreme Court decision on fair use).

219. *Google LLC*, 141 S. Ct. at 1203 (citing Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S 340, 349–50 (1991)).

220. Levendowski, *Copyright Law*, *supra* note 19, at 579; *see also* Lemley & Casey, *supra* note 26, at 745.

221. *See generally* Pamela Samuelson, *Unbundling Fair Uses*, 77 FORDHAM L. REV. 2537 (2009) (giving a qualitative assessment of fair use cases that identifies "policy-relevant clusters" with predictive power over fair use outcomes).

222. *See generally* Matthew Sag, *Predicting Fair Use*, 73 OHIO ST. L.J. 47 (2012) (giving an empirical analysis of fair use cases that reveals the rationality and consistency of fair use outcomes).

223. *See generally* Barton Beebe, *An Empirical Study of U.S. Copyright Fair Use Opinions Updated, 1978–2019*, 10 J. INTELL. PROP. & ENT. L. 1 (2020) [hereinafter Beebe, *An Empirical Study Updated*] (providing an empirical review of fair use cases that identifies trends in fair use outcomes); *see also* Barton Beebe, *An Empirical Study of U.S. Copyright Fair Use Opinions, 1978–2005*, 156 U. PA. L. REV. 549 (2008) (reviewing an earlier set of opinions).

somewhat transformative, favoring face surveillance companies. Sections III.B and III.C then observe that the nature of the work is creative and that the use features the photographs' faces—the "heart" of profile pictures, creating unfavorable outcomes for these companies under the middle two factors. Finally, Section III.D explains how using these photographs harms the unique licensing market for profile pictures, possibly foreclosing a favorable outcome under the final factor. Face surveillance can never be just, and it likely cannot be fair use either.

A. *Purpose, Transformation, and Character*

The first fair use factor explores "the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes."[224] As the Supreme Court recently explained, courts "consider[] whether the copier's use 'adds something new, with a further purpose or different character, altering' the copyrighted work 'with new expression, meaning[,] or message.'"[225] As a shorthand for this inquiry, courts ask whether the new work is "transformative."[226] A copier's work is transformative when it is "productive and . . . employ[s] the quoted matter in a different manner or for a different purpose from the original. A quotation of copyrighted material that merely repackages or republishes the original is unlikely to pass the test . . . ."[227] Or as Justice Story framed it, "[t]he central purpose of this investigation is to see . . . whether the new work merely 'supersede[s] the objects' of the original creation."[228]

1. Purpose

Purpose is a straightforward factor when two works "at least at a high level of generality, share the same overarching purpose."[229] This seems to be the case with face surveillance. Social media users, journalists, and coders, among many other web users, share photographs of their own faces to identify themselves and match those photos to their offline identities. Empirical work by Scott Counts and Kristin Stecher reveals that profile pictures are "particularly

224. 17 U.S.C. § 107(1).

225. Google LLC v. Oracle Am., Inc., 141 S. Ct. 1183, 1202 (2021) (quoting Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 579 (1994)).

226. *Campbell*, 510 U.S. at 579. Transformativeness is not necessary for a finding of fair use, but empirically it makes a great deal of difference. *See, e.g.*, Jiarui Liu, *An Empirical Study of Transformative Use in Copyright Law*, 22 STAN. TECH. L. REV. 163, 163 (2019) (finding that in dispositive decisions upholding transformative use, ninety-four percent led to a fair-use finding).

227. Leval, *supra* note 194, at 1111.

228. *Campbell*, 510 U.S. at 579 (quoting Folsom v. Marsh, 9 F. Cas. 342, 348 (C.C.D. Mass. 1841) (No. 4901)).

229. Andy Warhol Found. for the Visual Arts, Inc. v. Goldsmith, 11 F.4th 26, 40 (2d Cir. 2021), *amended*, 11 F.4th 26 (2d Cir. Aug. 24, 2021).

important for conveying online identity."[230] The purpose of every social media photograph may not overlap with face surveillance, but the purpose of profile pictures and face surveillance is the same: particularized identification.[231] Clearview AI, for example, characterizes the purpose of its face recognition technology as "identification and matching of facial image data to stored facial image and personal information data."[232] Social media users may be unlikely to consider law enforcement when choosing photographs of their faces for profile pictures, but the purpose remains that users are identifying themselves *as* themselves to friends, followers, and even police who view their profiles.

But shared purpose is insufficient to subvert fair use. In *Google*, Google copied portions of the Sun Java API "in part for the same reason that Sun created those portions."[233] As the Court noted, limiting fair use to wholly different purposes would "severely limit the scope of fair use."[234] Notably, Clearview AI claims a different, transformative purpose, as discussed below.

2. Transformativeness

Even if Clearview AI and companies like it use profile pictures, even in part, for the shared purpose of particularized identification, *Google* allows their use if it is transformative.[235] The company pitched itself as a "search engine . . . providing for highly accurate facial recognition."[236] Its lawyer claims that the service "operates in much the same way as Google's search engine."[237] And it is likely that other face surveillance companies believe the same. But search engine and private subscription service cases complicate where face surveillance companies fall on the spectrum of transformativeness.

In *Kelly v. Arriba Soft*,[238] Leslie Kelly, a professional photographer, sued an early search engine for "copying [his] images from other websites."[239] The

230. Scott Counts & Kristin Stecher, *Self-Presentation of Personality During Online Profile Creation*, 2009 PROC. THIRD ICWSM CONF. 191, 194.

231. NATHAN JURGENSON, THE SOCIAL PHOTO: ON PHOTOGRAPHY AND SOCIAL MEDIA 54 (2019) ("Anyone who has put together a profile page might recognize . . . the social photo may best illustrate this kind of identity work. The self—that feeling that you are you and not someone else—is a story you tell yourself to connect the person you once were to who you are now to who you will become. Photography plays an integral role in linking the self over time.").

232. U.S. Trademark Application Serial No. 88779027 (filed Jan. 30, 2020).

233. Google LLC v. Oracle Am., Inc., 141 S. Ct. 1183, 1203 (2021).

234. *Id.*

235. *Id.*

236. *Principles*, CLEARVIEW AI, https://www.clearview.ai/principles [https://perma.cc/GM3V-YJQA].

237. Ben Gilbert, *Clearview AI Scraped Billions of Photos from Social Media To Build a Facial Recognition App that Can ID Anyone—Here's Everything You Need To Know About the Mysterious Company*, BUS. INSIDER (Mar. 6, 2020, 12:31 PM), https://www.businessinsider.com/what-is-clearview-ai-controversial-facial-recognition-startup-2020-3 [https://perma.cc/3YCL-65UK].

238. Kelly v. Arriba Soft Corp., 336 F.3d 811 (9th Cir. 2003).

239. *Id.* at 815.

search engine proceeded to present Kelly's photographs as low-resolution thumbnails that "used in-line linking to display . . . a link to the original web site."[240] The Ninth Circuit explained that a "search engine functions as a tool to help index and improve access to images on the internet and their related web sites."[241] In that sense, the thumbnails of Kelly's images "do not supplant the need for the originals. In addition, they benefit the public by enhancing information-gathering techniques on the Internet."[242] Four years later, the Ninth Circuit revisited the transformativeness of search engines in *Perfect 10 v. Amazon*.[243] Perfect 10 sold subscriptions to access photographs of nude models.[244] The company also targeted Google's Image Search, which returned thumbnail images of Perfect 10 photographs, sometimes from infringing websites, along with "HTML instructions [that] also give the user's browser the address of the website publisher's computer that stores the full-size version of the thumbnail."[245] Judge Ikuta, writing for a unanimous panel, concluded that images could serve "an entertainment, aesthetic, or information function, [but] a search engine transforms the image into a pointer directing a user to a source of information."[246] The district court had acknowledged the "truism that search engines such as Google Image Search provide great value to the public."[247] Judge Ikuta agreed, finding that "the significantly transformative nature of Google's search engine, particularly in light of its public benefit" weighed for a favorable finding under the first factor.[248]

Both the Arriba Soft and Google search engines shared two key characteristics: publicly transforming images into pointers to the original source and serving a public benefit by organizing content for all internet users. As Smith detailed in reporting on his own Clearview AI face search results, the company includes links to the sources of each photograph at the bottom of the results, but those pointers are only available to law enforcement subscribers.[249] Directing users back to the source seems to be a necessary feature of search engines but perhaps not enough to automatically qualify as one.

Unsuccessful "search engines" instead take the form of private subscription services. In *Associated Press v. Meltwater U.S. Holdings, Inc.*,[250] a subscription news monitoring service called Meltwater launched a business

240. *Id.* at 816.
241. *Id.* at 818.
242. *Id.* at 820.
243. Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146 (9th Cir. 2007).
244. *Id.* at 1157.
245. *Id.* at 1155.
246. *Id.* at 1165.
247. *Id.* at 1166 (citing Perfect 10 v. Google, Inc., 416 F. Supp. 2d 828, 848–49 (C.D. Cal. 2006)).
248. *Id.*
249. Smith, *I Got My File*, *supra* note 173.
250. 931 F. Supp. 2d 537 (S.D.N.Y. 2013).

model around "'scrap[ing]' an article from an online news source, index[ing] the article, and deliver[ing] verbatim excerpts of the article to its customers in response to search queries."[251] Like Clearview AI, the company called itself an "Internet search engine," arguing that it "provid[ed] limited amounts of copyrighted material to its subscribers in response to their queries and thereby pointing its subscribers to a source of information online."[252] To support its claim, Meltwater noted that its digests generally included "a hyperlink to the URL for the website from which the article was indexed."[253] However, writing for the Southern District of New York, Judge Cote found that including links does not automatically render a search engine's use of copyrighted works transformative: "Instead of driving subscribers to third-party websites, Meltwater News acts as a substitute for news sites," Judge Cote observed.[254] The same may be true of Clearview AI and companies like it. But even if Clearview AI funnels customers back to other websites, it remains unlikely that the company fulfills that second search engine feature: serving a clear public benefit.

Unlike public search engines like Arriba Soft and Google, services like Clearview AI are pricey subscription services that are often available exclusively to law enforcement. Indeed, Judge Cote distinguished Meltwater from a search engine by noting that the company was "an expensive subscription service" rather than "a publicly available tool to improve access to content across the Internet."[255] Some may say that streamlining law enforcement investigations serves one kind of public benefit, though the contention remains hotly contested.[256]

Under its analysis of market effects in *Google*, the Supreme Court questioned what might constitute a "public benefit." The Court asked whether "those benefits, for example, [are] related to copyright's concern for creative production of new expression?"[257] Not surprisingly, the Court asked a version

251. *Id.* at 543. I previously worked on this matter as a summer associate at Davis Wright Tremaine, which litigated this case on behalf of the Associated Press. All comment is based on public information.

252. *Id.* at 550.

253. *Id.* at 545.

254. *Id.* at 554.

255. *Id.* at 553–54.

256. DJ Pangburn, *San Diego's Massive, 7-Year Experiment with Facial Recognition Technology Appears To Be a Flop*, FAST CO. (Jan. 9, 2020), https://www.fastcompany.com/90440198/san-diegos-massive-7-year-experiment-with-facial-recognition-technology-appears-to-be-a-flop [https://perma.cc/2EHU-UHKW (dark archive)]; Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. TIMES (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html [https://perma.cc/VZ34-CW7T (dark archive)]; Alfred Ng, *Facial Recognition in Schools: Even Supporters Say It Won't Stop Shootings*, CNET (Jan. 24, 2020), https://www.cnet.com/features/facial-recognition-in-schools-even-supporters-say-it-wont-stop-shootings/ [https://perma.cc/T34S-M578].

257. Google LLC v. Oracle Am., Inc., 141 S. Ct. 1183, 1206 (2021).

of this question when assessing the first factor by querying whether copying was consistent with "creative 'progress.'"[258] Here, as in *Google*, Clearview AI "seeks to create new products."[259] From the company's perspective, it "expand[s] the use and usefulness" of profile pictures.[260] Its "new product" offers law enforcement a "highly creative and innovative tool" for surveillance.[261] However, creative progress is supposed to be linked with the "basic constitutional objective of copyright itself," leaving open an argument that using profile pictures to fuel face surveillance fails to promote the constitutional purpose of progress of science and useful arts.[262]

Thus, it remains far from clear whether face surveillance services provide for the "public good." While not a factor to be considered in and of itself, whether a use serves the public good or benefit plays a role in courts' analysis of the first factor, including transformativeness. Face surveillance technology has certainly been used to solve crimes.[263] It has also been deployed to surveil marginalized people and wrongfully imprison multiple people based on demographic and deployment biases—and those are just the injustices that have been made public.[264] Creating massive searchable databases of millions of faces collected without consent, maintained without regulation, and sold without oversight to law enforcement strikes differently than presenting thumbnail photos or snippets from books. Face surveillance is contentious and controversial, certainly far from an unqualified public good.[265]

Setting aside whether face surveillance serves a public benefit or public good, it cannot be argued that face surveillance companies provide a "publicly available tool" in the manner of Arriba Soft and Google's search engines. Instead, face surveillance companies feel like an apt target of Judge Cote's conclusion that "using the mechanics of search engines to scrape material from the Internet and provide it to consumers in response to their search requests does not immunize a defendant from the standards of conduct imposed by law

258. *Id.* at 1203 (citing Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S 340, 349–50 (1991)).

259. *Id.*

260. *Id.*

261. *Id.*

262. *Id.* (citing U.S. CONST. art. I, § 8, cl. 8).

263. Law enforcement claims to have used Clearview AI, for example, to solve "shoplifting, identity theft, credit card fraud, murder and child sexual exploitation cases." Hill, *The Secretive Company*, *supra* note 8. But at least one law enforcement agency, the NYPD, has countered that Clearview AI's marketing claims were inaccurate on at least one occasion. Tim Cushing, *Facial Recognition Company Clearview Lied About Its Crime-Solving Power in Pitches to Law Enforcement Agencies*, TECHDIRT (Jan. 29, 2020, 6:59 AM), https://www.techdirt.com/articles/20200125/1846344379 8/facial-recognition-company-clearview-lied-about-crime-solving-power-pitches-to-law-enforcement-agencies.shtml [https://perma.cc/QV5X-J96Y].

264. Hill, *Wrongfully Accused*, *supra* note 1.

265. *See, e.g.*, *supra* notes 13–15 and accompanying text.

through the Copyright Act."[266] This may tilt against face surveillance companies as they exist presently, but it perversely means that a company that makes its tool available publicly—with all the use and abuse that entails—may be on more solid ground.

Clearview AI also boasts about enabling "quicker identifications and apprehensions."[267] Its argument tracks the Second Circuit observations in *Fox News v. TVEyes*[268] that "a secondary use may be a fair use if it utilizes technology to achieve the transformative purpose of improving the efficiency of delivering content without unreasonably encroaching on the commercial entitlements of the rights holder."[269] In that case, a company called TVEyes copied "essentially all television broadcasts as they happen, drawing from more than 1,400 channels, recording twenty-four hours a day, every day," along with the accompanying closed-captioning, and offered $500 monthly subscriptions to clients.[270] Judge Jacobs, writing for a unanimous panel, announced the court's conclusion that the service was

> not justifiable as a fair use. As to the first factor, TVEyes's Watch function [wa]s at least somewhat transformative in that it render[ed] convenient and efficient access to a subset of content; however, because the function d[id] little if anything to change the content itself or the purpose for which the content [wa]s used, its transformative character [wa]s modest at best.[271]

Face surveillance companies arguably make even less transformative uses than TVEyes, which "enable[d] nearly instant access to a subset of material . . . that would otherwise be irretrievable, or else retrievable only through prohibitively inconvenient or inefficient means."[272] While it is less convenient, law enforcement regularly and successfully uses social media to aid investigations without the help of face surveillance subscription services.

As Rachel Levinson-Waldman explains, "Perhaps the simplest way of learning more about a target or group of individuals online is to follow them on public social media platforms . . . . [This] easy availability of detailed information about individuals' activities has turned social media into a wellspring of information for law enforcement."[273] And aside from face

266. Associated Press v. Meltwater U.S. Holdings, Inc., 931 F. Supp. 2d 537, 556 (S.D.N.Y. 2013).

267. *Law Enforcement*, CLEARVIEW AI, https://clearview.ai/law-enforcement [https://perma.cc/C2BY-PGKY].

268. Fox News Network, LLC v. TVEyes, Inc., 883 F.3d 169, 177 (2d Cir. 2018).

269. *Id.* I formerly worked at Kirkland & Ellis, which litigated this case on behalf of Fox News. All comment is based on public information.

270. *Id.* at 175.

271. *Id.* at 180–81.

272. *Id.* at 177.

273. Levinson-Waldman notes that these efforts "inevitably put greater scrutiny on communities of color," not unlike face surveillance. Rachel Levinson-Waldman, *Government Access to and*

recognition technology, the FBI and U.S. Capitol Police used photographs on social media to identify, investigate, and charge suspects involved in the Capitol Riot on January 6, 2021.[274] ICE uses social media to identify, arrest, and deport undocumented immigrants.[275] Many other agencies rely on social media in their investigations.[276] Law enforcement has no problem using social media photographs to identify targets—face surveillance companies merely make accessing social media profile photos easier. The business model is nothing more than "aggregated content already available to the individual user who was willing to perform enough searches and cull enough results on the Internet."[277] Rather than providing a "database of otherwise unavailable content," as TVEyes did, Clearview AI and companies like it, "simply 'crawl[]' the Internet, gathering extant content."[278] Judge Cote summed it up in *Meltwater*: "[U]se of an algorithm to crawl over and scrape content from the Internet is surely not enough to qualify as a search engine engaged in transformative work."[279]

While being a private subscription service tends to weigh against transformativeness, it is not dispositive. In *A.V. ex rel Vanderhye v. iParadigms, LLC*,[280] the company Turnitin developed plagiarism detection software that used high school and college students' copyrighted works as training data for identifying lifted passages.[281] There, the Fourth Circuit determined that the software was "transformative," despite being a subscription service to schools

Manipulation of Social Media: Legal and Policy Challenges, 61 HOW. L. REV. 523, 527 (2018); *see also* Wayne A. Logan & Jake Linford, *Contracting for Fourth Amendment Privacy Online*, 104 MINN. L. REV. 101, 102–03 (2019).

274. Kevin Collier, *Selfies, Social Media Posts Making It Easier To Track Down Capitol Riot Suspects*, NBCNEWS (Jan. 16, 2021, 6:34 PM), https://www.nbcnews.com/tech/social-media/selfies-social-media-posts-making-it-easier-fbi-track-down-n1254522 [https://perma.cc/NM5D-YMSD]; Sara Morrison, *The Capitol Rioters Put Themselves All Over Social Media. Now They're Getting Arrested*, VOX, https://www.vox.com/recode/22218963/capitol-photos-legal-charges-fbi-police-facebook-twitter [https://perma.cc/VP7N-NUPC] (Jan. 19, 2021, 6:52 PM). Law enforcement also used face recognition technology in investigating the January 6 insurrection. Drew Harwell, *How America's Surveillance Networks Helped the FBI Catch the Capitol Mob*, WASH. POST (Apr. 2, 2021, 9:00 AM), http://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy/ [https://perma.cc/5QC3-V2AT (dark archive)].

275. Max Rivlin-Nadler, *How ICE Uses Social Media To Surveil and Arrest Immigrants*, INTERCEPT (Dec. 22, 2019, 8:00 AM), https://theintercept.com/2019/12/22/ice-social-media-surveillance/ [https://perma.cc/7MLN-S6TJ].

276. *See generally* FAIZA PATEL, RACHEL LEVINSON-WALDMAN, SOPHIA DENUYL & RAYA KOREH, BRENNAN CTR. FOR JUST., SOCIAL MEDIA MONITORING: HOW THE DEPARTMENT OF HOMELAND SECURITY USES DIGITAL DATA IN THE NAME OF NATIONAL SECURITY (2019), https://www.brennancenter.org/sites/default/files/publications/2019_DHS-SocialMediaMonitoring_FINAL.pdf [https://perma.cc/K6Q6-TSGN] (detailing the Department of Homeland Security's collection, use, and sharing of social media information).

277. Fox News Network, LLC v. TVEyes, Inc., 43 F. Supp. 3d 379, 393 (S.D.N.Y. 2014).

278. *Id.*

279. Associated Press v. Meltwater U.S. Holdings, Inc., 931 F. Supp. 2d 537, 555 (S.D.N.Y. 2013).

280. 562 F.3d 630 (4th Cir. 2009).

281. *Id.* at 634.

and universities, "[because] iParadigms' use of these works was completely unrelated to expressive content and was instead aimed at detecting and discouraging plagiarism."[282] Unlike Turnitin and many other applications of ML,[283] however, face surveillance is expressly related to the expressive content of profile pictures: the images primarily communicate that the named user is the person in the photograph.

3. Character

That leaves the character of the use. In the past, this would make for a simple assessment: in 1985, the Supreme Court believed that "every commercial use of copyrighted material is presumptively an unfair exploitation of the monopoly privilege that belongs to the owner of the copyright."[284] That view has softened considerably. In *Google*, the Supreme Court clarified that commercial use "is not dispositive of the first factor," particularly if the use is "inherently transformative."[285] Matthew Sag's empirical work, however, reveals that "[c]ommercial use by the defendant makes a finding of fair use less likely."[286]

Face surveillance companies' uses are indisputably commercial. In 2020, Clearview AI announced that it would end partnerships with private companies and contract exclusively with "law enforcement or some other federal, state, or local government department, office, or agency."[287] Despite losing the private portion of its business, Clearview AI contracts with more than six hundred law enforcement agencies, selling its services for tens of thousands of dollars—or more.[288] As recently as August 2020, ICE signed a contract for $224,000.[289]

Another case involving a searchable database of copyrighted works reveals that commerciality may be especially likely to weigh against a copier where there is no clear public benefit to the copying. In *Authors Guild v. Google, Inc.*,[290] the Second Circuit examined whether the Google Books search engine, which

282. *Id.* at 640.

283. Levendowski, *Copyright Law*, *supra* note 19, at 590–91.

284. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 451 (1984). This was dicta, but it nevertheless informed courts' approaches to commerciality.

285. Google LLC v. Oracle Am., Inc., 141 S. Ct. 1183, 1204 (2021).

286. Sag, *supra* note 222, at 58.

287. Ryan Mac, Caroline Haskins & Logan McDonald, *Clearview AI Has Promised To Cancel All Relationships with Private Companies*, BUZZFEED NEWS (May 7, 2020, 6:50 PM), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies [https://perma.cc/4YME-CTDP].

288. Gilbert, *supra* note 237.

289. Lyons, *supra* note 103. Even the U.S. Post Office police use facial recognition technology. Jana Winter, *Facial Recognition, Fake Identities and Digital Surveillance Tools: Inside the Post Office's Covert Internet Operations Program*, YAHOO! NEWS (May 18, 2021), https://news.yahoo.com/facial-recognition-fake-identities-and-digital-surveillance-tools-inside-the-post-offices-covert-internet-operations-program-214234762.html [https://perma.cc/T2AC-3XDT].

290. 804 F.3d 202 (2d Cir. 2015).

provides short, searchable "snippet" views of scanned books to any internet user, constituted fair use.[291] Google, like face surveillance companies, "is a profit-motivated commercial corporation."[292] Writing for a unanimous court, Judge Leval explained that "[m]embers of the public who access the Google Books website can enter search words or terms of their own choice . . . . The search engine also makes possible new forms of research, known as 'text mining' and 'data mining.'"[293] As with other transformative search engines, like Arriba Soft and Google Images, Google Books not only provides a clear public benefit, but it also does so publicly.[294]

In her qualitative analysis of fair use cases, Pamela Samuelson determined that

> copyright also promotes the public good when members of the public are able to use copyrighted materials in a way that allows them to make a range of reasonable uses that pose no meaningful likelihood of harm to the markets for protected works, and when developers of new technologies provide new opportunities for the public to make such reasonable uses.[295]

Face surveillance does no such thing. The public cannot access face surveillance databases or technologies, let alone do good with them. Researchers cannot use face surveillance technology to audit whether companies' algorithms reflect or amplify demographic biases. Civil society cannot scrutinize whether law enforcement customers deploy the technology without bias. Scholars cannot examine whether there are more privacy-protective approaches to curating face recognition databases. The limitations go on and on. Simply put, the public cannot engage in any "new forms of research."

When face surveillance services copy profile pictures and reproduce them in response to face search matches, it imbues those scraped photographs with no new expression, meaning or message. Those services share the same purpose with web users who adopt photographs of their faces as profile pictures: particularized identification. As Judge Cote concluded, commercial services may "perform an important function for their clients, [but] the public interest in the existence of such commercial enterprise does not outweigh the strong public interest in the enforcement of copyright laws."[296] However, *Google* and *TVEyes* suggest that face surveillance companies may nevertheless be somewhat transformative. This factor tilts slightly in favor of face surveillance companies.

291. *Id.* at 207.

292. *Id.* at 217.

293. *Id.* at 208–09.

294. Kelly v. Arriba Soft Corp., 336 F.3d 811, 820 (9th Cir. 2003); Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1166 (9th Cir. 2007).

295. Samuelson, *supra* note 221, at 2617.

296. Associated Press v. Meltwater U.S. Holdings, Inc., 931 F. Supp. 2d 537, 553 (S.D.N.Y. 2013).

B. *Creativity and Publication*

The second fair use factor examines "the nature of the copyrighted work."[297] Courts examine two features of a work when assessing its nature. First, recognizing that "some works are closer to the core of intended copyright protection than others, with the consequence that fair use is more difficult to establish when the former works are copied,"[298] courts "consider whether the protected writing is of the creative or instructive type that the copyright laws value and seek to foster."[299] Creative works garner greater protection against fair use than more factual ones.[300] And second, courts consider whether the work has been published, which provides greater latitude for fair use over unpublished works.[301] Until *Google*, the Supreme Court had little to say about the second factor, dedicating between one sentence and several paragraphs to its analysis in written opinions.[302]

Since *Burrow-Giles Lithographic Co. v. Sarony*,[303] courts have recognized that photographs are creative works protected by copyright law.[304] The protection of photographs is codified in the Copyright Act.[305] In cases involving copies of photographs, courts practically take for granted that photographs qualify as creative. The Ninth Circuit observed in *Arriba Soft*, for example, that Kelly's photographs of the American West were "meant to be viewed by the public for informative and aesthetic purposes [and] are creative in nature."[306] Revisiting the issue with nude photographs, the court determined that "our decision in *Kelly* is directly on point. There we held that the photographer's images were 'creative in nature.'"[307]

The calculus holds true in the Second Circuit as well. In *Rogers v. Koons*,[308] the Second Circuit determined that Art Rogers' photographic portraits of a

297. 17 U.S.C. § 107(2).

298. Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 586 (1994).

299. Leval, *supra* note 194, at 1117.

300. *See, e.g.*, *Campbell*, 510 U.S. at 586 (citing Stewart v. Abend, 495 U.S. 207, 237–38 (1990)) (contrasting fictional short story with factual works); Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 563–64 (1985) (contrasting soon-to-be-published memoir with published speech); Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 455–56 n.40 (1984) (contrasting motion pictures with news broadcasts); Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 348–51 (1991) (contrasting creative works with bare factual compilations).

301. *Harper & Row*, 471 U.S. at 564.

302. *See Sony Corp.*, 464 U.S. at 449–50 (providing one sentence); *Harper & Row*, 471 U.S. at 550–55 (writing several paragraphs, but focusing on unpublished works); *Campbell*, 510 U.S. at 586 (providing one paragraph); Google LLC v. Oracle Am., Inc., 141 S. Ct. 1183, 1201–02 (2021) (writing several paragraphs).

303. 111 U.S. 53 (1884).

304. *Id.* at 59–61 (finding copyright in photograph of Oscar Wilde).

305. *See* 17 U.S.C. § 102(5).

306. Kelly v. Arriba Soft Corp., 336 F.3d 811, 820 (9th Cir. 2003).

307. Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1167 (9th Cir. 2007).

308. 960 F.2d 301 (2d Cir. 1992).

couple holding puppies was "an original expression [that] has more in common with fiction than with works based on facts," concluding that the photograph was "creative and imaginative."[309] Years later, in *Cariou v. Prince*,[310] the court reached the same conclusion about Patrick Cariou's photographic portraits of Rastafarians with a single sentence: "[T]here is no dispute that Cariou's work is creative."[311] Recently, the court reiterated that photographs are creative works in *Warhol v. Goldsmith*,[312] agreeing with the district court that Lindsey Goldsmith's photographic portrait of Prince is "creative."[313]

Courts rarely provide lengthy analyses backing their conclusions that photographs are creative, but photographs—particularly photographic portraits—are consistently found to be so. On the other hand, profile pictures may seem a far cry from a formal portrait of Oscar Wilde. However, as the Supreme Court observed more than a century ago: "It would be a dangerous undertaking for persons trained only to the law to constitute themselves the final judges of the worth of pictorial illustrations . . . . Their very novelty would make them repulsive until the public had learned the new language in which their author spoke."[314] At the time, the Court was discussing painted advertisements rather than profile pictures, but the idea of profile pictures is no longer new—profile pictures are ubiquitous across social media, as well as personal and professional websites. Photographic portraits adopted by website users as profile pictures, including selfies, often involve specialized lighting, camera positioning, and filtering—all creative qualities, and all weighing against face surveillance companies.

In determining the nature of the work, courts also examine whether a work has been published previously. Courts are more likely to find fair use if a work has been published by the author. As the Supreme Court has noted, "[T]he author's right to control the first public appearance of [their] undisseminated expression will outweigh a claim of fair use."[315] Here, the photographs have already "appeared on the [internet]" before they were used by face surveillance companies.[316] Even where photographs are published, however, courts find that the second factor disfavors copiers' uses when the work is creative.[317] As a result,

309. *Id.* at 310.

310. 714 F.3d 694 (2d Cir. 2013).

311. *Id.* at 709.

312. Andy Warhol Found. for the Visual Arts, Inc. v. Goldsmith, 11 F.4th 26 (2d Cir. 2021).

313. *See id.* at 35–36.

314. Bleistein v. Donaldson Lithographing Co., 188 U.S. 239, 251 (1903).

315. Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 555 (1985).

316. Kelly v. Arriba Soft Corp., 336 F.3d 811, 820 (9th Cir. 2003).

317. *See, e.g.*, *Kelly*, 336 F.3d at 820 (finding use of a creative, published work "weighs only slightly in favor" of original photographer); Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1167 (9th Cir. 2007) (holding that the district court "did not err" in finding that use of a creative, published work "weighed only slightly in favor" of original publisher); Rogers v. Koons, 960 F.2d 301, 310 (2d Cir. 1992) (finding use of a creative, published work "militates against a finding of fair use"); Cariou v.

the nature of the works—published, creative photographs—weighs slightly against face surveillance companies.

C. *Amount and Substantiality*

The third factor considers "the amount and substantiality of the portion used in relation to the copyrighted work as a whole."[318] In *Google*, the Supreme Court reiterated that "even a small amount of copying may fall outside the scope of fair use where the excerpt copied consists of the 'heart' of the original work's creative expression," though that may shift where "the amount of copying [is] tethered to a valid, and transformative, purpose."[319] Barton Beebe's latest empirical assessment of fair use cases revealed that the outcome under the third factor "continues to correlate very strongly with the overall test outcome."[320]

The face depicted in a social media profile picture identifies the user *as* the user. It is the most important part of a profile picture. In *Harper & Row, Publishers, Inc. v. Nation Enterprises*,[321] the Supreme Court was confronted with the magazine equivalent of the profile picture. *The Nation* chose to excerpt key portions of President Gerald Ford's yet-unpublished memoir that reflected on his decision to pardon President Richard Nixon.[322] While the quotations were "[i]n absolute terms . . . an insubstantial portion," the Court emphasized that the article was "structured around the quoted excerpts which serve as its dramatic focal points."[323] The Court reiterated the force of *Harper & Row* in *Google*.[324] Specifically, the Court noted that

> [i]f a defendant had copied one sentence in a novel, that copying may well be insubstantial. But if that single sentence set forth one of the world's shortest short stories—"When he awoke, the dinosaur was still there."—the question looks much different, as the copied material constitutes a small part of the novel but the entire short story.[325]

The heart of a profile picture is the user's face, which identifies that individual. That key portion of the work is copied for use as training data and reproduced

Prince, 714 F.3d 694, 710 (2d Cir. 2013) (finding use of a creative, published work "weighs against a fair use determination").

318. 17 U.S.C. § 107(3).

319. Google LLC v. Oracle Am., Inc., 141 S. Ct. 1183, 1205 (2021) (first citing *Harper & Row*, 471 U.S. at 564–65; then citing Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 586–87 (1994)).

320. Beebe, *An Empirical Study Updated*, *supra* note 223, at 31.

321. 471 U.S. 539 (1985).

322. *Id.*

323. *Id.* at 565–66.

324. *See Google LLC*, 141 S. Ct. at 1205.

325. *Id.*

in response to face match searches.[326] Indeed, search results are literally "structured around" photographs of faces comprising the results.[327]

Limited information is available about the internal mechanics of face surveillance companies' use of copyrighted works as training data. It is not clear whether face surveillance companies copy entire profile pictures, excerpt users' faces, or some combination of both.[328] In any scenario, these companies ultimately put the "face" in "face surveillance" and, in so doing, take the heart of the work.

Making unauthorized copies of the "hearts" of profile pictures creates other problems, but face surveillance companies could rely only on mugshots, create their own original datasets, or combine both to avoid implicating copyright law. But doing so may be legally unnecessary. The Supreme Court explained that "[i]n principle, Google might have created its own, different system of declaring code . . . [but] the declaring code was the key that it needed to unlock the programmers' creative energies. And it needed those energies to create and improve its own innovative Android systems."[329] Like the declaring code, existing profile pictures are the "key" to unlocking effective and efficient face surveillance, and companies like Clearview AI need those "energies" to create and improve their own face surveillance systems.

The sentiment underlying the Court's analysis is not new. The Second Circuit explained in *Google Books* that "complete unchanged copying has repeatedly been found justified as fair use when the copying was reasonably appropriate to achieve the copier's transformative purpose and was done in such a manner that it did not offer a competing substitute for the original."[330] But, as discussed above, face surveillance companies have a weak "transformative purpose" claim. A return to other public search engine and private subscription services cases proves instructional. Those cases illustrate that copiers' use of works falls into three categories: (1) uses that take the entire work and display versions of it publicly, like Arriba Soft and Google Images;[331] (2) uses that take

326. *See* Smith, *I Got My File*, *supra* note 173.

327. *See id*.

328. It seems likely, however, that these companies are copying entire photographs at some stage in their algorithmic development. *See* Levendowski, *Copyright Law*, *supra* note 19, at 627.

329. *Google LLC*, 141 S. Ct. at 1205–06.

330. Authors Guild v. Google, Inc., 804 F.3d 202, 221 (2d Cir. 2015).

331. *See* Kelly v. Arriba Soft Corp., 336 F.3d 811, 821 (9th Cir. 2003) ("It was necessary for Arriba to copy the entire image to allow users to recognize the image and decide whether to pursue more information about the image or the originating web site. If Arriba only copied part of the image, it would be more difficult to identify it, thereby reducing the usefulness of the visual search engine."); Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1167–68 (9th Cir. 2007) ("Because the same analysis [as Arriba Soft] applies to Google's use of Perfect 10's image, the district court did not err in finding that this factor favored neither party.").

the entire work and display parts of it publicly, like Google Books;[332] (3) and uses that take the entire work and display parts of it to paid subscribers, like Meltwater, TVEyes, and iParadigms.[333] The former two categories consistently favor companies under this factor—but the third category does not.

In *Meltwater*, the Southern District of New York assessed that Meltwater took

> between 4.5% and 61% of the [Associated Press articles]. It automatically took the lede from every AP story. As described by AP's Standards Editor, the lede is 'meant to convey the heart of the story' . . . . There is no other single sentence from an AP story that is as consistently important from article to article . . . .[334]

Similarly, there is no more important part of a profile picture than one's face. Companies such as Clearview AI take faces—the "ledes" of profile pictures—from every profile picture. Notably, Judge Cote rejected Meltwater's argument that the "extent of its copying is justified because its purpose is to serve as a search engine," observing that the company "failed to show that it takes only that amount of material from AP's articles that is necessary for it to function as a search engine."[335] Clearview AI makes no representations suggesting that it takes just enough of profile pictures to support its purported purpose as a search engine. Indeed, there is nothing preventing the company from alternately structuring its face match results to show only confidence percentages and referral links rather than reproducing faces from profile pictures.

The Second Circuit in *TVEyes* further distinguished the amount of TVEyes' use from that of transformative search engines. There, Judge Jacobs explained that TVEyes' service was "radically dissimilar to the service at issue in Google Books," which provides publicly only small snippets of text in response to searches.[336] Instead, TVEyes "redistributes Fox's news programming in ten-minute clips, which—given the brevity of the average news segment on a particular topic—likely provide TVEyes's users with all of the Fox programming that they seek and the entirety of the message conveyed by Fox to authorized viewers of the original."[337] Analyzing the third factor, Judge Jacobs concluded that "TVEyes's use of Fox's content is therefore both

332. *Compare Authors Guild*, 804 F.3d at 221–22 ("While Google makes an unauthorized digital copy of the entire book, it does not reveal that digital copy to the public. The copy is made to enable the search functions to reveal limited, important information about the books."), *with* Authors Guild v. HathiTrust, 755 F.3d 87, 91, 99 (2d Cir. 2014) (characterizing a searchable digital library as not being a search engine).

333. *See* Associated Press v. Meltwater U.S. Holdings, Inc., 931 F. Supp. 2d 537, 558 (S.D.N.Y. 2013); Fox News Network, LLC v. TVEyes, Inc., 43 F. Supp. 3d 379, 393 (S.D.N.Y. 2014).

334. *See Associated Press*, 931 F. Supp. 2d at 558.

335. *Id.* at 559.

336. Fox News Network, LLC v. TVEyes, Inc., 883 F.3d 169, 179 (2d Cir. 2018).

337. *Id.*

'extensive' and inclusive of all that is 'important' from the copyrighted work."[338] Profile pictures are not as substantial as reproducing all programming by a single provider, but users' faces comprise the most important part of profile pictures. By copying and displaying that portion of users' photographs, companies such as Clearview AI "likely provide" their law enforcement subscribers with "all of the [faces] that they seek and the entirety of the message" conveyed by social media users who selected the images, that message being, "We are the people in these photographs."[339] Accordingly, this factor weighs heavily against face surveillance companies.

D. *Market Harms*

The fourth fair use factor analyzes "the effect of the use upon the potential market for or value of the copyrighted work."[340] In *Sony Corp. v. Universal Studios*,[341] the Supreme Court noted that "[w]hat is necessary is a showing by a preponderance of the evidence that *some* meaningful likelihood of future harm exists. If the intended use is for commercial gain, that likelihood may be presumed."[342] Years later, the Supreme Court developed the phrase "market harm" as a shorthand for the final fair use factor.[343] In *Acuff-Rose*,[344] the Court stated that the factor

> requires courts to consider not only the extent of the market harm caused by the particular actions of the alleged infringer, but also 'whether unrestricted and widespread conduct of the sort engaged in by the defendant . . . would result in a substantially adverse impact on the potential market' for the original.[345]

The Court further advised that "[t]he market for potential derivative uses includes only those that creators of original works would in general develop or license others to develop."[346] While the Supreme Court has walked back its decades-old dictum stating that the fourth factor was "undoubtedly the single

338. *Id.*

339. *Id.*

340. 17 U.S.C. § 107(4).

341. Sony Corp. of Am. v. Universal Studios, Inc., 464 U.S. 417 (1984).

342. *Id.* at 451 (emphasis in original). The Supreme Court has since moved away from the presumption that commercial use causes harm.

343. *See* Dave Fagundes, *Market Harm, Market Help, and Fair Use*, 17 STAN. TECH. L. REV. 359, 365–66 (2014). Thanks to Dan Bateyko for this insight.

344. 510 U.S. 569 (1994).

345. *Id.* at 590 (quoting 4 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 13.05[A][4] (2022)).

346. *Id.* at 592.

most important element of fair use,"[347] Barton Beebe's empirical work reveals that the factor continues to dominate courts' analyses.[348]

In *Google*, the Court expressed skepticism at claims that Oracle could have competed in Google's Android market.[349] But the licensing market for profile pictures is not so speculative; it is robust and well-established. Many web users spend considerable energy curating their online presence, which includes choosing photographs to operate as profile pictures on social media networks and professional websites. Those pictures are particularly valuable to social media networks, media outlets, and company websites.[350] All five of the social media companies that sent cease-and-desist letters to Clearview AI take nonexclusive licenses in users' copyrighted works, including profile pictures.[351] Some companies, such as Facebook, even used their social network to acquire licenses to users' photographs to train their own face recognition algorithms.[352]

Despite the flaws of "terms of service" as readable contracts,[353] users can choose whether to license their profile pictures in exchange for access to friends'

347. *Compare* Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 566 (1985) (describing how the "effect of the use upon the potential market for or value of the copyrighted work . . . is undoubtedly the single most important element of fair use"), *with Campbell*, 510 U.S. at 578 ("All [factors] are to be explored, and the results weighed together, in light of the purposes of copyright.").

348. Barton Beebe's empirical work suggests that "factor four has remained the single dominant factor in courts' adjudication of the fair use defense." Beebe, *An Empirical Study Updated*, *supra* note 223, at 4.

349. *See* Google LLC v. Oracle Am., Inc., 141 S. Ct. 1183, 1217 (2021).

350. *See, e.g.*, Edgar Gómez & Elisenda Ardévol, *Playful Embodiment: Body and Identity Performance on the Internet*, 26 QUADERNS 41, 42 (2010) (discussing self-presentation on the internet as a form of self-expression and opportunity to play with performance of one's identity); Jiao Huant, Sameer Kumar & Chuan Hu, *A Literature Review of Online Identity Reconstruction*, 12 FRONTIERS PSYCH., Aug. 2021, at 1, 1 (reviewing scholarship centered on how online self-presentation, including profile pictures, contribute to constructing identity).

351. *See Terms of Service*, FACEBOOK, https://www.facebook.com/legal/terms [https://perma.cc/N9C4-S49J]; *Terms of Service*, YOUTUBE, https://www.youtube.com/static?template=terms [https://perma.cc/CC4A-3X4S]; *User Agreement*, LINKEDIN, https://www.linkedin.com/legal/user-agreement [https://perma.cc/HS2T-NZWQ]; *User Agreement*, VENMO, https://venmo.com/legal/us-user-agreement/ [https://perma.cc/7DHH-UJL9]; *Twitter Terms of Service*, TWITTER, https://twitter.com/en/tos [https://perma.cc/59PT-V4JG].

352. *See, e.g.*, Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato & Lior Wolf, *DeepFace: Closing the Gap to Human-Level Performance in Face Verification*, 2014 IEEE CONF. ON COMPUTER VISION & PATTERN RECOGNITION 1, 5 (explaining that Facebook's "DeepFace" AI achieved facial verification accuracy of 97.35% identification by training on "a large collection of photos from Facebook"). In prior works, I have referred to this approach as the "build-it" model for acquiring training data for AI systems. *See* Levendowski, *Copyright Law*, *supra* note 19, at 606.

353. *See* Jonathan A. Obar & Anne Oeldorf-Hirsch, The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services 2, 14, 16 (June 2018) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465 [https://perma.cc/CBG4-XAFX] (including that in one study, seventy-four percent of participants skipped reading a privacy policy with a "quick join" clickwrap and eighty-six percent of participants spent less than a minute reading terms of service that researchers determined took more than fifteen minutes to read).

and followers' (and even strangers') status updates and selfies. Face surveillance companies circumvent that market, making unauthorized decisions for other networks' users and offering nothing of value in return for their takings. Yet, at the same time, these companies profit handsomely from selling such ill-gotten photographs to private subscribers in law enforcement.[354]

Licensing markets play a decisive role in subscription service cases in ways that pose problems for face surveillance companies. Concluding that the fourth factor "weighs strongly against Meltwater," the Southern District for New York explained that the Associated Press put effort into developing an online presence, including licensing its content to competitors of Meltwater.[355] Judge Cote proceeded to observe that Meltwater's unlicensed use of Associated Press stories "cheapen[ed] the value of AP's work by competing with companies that *do*" license AP content.[356] She concluded that using the Associated Press's content without a license created an "unfair commercial advantage in the marketplace and directly harmed the creator of expressive content protected by the Copyright Act."[357] The Second Circuit in *TVEyes* similarly noted that "[t]he success of the TVEyes business model demonstrates that deep-pocketed consumers are willing to pay well for a service that allows them to search for and view selected television clips, and that this market is worth millions of dollars in the aggregate."[358] "[B]y selling access to Fox's audiovisual content without a license," Judge Jacobs concluded, "TVEyes deprives Fox of revenues to which Fox is entitled as the copyright holder."[359]

But the Supreme Court in *Google* cautioned that "a potential loss of revenue is not the whole story."[360] The Court acknowledged in *Sony* that

> copyright law does not require a copyright owner to charge a fee for the use of his works, and . . . the owner of a copyright may well have economic or noneconomic reasons for permitting certain kinds of

354. In the context of so-called "utility-expanding fair uses," which likely encompass many other applications of ML beyond face surveillance, scholars have called for variations on compulsory licenses where licensing would be otherwise impracticable. *See, e.g.*, Jacob Victor, *Utility-Expanding Fair Use*, 105 MINN. L. REV. 1887, 1921 (2021). Face surveillance, however, seems positioned to afford licenses: Amid its legal troubles, Clearview AI has raised $30 million dollars at a $130 million valuation. Its Israeli competitor, AnyVision, raised $235 million in a single month. Kashmir Hill, *Clearview AI Raises $30 Million from Investors Despite Legal Troubles*, N.Y. TIMES, https://www.nytimes.com/2021/07/21/technology/clearview-ai-valuation.html [https://perma.cc/PM4F-QHF8 (dark archive)] (Oct. 28, 2021).

355. Associated Press v. Meltwater U.S. Holdings, Inc., 931 F. Supp. 2d 537, 560–61 (S.D.N.Y. 2013).

356. *Id.* at 561 (emphasis in original).

357. *Id.*

358. Fox News Network, LLC v. TVEyes, Inc., 883 F.3d 169, 180 (2d Cir. 2018).

359. *Id.*

360. Google LLC v. Oracle Am., Inc., 141 S. Ct. 1183, 1206 (2021).

> copying to occur without receiving direct compensation from the copier.[361]

Jane Ginsburg, drawing from decisions of multiple courts, determined that valuation under the fourth factor "need not be monetary."[362]

The profile picture licensing market presents a conundrum. Licensing is not, and should not be, necessary for every secondary use—particularly for many uses by artists, libraries, reporters, and educators—yet it seems important for uses in commercial face surveillance technology.[363] Face surveillance engages with the emerging market for an individual's privacy, which people license away for no fee. But face surveillance companies do deprive users of the right to choose whether and to whom to license their works. There is a striking similarity between the Second Circuit's observation in *TVEyes* that "deep-pocketed consumers are willing to pay well" for subscription services that serve up unlicensed copies and the business model of face surveillance companies.[364] A just exchange for use of the profile pictures for face surveillance hinges on consent, not compensation. This is tricky to value under the final factor—or within copyright at all.

As discussed under the first factor previously, the Court in *Google* stated that, as part of the fourth factor, "we must take into account the public benefits the copying will likely produce . . . . Are they comparatively important or unimportant, when compared with dollar amounts likely lost . . . ?"[365] It remains

361. Sony Corp. of Am. v. Universal City Studios, 464 U.S. 417, 447 n.28 (1984).

362. Jane C. Ginsburg, *Fair Use Factor Four Revisited: Valuing the "Value of the Copyrighted Work*," 67 J. COPYRIGHT SOC'Y U.S.A. 19, 30 (2020) (citing Soc'y of Holy Transfiguration Monastery, Inc. v. Gregory, 689 F.3d 29, 64 (1st Cir. 2012)); *see also* Worldwide Church of God v. Phila. Church of God, Inc., 227 F.3d 1110, 1119 (9th Cir. 2000) ("Those rewards [from noncommercial copying] need not be limited to monetary rewards; compensation may take a variety of forms."); Chi. Sch. Reform Bd. of Trs. v. Substance, Inc., 79 F. Supp. 2d 919, 933–34 (N.D. Ill. 2000), *aff'd in part, vacated in part sub nom.* Chi. Bd. of Educ. v. Substance, Inc., 354 F.3d 624, 632 (7th Cir. 2003) ("Defendants' publication of the tests significantly decreased that value, and the court need not determine at this time the monetary damage Defendants caused. The court finds no difference between a copyright holder losing future profits because of a copyright infringement and the Board losing its future educational value of its copyrighted work."); *Gregory*, 689 F.3d at 64 ("[T]he fourth factor of the fair use inquiry cannot be reduced to strictly monetary terms."); Video Pipeline, Inc. v. Buena Vista Home Ent., Inc., 342 F.3d 191, 202 (3d Cir. 2003) ("The statute directs us to consider 'the effect of the use upon the . . . *value* of the copyrighted work,' not only the effect upon the 'market,' however narrowly that term is defined. And the value 'need not be limited to monetary rewards; compensation may take a variety of forms.'" (emphasis in original) (first quoting 17 U.S.C. § 107(4); then quoting *Worldwide Church of God*, 227 F.3d at 1119)), *abrogated by* TD Bank N.A. v. Hill, 928 F.3d 259, 278 (3d Cir. 2019).

363. *See* 17 U.S.C. § 107 ("Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright.").

364. *TVEyes*, 883 F.3d at 180.

365. *Google LLC*, 141 S. Ct. at 1206.

unclear how a court would weigh the comparative importance of identifying some alleged criminals against the fundamental destruction of privacy. To tilt against face surveillance companies, a court would need to credit the idea that a market is not exclusively measured by money—which is not impossible. But that finding may be colored by how the court characterizes the benefits (and harms) of face surveillance.

It is also worth noting that the approach currently taken by face surveillance companies is quickly falling out of favor.[366] Not only do many companies acquire licenses to use profile pictures, but face recognition training datasets reliant on scraped photographs are also being phased out in favor of images obtained with consent. Multiple academic institutions, including Stanford[367] and the University of Washington,[368] took hallmark public datasets, all comprised of images used without consent, offline. Microsoft, formerly a leader in face recognition before issuing its corporate moratoria, decommissioned its popular MS Celeb dataset comprised of nearly 100,000 individuals featured in ten million scraped photographs.[369] And the Conference on Neural Information Processing Systems, a prestigious ML conference better known as NeurIPS, recently proposed that its reviewers will account for whether "people provide[d] their consent on the collection of such data" when assessing submitted research.[370]

Licensing each work used as ML training data is often legally unnecessary,[371] but custom is changing for face recognition. This shift spells further trouble for face recognition companies under the fourth factor. As Jennifer Rothman observes, "courts often rely on custom as a proxy in making other inquiries, such as determining the market effects of using another's IP."[372] If this trend continues, a "plausibly exploitable market" may emerge for licensing photographs to train face recognition algorithms, further disfavoring face surveillance companies.[373]

366. RAJI & FRIED, *supra* note 180, at 8.

367. *See* Russell Stewart, *Brainwash Dataset*, STAN. DIGIT. REPOSITORY (2015), https://purl.stanford.edu/sx925dc9385 [https://perma.cc/MDG5-8G5S].

368. *MegaFace and MF2: Million Scale Face Recognition*, UNIV. WASH., http://megaface.cs.washington.edu/ [https://perma.cc/DUS2-7DEN].

369. Madhumita Murgia, *Microsoft Quietly Deletes Largest Public Face Recognition Data Set*, FIN. TIMES (June 6, 2019), https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2 [https://perma.cc/7J8Q-JLKD (dark archive)]. The images were shared under Creative Commons licenses. *Id.*

370. *Ethics Guidelines*, NEURIPS 2021 (2022), https://neurips.cc/public/EthicsGuidelines [https://perma.cc/LHW6-SXRC]. I consulted on the development of the Ethics Guidelines as an advisor to the Research Ethics Committee.

371. *See* Levendowski, *Copyright Law*, *supra* note 19, at 629; Lemley & Casey, *supra* note 26, at 759.

372. Jennifer E. Rothman, *The Questionable Use of Custom in Intellectual Property*, 93 VA. L. REV. 1899, 1906 (2007).

373. *See* Fox News Network, LLC v. TVEyes, Inc., 883 F.3d 169, 180 (2d Cir. 2018). A plausibility framing is both novel and singular among fair use analyses, but subsequent Second Circuit cases have

CONCLUSION

In *Acuff-Rose*, the Supreme Court explained that "the four statutory factors [cannot] be treated in isolation, one from another. All are to be explored, and the results weighed together, in light of the purposes of copyright."[374] Promoting public access to knowledge remains a principal purpose of copyright law.[375] But face surveillance companies' secretive sales of subscription services to law enforcement do not promote public access to knowledge—quite the contrary. Taken together, the fair use factors *could* weigh against companies' copying and reproduction of web users' copyrightable profile pictures for face surveillance.

Even so, copyright law remains no one's first choice for resisting face surveillance. Copyright can permit, and even perpetuate, biases that animate invasive face recognition.[376] It protects against profile pictures being copied by face surveillance companies, but not against wedding pictures and vacation photos being used to fuel face surveillance. It also requires some knowledge of face surveillance datasets to effectively litigate.[377] But the alternatives, barring a ban, are no less limiting. Jeanne Fromer has asked whether we should care about the reasons why copyright is being invoked.[378] We should care deeply when copyright is weaponized for censorship or harassment.[379] But face surveillance is actively harming marginalized communities, and the remaining public is unlikely to fare much better. Perhaps the more urgent question is whether the assertion of copyright can effectively do good. Here, the answer is yes.

The Venn diagram of modern technological copyright challenges and privacy puzzles continues to more closely resemble a circle, at the center of which sit three fundamental questions: who must give consent, to whom, and for what purposes. We must also grapple with the reality that decades of lobbying created an environment in which existing copyright law does a better

not walked it back. *See, e.g.*, Andy Warhol Found. for the Visual Arts, Inc. v. Goldsmith, 11 F.4th 26, 49 (2d Cir. 2021) (citing *TVEyes* without rejecting its plausibility framing).

374. Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 578 (1994).

375. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 429 (1984).

376. *See* Levendowski, *Copyright Law*, *supra* note 19, at 630.

377. This information is not impossible to uncover. Clearview AI offers a portal for Californians to request their photographs, which is how journalists Thomas Smith and Anna Merlan acquired their face search results. *See CCPA Data Access Form*, CLEARVIEW.AI, https://clearviewai.typeform.com/to/wDa2sO [https://perma.cc/N4NA-6ZWW (staff-uploaded archive)].

378. Fromer, *supra* note 24, at 549.

379. *See, e.g.*, Smith, *Weaponizing Copyright*, *supra* note 31, at 68 ("Advocating for copyright to be weaponized to protect privacy interests might serve victims of nonconsensual pornography and victims of other forms of forced disclosure of private information, and allow them to control the removal or dissemination of their personal content or images. However, it could also open the door for copyright owners to claim protection of privacy interests when their ultimate goal is to suppress unwelcome speech and silence and erase basic information and facts.").

job of protecting the public against privacy harms than many alternatives.[380] As it stands, copyright remains a powerful means of preventing invasive face surveillance technology from dismantling privacy.

Make no mistake, the use of face recognition technology by law enforcement should be banned. In the meantime, researchers must continue interrogating which uses of face recognition technology recalibrate power and promote justice rather than settling for ones that are legally defensible. Lawyers must continue thinking creatively about holding face surveillance companies legally accountable.[381] And activists must continue pressing politicians to pass local oversight regulations. David Scalzo, one of Clearview AI's early investors, speculated that "[l]aws have to determine what's legal, but you can't ban technology. Sure, that might lead to a dystopian future or something, but you can't ban it."[382] So far, he has been largely correct. But if we invoke existing copyright law to protect the public from face surveillance, we may buy ourselves enough time to wait for the federal ban we need.

380. *See, e.g.*, Hauser, *supra* note 27 (awarding $450,000 for copyright infringement).

381. *See, e.g.*, Vermont Clearview AI Complaint, *supra* note 25, at 1 (alleging violation of UDAP law); Renderos Complaint, *supra* note 25, at 1 (alleging violation of invasion of likeness law).

382. Hill, *The Secretive Company*, *supra* note 8.