THE END OF ANONYMITY – HOW FACIAL RECOGNITION TECHNOLOGY WILL WORSEN ONLINE HARASSMENT

COURTNEY HINKLE*

In January 2020, the New York Times published a bombshell report detailing how a little-known company, Clearview AI, had quietly developed facial-recognition software to help law enforcement agencies match photos of unknown persons with their online images.[1] The company allows photos to be uploaded and cross-referenced with a massive database of more than 3 billion images scraped from Facebook, YouTube, Venmo, and millions of other websites. The revelations immediately sparked public outcry from lawmakers, tech companies, as well as the privacy and civil rights activists. Google, Twitter, LinkedIn, Venmo, YouTube, and Facebook all sent cease-and-desist letters.[2] Apple blocked the company's iPhone app for violating its terms of its enterprise developer program.[3] And the company has been widely panned for its failure, or indifference to, the potentially dangerous and unethical uses of its technology.[4]

The debate over the use of facial recognition technology has reached a fever pitch in recent months with many activists and scholars calling for lawmakers to impose a complete ban on the technology.[5] In the U.S., their engagement has achieved a modicum of success at the local level; for example, San Francisco, Somerville (a Boston suburb), and Oakland have banned government use of the technology.[6] In Europe, lawmakers were briefly considering a five-year moratorium on the technology in public spaces,[7] but the idea was walked-back in favor of a non-binding commitment that encourages extra-testing and human oversight.[8] Of course, the use of facial recognition technologies for mass surveillance is widespread in authoritarian regimes, most notably China.[9]

---

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

[2] *Google, YouTube, Venmo and LinkedIn send cease-and-desist letters to facial recognition app that helps law enforcement*, CBS NEWS (last updated: Feb. 5, 2020, 6:25 AM), https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/.

[3] Zack Whittaker, *Apple has blocked Clearview AI's iPhone app for violating its rules*, TECHCRUNCH (Feb. 28, 2020, 3:11 PM), https://techcrunch.com/2020/02/28/apple-ban-clearview-iphone/.

[4] Kashmir Hill, *Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos*, N.Y. TIMES (Jan. 20, 2020), https://www.nytimes.com/2020/01/22/technology/clearview-ai-twitter-letter.html.

[5] Davey Alba, *Privacy And Civil Rights Groups Ask The US Government To End Its Use Of Facial Recognition Tech On The Public*, BUZZFEED NEWS (last updated: July 9, 2019, 6:11 PM), https://www.buzzfeednews.com/article/daveyalba/campaign-against-facial-recognition-house-homeland-security; Sigal Samuel, *Activists want Congress to ban facial recognition. So they scanned lawmakers' faces*, VOX (Nov. 15, 2019, 10:10 AM), https://www.vox.com/future-perfect/2019/11/15/20965325/facial-recognition-ban-congress-activism.

[6] Blake Montgomery, *Facial Recognition Bans: Coming Soon to a City Near You*, THE DAILY BEAST (July 31, 2019, 2:47 PM, https://www.thedailybeast.com/facial-recognition-bans-coming-soon-to-a-city-near-you.

[7] Foo Yun Chee, *EU Drops Idea of Facial Recognition Ban in Public Areas*, REUTERS (Jan. 29, 2020, 6:09 PM), https://www.reuters.com/article/us-eu-ai/eu-drops-idea-of-facial-recognition-ban-in-public-areas-paper-idUSKBN1ZS37Q.

[8] Amrita Khalid, *The EU's agenda to regulate AI does little to rein in facial recognition*, QUARTZ (Feb. 20, 2020), https://qz.com/1805847/facial-recognition-ban-left-out-of-the-eus-agenda-to-regulate-ai/

[9] Lily Kuo, *China Brings In Mandatory Facial Recognition for Mobile Phone Users*, THE GUARDIAN (Dec. 2, 2019, 12:55 AM), https://www.theguardian.com/world/2019/dec/02/china-brings-in-mandatory-facial-recognition-for-mobile-phone-users.

The revelations about Clearview have only increased pressure on lawmakers to address the use of the technology, which currently is unregulated at the federal level.[10] The power of Clearview's technology raise serious privacy and ethical concerns; in particular, the technology poses a grave threat to stalking victims and survivors of gender-based violence. With this tool, anyone could snap a photo of you on the street, and quickly find out your name, address, phone number, social media profile, place of employment, and more.[11] The disproportionate impact of online abuse directed at women and sexual minorities, particularly persons of color, is well-known.[12] Even without this tool, sophisticated online actors have inflicted hell on thousands of individuals through online harassment campaigns, including "swatting" or "doxing."[13]

But this tool—if made public and in the hands of the wrong person—elevates the threat to new levels. For example, consider this troubling but realistic scenario: a man meets a woman at a bar, or in-line at her local coffee shop. They exchange pleasantries for a few minutes. The man asks for her number; she declines (not interested). Infuriated by the rejection, the man takes a photo of the woman. He then uses the same technology developed by Clearview to find out her name, her address. He finds her social media profile. What is to stop him from waging a relentless campaign of harassment, or doxing her, or stalking and killing her?[14] Whereas before there might have been a boundary between the digital and real world for those wishing to avoid recognition, or the comfort of being able to disappear into anonymity, this technology may forecloses that possibility.

To be clear, Clearview has publicly rejected the idea that its product will become available to the public, and stated the company "exists to help law enforcement agencies solve the toughest cases and our technology comes with strict guidelines and safeguards to ensure investigators use it for its intended purpose only." Further emphasizing this point, the company stated in a blog that "while many people have advised us that a public version would be more profitable, we have rejected the idea."[15]

However, in a series of emails exchanged with a police department in Green Bay, Wisconsin, company representatives were encouraging individual officers to test the technology on themselves and their acquaintances.[16] The company representative boasted a Clearview account provided "unlimited searches," and encouraged the officer to "tak[e] a selfie" in order to "see the power in real time."
This exchange exposed the inconsistencies between the company's claims that the tool be used strictly for legitimate law enforcement purposes and in adherence with strict use policies, and its private encouragement to would-be customers that the tool be used on family and friends. Moreover, hackers recently infiltrated the company's client list, revealing partnerships that extend beyond law enforcement

---

[10] Mark Sullivan, *Privacy Groups Want A Federal Facial-Recognition Ban, But It's A Long Shot*, FAST COMPANY (Jan. 28, 2020), https://www.fastcompany.com/90456414/privacy-groups-want-a-national-facial-recognition-ban-but-its-a-longshot.
[11] Maya Shwayder, *Clearview AI's facial-recognition app is a nightmare for stalking victims*, DIGITAL TRENDS (Jan. 22, 2020), https://www.digitaltrends.com/news/clearview-ai-facial-recognition-domestic-violence-stalking/.
[12] *See* DANIELLE K. CITRON, HATE CRIMES IN CYBER SPACE (Harvard Univ. Press, 2014).
[13] *See id.*; *see also,* CARRIE GOLDBERG, NOBODY'S VICTIM: FIGHTING PSYCHOS, STALKERS, PERVS, AND TROLLS (Plume, 2019).
[14] Jessica Mason, *The App That Lets People Search You via Your Face is Real and Terrifying*, THE MARY SUE (Jan. 21, 2020, 3:48 PM), https://www.themarysue.com/clearview-ai-facial-recognition-app-terrifying/.
[15] *Clearview Is Not a Consumer Application*, CLEARVIEW AI (Jan. 23, 2020), https://blog.clearview.ai/post/2020-01-23-clearview-is-not-public/.
[16] Ryan Mac, Caroline Haskins, & Logan McDonald, *Clearview AI Once Told Cops To "Run Wild" With Its Facial Recognition Tool. It's Now Facing Legal Challenges*, BUZZFEED NEWS (Jan. 28, 2020, 3:34 PM), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-cops-run-wild-facial-recognition-lawsuits.

agencies as previously disclosed, including retailers Best Buy and Macy's, and a sovereign wealth fun in the United Arab Emirates.[17]

The risk of this type of improper use has repeatedly been raised by civil rights activists, who have expressed concerns about bad apples within law enforcement agencies who with access to such tools, particularly facial recognition technology, could use them for personal, nefarious purposes. This concern is not unfounded: studies have shown women in around forty-percent of law enforcement families experience domestic violence.[18] And many experts also believe this number is likely underinclusive.[19]

But even if it is not Clearview's program that is being used, that the capability for such a program already exists means it is only a matter of time before a more unscrupulous company sprouts up and provides unfettered access to the program, regardless of intended use or concern for privacy safeguards. This is why self-governance models should be treated with the utmost skepticism. We need strong policies in place to regulate the proper uses of such technology, or perhaps, the technology should be banned entirely given the serious threat to individual liberty and privacy.

In addition to city-wide bans on the technology, some states have adopted strict regulations on the collection of biometric data, which would cover facial recognition technology. For example, in 2008, Illinois passed the strongest biometric data protection law in the country, the Biometric Information Privacy Act (BIPA); the law has already been used to enforce meaningful oversight for companies collecting this data. Facebook recently agreed to pay $55 million to settle a class action lawsuit over the use of its facial-recognition technology to collect users' biometric face information without notice or consent. The lawsuit alleged the company's photo-labeling service, Tag Suggestions, deployed face-matching software to suggest the names of persons in users' photos.[20] The settlement came after the Supreme Court recently denied Facebook's appeal to review the Northern District of California's class certification decision.[21]

This favorable outcome for plaintiffs further proves the need for a robust federal privacy law.[22] Experts have credited BIPA's private right of enforcement provision and statutory fine of $5,000 per violation as providing effective tools for individuals to assert their privacy rights.[23] However, merely obtaining consent—even if a more robust understanding of "consent"—may prove inadequate given the significant power imbalance between every day consumers and the companies profiting off a massive data industrial

---

[17] 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 (last updated: Feb. 27, 2020, 11:37 PM), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.
[18] Rafaqat Cheema, *Black and Blue Bloods: Protecting Police Officer Families from Domestic Violence*, 54 FAM. CT. REV. 487, 489 (2016).
[19] Leigh Goodmark, *Hands Up at Home: Militarized Masculinity and Police Officers Who Commit Intimate Partner Abuse*, 2015 B.Y.U. L. REV. 1183, 1195 (2015) (quoting Peter H. Neidig et al., *Interspousal Aggression in Law Enforcement Families: A Preliminary Investigation*, 15 POLICE STUD. INT'L REV. POLICE DEV. 30, 31 (1992)).
[20] Patel v. Facebook, Inc., No. 18-15982 (9th Cir. 2019) (order granting class certification).
[21] Emily Birnbaum, *Supreme Court Declines to Hear Facebook Facial Recognition Case*, THE HILL (Jan. 21, 2020, 10:55 AM), https://thehill.com/policy/technology/479126-supreme-court-declines-to-hear-facebook-facial-recognition-case.
[22] Jamie Williams, *Clearview's Face Surveillance Shows Why We Need a Strong Federal Consumer Privacy Law*, ELECTRONIC FRONTIER FOUNDATION (Jan. 27, 2020), https://www.eff.org/deeplinks/2020/01/clearviews-face-surveillance-shows-why-we-need-strong-federal-consumer-privacy-law.
[23] *Id.*

complex, as well as the fundamental threat many believe the technology poses to our "delicate social fabric."[24]

Both approaches should be contemplated by legislators, and a robust debate over the merits of procedural safeguards as compared to a complete ban is warranted. However, what is untenable is inaction. Such a policy failure would leave vulnerable populations exposed to increasing levels of exploitation and harm – both online and offline.

[24] *See* Woodrow Hartzog, *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.