UNCOVERED: FACIAL RECOGNITION AND A SYSTEMIC EFFECTS APPROACH TO FIRST AMENDMENT COVERAGE

Lucas Evans[*]

CITE AS: 6 GEO. L. TECH. REV. __ (2022)

TABLE OF CONTENTS

I. INTRODUCTION

As governments and private companies alike increasingly invest in surveillance tools such as facial recognition technology (FRT), the specter of a much more pervasive surveillance state looms. Clearview AI—a startup that scrapes publicly available photos on the Internet and sells a facial recognition search engine to law enforcement—has in turn faced numerous lawsuits alleging violations of privacy laws. The company has responded that those privacy laws are unconstitutional as applied to its FRT computer application

[*] Director of Technology and Solicitations Editor, Georgetown Law Technology Review; Georgetown Law, J.D. expected 2022; Belmont University, B.B.A. 2019. Thank you to Professor Julie Cohen for providing guidance and support in the paper's early stages. Thank you also to the GLTR staff, whose insightful edits were critical to making this piece fit for publication.

because its information processing activities are protected First Amendment speech. Although that defense has been unsuccessful so far, a new, important question has arisen: is the activity of measuring a person's facial biometrics protected speech under the First Amendment? Stated differently, should courts apply constitutional scrutiny to laws that seek to regulate the collection and use of biometric information? The debate comes at an inflection point. While law enforcement adopts these technologies at scale, states are increasingly regulating FRT and there is momentum to do the same at the federal level.

This Note contends that, as applied to FRT in the police context, laws regulating the collection and use of facial biometric information do not raise First Amendment concerns because First Amendment coverage does not extend to facial measurement in service of police surveillance. Using Clearview AI as a case study and building upon the literature pertaining to First Amendment coverage, this Note argues that "faceprinting" of the sort Clearview engages in is not protected First Amendment activity because it is anathema to core First Amendment values and undermines the population's ability to engage in free expression and association.

Part II tees up the FRT debate and recounts the story of Clearview AI. It details the company's First Amendment defense to alleged biometric privacy law violations and situates that defense in the broader context of conversations around First Amendment *Lochner*ism. Part III builds upon existing scholarship by offering an updated First Amendment coverage framework that accounts for the systemic effects of the activity in question. Scholars have illustrated that the traditional test employed by the Supreme Court for assessing whether a given activity is protected speech is flawed because it fails to recognize that courts make normative judgments about social context and the core purposes served by the First Amendment when determining whether coverage extends. In light of this, Part III argues that courts should consider the potential systemic effects of a given activity and whether they relate to recognized First Amendment values such as deliberative democracy and individual autonomy.

Applying this framework, Part IV argues that the regulation of Clearview's faceprinting in service of government surveillance does not trigger First Amendment concerns. Rather, its technology undermines the public's capacity to remain anonymous when engaging in political speech and could lead to pervasive chilling effects. Therefore, Clearview has a weak claim to First Amendment protection.

II. BACKGROUND

The information economy has increasingly become characterized by the monitoring and manipulation of human behavior.[1] While large private sector platforms have engendered part of this shift, the last twenty years have also seen a phase shift towards public and private partnerships dedicated to equipping governments with surveillance technologies.[2] Key components in these architectures are biometric technologies, such as fingerprints or iris scans, which measure distinctive physical characteristics of individuals.[3] One particularly powerful form of biometrics is face recognition.

There are two main use cases for FRT: verification and identification.[4] On one hand, FRT can increase security in *verification* of identity.[5] Whereas keycards can be lost, and passwords forgotten, biometrics are "something you are," which cannot be lost or stolen.[6] For instance, airports have begun to use face scans to identify passengers.[7] Smartphones have also applied FRT by scanning the owner's face to unlock.[8]

[1] *See generally* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 197–328 (2019).

[2] *See generally* Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. 19 (2017) (taking account of widespread police procurement of body cameras, location trackers, and big-data analytics software); *NSA Timeline 1791–2015*, ELEC. FRONTIER FOUND., https://www.eff.org/nsa-spying/timeline (last visited Nov. 17, 2021) (detailing the history of the National Security Agency's bulk telephone metadata collection program) [https://perma.cc/9YCH-AMJW]; Antoaneta Roussi, *Resisting the Rise of Facial Recognition*, NATURE (Nov. 18, 2020), https://www.nature.com/articles/d41586-020-03188-2 (describing how cities around the world have installed thousands of cameras in discrete locations in the name of increasing security and enabling data-driven "smart cities") [https://perma.cc/94AQ-A55D]; Lily Hay Newman, *How Baltimore Became America's Laboratory for Spy Tech*, WIRED (Sept. 4, 2016), https://www.wired.com/2016/09/baltimore-became-americas-testbed-surveillance-tech/ (detailing police use of aerial surveillance devices and Stingrays, which track subjects using cell-site location data) [https://perma.cc/G7BK-TLZK].

[3] *See* John D. Woodward, Jr., Christopher Horn, Julius Gatune & Aryn Thomas, RAND PUB. SAFETY AND JUST., *Biometrics: A Look at Facial Recognition* 1 (2003) [hereinafter RAND Report].

[4] GOV'T ACCOUNTABILITY OFF., *Facial Recognition: Current and Planned Uses by Federal Agencies* 4 (2021) [hereinafter GAO Report].

[5] *See* Natasha Singer, *Never Forgetting a Face*, N.Y. TIMES (May 17, 2014), https://www.nytimes.com/2014/05/18/technology/never-forgetting-a-face.html [https://perma.cc/LY86-4NEC].

[6] *See* RAND Report, *supra* note 3, at 6.

[7] Lori Aratani, *Officials Unveil New Facial Recognition System at Dulles International Airport*, WASH. POST (Sept. 7, 2018), https://www.washingtonpost.com/transportation/2018/09/06/officials-unveil-new-facial-recognition-system-dulles-international-airport/ [https://perma.cc/PL9E-A3GD].

[8] GAO Report, *supra* note 4, at 4.

Likewise, FRT systems in the *identification* category are often used to identify unknown criminal suspects, either after-the-fact or in real-time. These FRT algorithms generally assign unique values to measurements of faces—renderings of facial geometry often called "faceprints."[9] They typically employ neural networks to derive "similarity scores" for images uploaded by a user.[10] If a score meets a certain threshold, the tool indicates a match between a photo in the database and the one uploaded.[11] Companies like Clearview have touted it as an effective tool with which to fight human trafficking[12] and protect schools from mass shootings.[13]

Today face recognition is controversial on multiple levels. First, some technologies have been plagued by accuracy problems.[14] One study found that error rates of Microsoft's, IBM's, and Face++'s FRT systems for darker-skinned females reached 34.7%, compared to 0.8% for lighter-skinned males.[15] A potential reason is that data used to train an FRT algorithm may differ significantly from data captured in the wild.[16] For example, in 2020, a Detroit man was wrongfully arrested in front of his family and detained by police for a robbery he did not commit.[17] Police had uploaded a "grainy"

[9] *See* Singer, *supra* note 5.

[10] Patrick Grother, Mei Ngan & Kayee Hanaoka, NAT'L INST. OF STANDARDS AND TECH., FACE RECOGNITION VENDOR TEST, PART 3: DEMOGRAPHIC EFFECTS (2019), https://doi.org/10.6028/NIST.IR.8280 [hereinafter NIST Demographic Study].

[11] *Id.*

[12] Lisa Lacy, *This Startup is Using Facial Recognition to Fight Human Trafficking*, ADWEEK (May 31, 2018), https://www.adweek.com/performance-marketing/this-startup-is-using-facial-recognition-to-fight-human-trafficking/ [https://perma.cc/XL2V-BVK5].

[13] Benjamin Herold, *Facial-Recognition Systems Pitched as School-Safety Solutions, Raising Alarms*, EDWEEK (July 18, 2018), https://www.edweek.org/leadership/facial-recognition-systems-pitched-as-school-safety-solutions-raising-alarms/2018/07 [https://perma.cc/45A5-W75Y].

[14] *See* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. OF MACH. LEARNING RES. 1 (2018); *see also* NIST Demographic Study, *supra* note 10, at 2; Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-up: Unregulated police face recognition in America*, GEO. L. CTR. ON PRIV. & TECH. (2016), https://www.perpetuallineup.org/ [https://perma.cc/2NE3-6FDQ].

[15] Buolamwini & Gebru, *supra* note 14.

[16] Daniel E. Ho, Emily Black, Maneesh Agrawala & Li Fei-Fei, STAN. INST. FOR HUMAN-CENTERED A.I., EVALUATING FACIAL RECOGNITION TECHNOLOGY: A PROTOCOL FOR PERFORMANCE ASSESSMENT IN NEW DOMAINS 9 (2020) (characterizing the phenomenon as a "domain shift").

[17] Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/747V-8ASQ]; *see also* John General & Jon Starlin, *A false facial recognition match sent this innocent Black man to jail*, CNN (Apr. 29, 2021), https://edition.cnn.com/2021/04/29/tech/nijeer-parks-facial-recognition-police-arrest/index.html [https://perma.cc/AY4K-WTFN].

surveillance camera still to an FRT search engine, and it returned the man's driver's license as a match.[18] Moreover, police departments often have differing use procedures. Police could use the tool only for targeted searches for suspects, or they could conduct dragnet surveillance.[19] Some may only use FRT retroactively, while others may conduct real-time monitoring. These sorts of institutional differences make it difficult to standardize the most effective use policies.[20]

For its part, Clearview has recently performed well on the National Institute for Standards in Technology's (NIST's) 1:N Face Recognition Vendor Test (FRVT), which evaluates FRT algorithms used for identification.[21] In one assessment, Clearview scored 24th out of 316 participating algorithms in identifying subjects within a database of 1.6 million frontal mugshots, with a false negative rate of 0.58% and false positive rate of 0.18%.[22]

But aside from potential inaccuracy and bias problems, the proliferation of FRT raises profound risks to personal privacy and free expression. As opposed to a fingerprint—where a suspect must be present—FRT can identify individuals remotely, increasing the surveillance capability of the government dramatically.[23] Researchers of FRT policies worldwide have argued that robust FRT systems primarily increase the power of would-be authoritarian governments to control political discourse and oppress marginalized groups.[24] Beyond whether identification is accurate, there are very real questions about whether a society characterized by pervasive measurement and prediction of human activity is desirable.[25]

[18] Hill, *supra* note 17.

[19] *See* Garvie et al., *supra* note 14 (risk factors section).

[20] *See* Ho et al., *supra* note 16, at 11 (describing these problems as "institutional shifts").

[21] *See* Kashmir Hill, *Clearview AI does well in another round of facial recognition accuracy tests.*, N.Y. TIMES (Nov. 23, 2021), https://www.nytimes.com/2021/11/23/technology/clearview-ai-facial-recognition-accuracy.html [https://perma.cc/23X9-NWX7]; s*ee also* Patrick Grother, Mei Ngan & Kayee Hanaoka, NAT'L INST. OF STANDARDS AND TECH., FACE RECOGNITION VENDOR TEST, 1:N IDENTIFICATION (2021), https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf [https://perma.cc/VSK8-S9QZ].

[22] Grother et al., *supra* note 21. For a report card detailing Clearview's individual results, see https://pages.nist.gov/frvt/reportcards/1N/clearviewai_000.pdf [https://perma.cc/D6L5-RPTN].

[23] *See* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 410 (2012) (describing the shift towards remote surveillance).

[24] *See* Roussi, *supra* note 2; *see also* Hill, *supra* note 21 (discussing how the highest-performing algorithm in NIST's tests has been used to pervasively surveil the Uyghur Muslim population in China).

[25] *See generally* Jake Goldenfein, *Facial Recognition Is Only the Beginning*, PUB. BOOKS (Jan. 27, 2020), https://www.publicbooks.org/facial-recognition-is-only-the-beginning/

Nevertheless, governments increasingly seek to procure FRT. In summer 2021, amidst heightened attention from the public and Capitol Hill,[26] Clearview raised $30 million in new venture funding.[27] Furthermore, AnyVision, a real-time FRT company based in Israel, raised $235 million from SoftBank.[28] In addition to private investment, two recent reports from the Government Accountability Office (GAO) show that eighteen of 24 surveyed federal agencies currently use FRT systems, either owned internally or sourced from third parties.[29] Ten agencies report conducting research and development on FRT, and ten plan to expand usage of FRT in the next year.[30] In addition to agencies that fulfill traditional law enforcement and national security functions such as the Departments of Defense and Homeland Security, agencies such as the Department of Health and Human Services and the Department of the Treasury report using FRT for "domestic law enforcement" purposes.[31] The Department of Justice alone owns seven different FRT systems.[32]

While government adoption of FRT has increased, many states already regulate the capture and use of biometric information, and there is increasing momentum at both the state and federal levels to set parameters for FRT specifically. Illinois's Biometric Information Privacy Act (BIPA) is the leader in this sphere.[33] BIPA requires that users of biometric information obtain consent from the subject before collecting, capturing, or purchasing biometric information.[34] Other states, including California and New York, have also

(arguing that the proliferation of surveillance technology primarily serves the interests of powerful state and corporate interests, possibly at the expense of wider societal values) [https://perma.cc/782G-M5CE]; Monte Reel, *Secret Cameras Record Baltimore's Every Move From Above*, BLOOMBERG BUSINESSWEEK (Aug. 23, 2016), https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/ [https://perma.cc/T722-5QLS].

[26] *See generally Facial Recognition Technology: Examining Its Use by Law Enforcement: Hearing Before the Subcomm. On Crime, Terrorism, and Homeland* Security, 117th Cong. (2021) (Witness testimony) https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4635 [https://perma.cc/2LQV-MUFX].

[27] *Clearview AI takes steps to address facial recognition usage controversies*, VERDICT (Aug. 23, 2021), https://www.verdict.co.uk/clearview-ai-facial-recognition-technology/ [https://perma.cc/TEB4-DDCZ].

[28] *Id.*

[29] GAO Report, *supra* note 4.

[30] *Id.*

[31] *Id.* at 11.

[32] *Id.* at 16.

[33] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/15 (2008) [hereinafter BIPA].

[34] *Id.*

enacted biometric privacy legislation.[35] With respect to FRT, some large cities and states have banned law enforcement use,[36] in line with proposals from numerous scholars.[37] In 2020, several bills were introduced in the United States Congress aimed at regulating the collection and use of biometric information.[38] At the time of this writing, none have passed.

A. The Clearview AI Case Study

Clearview AI is perhaps the most high-profile face recognition company in the United States. It burst onto the national scene in January 2020 after a *New York Times* article[39] detailed its inner workings. The company provides a searchable database of ten billion images containing human faces.[40] The user of its application uploads a picture, and the search engine returns photos scraped from public social media profiles that "match" the uploaded photograph.[41] The matching pictures are paired with links to the sites from which they are scraped, so one can glean personal information from the

[35] Natalie Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020*, NAT'L L. REV. (Jan. 15, 2020), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020 [https://perma.cc/AM6K-CTF7].

[36] Boston and San Francisco are two notable examples. *See, e.g.*, Ally Jarmanning, *Boston Lawmakers Vote to Ban the Use of Facial Recognition Technology by the City*, NPR (June 24, 2020), https://www.npr.org/sections/live-updates-protests-for-racialjustice/2020/06/24/883107627/boston-lawmakers-vote-to-ban-use-of-facial-recognition-technology-by-the-city [https://perma.cc/NL4X-ZPW4]; Shannon Van Sant & Richard Gonzales, *San Francisco Approves Ban On Government's Use Of Facial Recognition Technology*, NPR (May 14, 2019), https://www.npr.org/2019/05/14/723193785/san-francisco-considers-ban-on-governments-use-of-facial-recognition-technology [https://perma.cc/8X9J-HMXK].

[37] *See, e.g.*, Lindsey Barrett, *Ban Facial Recognition Technologies for Children, and for Everyone Else*, B.U. J. SCI. & TECH. L. (2020); 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 [https://perma.cc/4B27-QBFL].

[38] Kelsey Y. Santamaria, *Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations*, CONG. RES. SERV. 27 (Sept. 24, 2020), https://crsreports.congress.gov/product/pdf/R/R46541.

[39] 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 [https://perma.cc/BF7H-3VPC].

[40] *Id.*

[41] "Mr. Ton-That described [the technology] as a 'state-of-the-art neural net' to convert all the images into mathematical formulas, or vectors, based on facial geometry—like how far apart a person's eyes are. Clearview created a vast directory that clustered all the photos with similar vectors into 'neighborhoods.' When a user uploads a photo of a face into Clearview's system, it converts the face into a vector and then shows all the scraped photos stored in that vector's neighborhood—along with the links to the sites from which those images came." *Id.*

subject's social media accounts.[42] Whereas earlier FRT datasets may have been created internally—say, by a casino identifying repeat gamblers or by law enforcement using a database of mugshots[43]—Clearview's tool uses public images on social media sites to constitute the template dataset. Clearview maintains that it exclusively sells its technology to law enforcement and that this is the app's only planned use,[44] but it has also been tested by private investors and companies such as Macy's.[45] One of Clearview's initial backers was a far right-wing media consultant who said he saw potential in the technology because it could "identify every illegal alien in the country."[46] Clearview employees have also been linked to white nationalist groups.[47]

The tool is popular among law enforcement agencies, at least at the software trial level.[48] As of April, 2021, over 1,800 law enforcement entities in the United States had at least tested the engine,[49] and law enforcement

[42] *Id.*

[43] *See* Singer, *supra* note 5.

[44] Caroline Haskins, *A Clearview AI Patent Application Describes Facial Recognition For Dating, And Identifying Drug Users And Homeless People*, BUZZFEED NEWS (Feb. 11, 2021), https://www.buzzfeednews.com/article/carolinehaskins1/facial-recognition-clearview-patent-dating [https://perma.cc/R8EY-M79T]. Sometimes actions speak louder than words. In a 2020 patent application, Clearview described potential applications of its technology as follows: "In many instances, it may be desirable for an individual to know more about a person that they meet, such as through business, dating, or other relationship." *Id.*

[45] Kashmir Hill, *Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*, N.Y. TIMES (Mar. 5, 2020), https://www.nytimes.com/2020/03/05/technology/clearview-investors.html [https://perma.cc/P44T-L89N]; 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 (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement [https://perma.cc/C7SE-EJ7W]. While this Note assesses Clearview's First Amendment claims under the assumption that it partners exclusively with law enforcement, private use of FRT in general is certainly on the horizon and also poses complex questions about expressive rights in light of widespread private surveillance.

[46] Luke O'Brien, *The Far-Right Helped Create The World's Most Powerful Facial Recognition Technology*, HUFFPOST (Apr. 7, 2020), https://www.huffpost.com/entry/clearview-ai-facial-recognition-alt-right_n_5e7d028bc5b6cb08a92a5c48 [https://perma.cc/UC8Z-2BSF].

[47] *Id.*

[48] So popular, in fact, that Clearview was added to Time's list of Most Influential Companies in 2021. *Time 100 Most Influential Companies*, TIME (2021), https://time.com/collection/time100-companies/ [https://perma.cc/P8XU-PBQ7].

[49] Ryan Mac et. al., *Your Local Police Department Might Have Used This Facial Recognition Tool To Surveil You. Find Out Here*, BUZZFEED NEWS (Apr. 9, 2021), https://www.buzzfeednews.com/article/ryanmac/facial-recognition-local-police-clearview-ai-table [https://perma.cc/DVX3-STZ9].

agencies in at least 24 other countries have as well.[50] As documents detailing private emails between Clearview and the New York Police Department (NYPD) have shown, officers "trialing" the software have conducted thousands of searches over multiple years, with officers downloading the app onto their personal devices—all in violation of department policies.[51]

In the wake of the *New York Times* story, Clearview CEO Hoan Ton-That went to major media outlets to defend the technology, likening it to other search engines such as Google and highlighting its potential to help catch criminals.[52] More recently, Clearview's attorneys have touted law enforcement's increased usage of facial recognition software in the wake of the January 6, 2021 Capitol riot.[53] Although platforms like Twitter and Facebook have sent Clearview cease and desist letters for violating their terms of service,[54] Ton-That claims Clearview has a "First Amendment right" to scrape publicly available images and measure the faces of those captured.[55]

In 2020, the American Civil Liberties Union (ACLU) sued Clearview in Illinois state court, alleging that Clearview's use of FRT to measure faces of Illinois residents without consent violated BIPA.[56] Signaling its intent to fight hard to escape liability, Clearview hired prominent First Amendment lawyer Floyd Abrams.[57] In a motion to dismiss the state court lawsuit,

[50] Ryan Mac et. al., *Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here*, BUZZFEED NEWS (Aug. 25, 2021), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table [https://perma.cc/4FED-MSU9].

[51] Tate Ryan-Mosley, *The NYPD used a controversial facial recognition tool. Here's what you need to know*, MIT TECH. REV. (Apr. 9, 2021), https://www.technologyreview.com/2021/04/09/1022240/clearview-ai-nypd-emails/ [https://perma.cc/3RMF-2FYD].

[52] *CEO speaks out about Clearview AI's controversial facial recognition technology*, CBS NEWS (Feb. 5, 2020), https://www.youtube.com/watch?v=-JkBM8n8ixI&t=334s [hereinafter *CEO Speaks Out*]; Donie O'Sullivan, *This man says he's stockpiling billions of our photos*, CNN (Feb. 10, 2020), https://www.cnn.com/2020/02/10/tech/clearview-ai-ceo-hoan-ton-that/index.html [https://perma.cc/89LH-N6SB].

[53] Floyd Abrams & Lee Wolosky, *The Promise and Peril of Face Recognition*, WALL ST. J. (Jan. 13, 2021), https://www.wsj.com/articles/the-promise-and-peril-of-facial-recognition-11610579445?st=bj9rle5jnvcfet6&reflink=article_copyURL_share [https://perma.cc/2UUF-88KU].

[54] Kaixin Fan, *Clearview AI Responds to Cease-and-Desist Letters by Claiming First Amendment Right to Publicly Available Data*, HARV. J. L. & TECH. (Feb. 25, 2020), https://jolt.law.harvard.edu/digest/clearview-ai-responds-to-cease-and-desist-letters-by-claiming-first-amendment-right-to-publicly-available-data [https://perma.cc/B24A-UJHG].

[55] *CEO Speaks Out*, *supra* note 52.

[56] Compl., ACLU v. Clearview AI*,* No. 20 CH 4353 (Ill. Cir. Ct. filed May 28, 2020) [hereinafter Clearview BIPA Litigation]. For court documents relating to the litigation, see ACLU v. Clearview AI, ACLU (May 27, 2020), https://www.aclu.org/cases/aclu-v-clearview-ai [https://perma.cc/7X87-Z9XY].

[57] Kashmir Hill, *Facial Recognition Start-Up Mounts a First Amendment Defense*, N.Y. TIMES (Aug. 11, 2020), https://www.nytimes.com/2020/08/11/technology/clearview-floyd-

Clearview argued that its activities—the scraping of images, measuring them, and selling search results to law enforcement—are protected by the First Amendment.[58] As applied to Clearview, the company urged, BIPA violates the First Amendment.[59] Numerous amici weighed in, with two First Amendment scholars supporting Clearview's claims.[60] A separate group of professors supported the ACLU,[61] while the Electronic Frontier Foundation (EFF) argued that, although Clearview's faceprinting is protected speech, BIPA should withstand the court's intermediate scrutiny.[62]

The court denied Clearview's motion to dismiss, but still held that Clearview's faceprinting is entitled to "some First Amendment protection."[63] Instead of engaging in a full-fledged analysis to determine whether Clearview's faceprinting is covered by the First Amendment, the court instead repeated Clearview's arguments that the First Amendment protects some necessary predicates to expression, such as data collection.[64] It also noted that the parties and amici all essentially agreed or assumed that faceprinting involves some level of protected First Amendment activity.[65] Nevertheless, BIPA survived the court's intermediate scrutiny as a reasonable regulation of protected speech.[66] Here, the court failed to consider the possibility that algorithmic measurement of facial geometry is not speech within the meaning of the First Amendment. The next Section explains a possible reason for this omission.

abrams.html [https://perma.cc/M5GJ-56JS]. During a phone call with the *Times*' reporter, Abrams said that he had "never used the words 'facial biometric algorithms' until this phone call." *Id.*

[58] *See* Def.'s Mem. of Law in Supp. of Its Mot. to Dismiss, Clearview BIPA Litigation, *supra* note 56, at 16–19.

[59] *Id.* at 16, 19–21. The company has also raised the same defense in an ongoing federal multidistrict litigation. *See* Defs.' Opp'n to Pls.' Mot. for Prelim. Inj. at 12, In re Clearview AI, Inc. Consumer Privacy Litig., No. 1:21-cv-00135 (N.D. Ill. 2021), ECF No. 43.

[60] Br. of Amici First Amendment Clinic at Duke Law and Professors of Law Eugene Volokh and Jane Bambauer in Supp. of Def.'s Mot. to Dismiss, Clearview BIPA Litigation, *supra* note 56.

[61] Br. of Amici Law Professors in Opp'n to Def.'s Mot. to Dismiss, Clearview BIPA Litigation, *supra* note 62.

[62] Br. of Amicus Electronic Frontier Foundation in Opp'n to Def.'s Mot. to Dismiss, Clearview BIPA Litigation, *supra* note 56, at 4.

[63] *See* Mem. Op. and Order, Clearview BIPA Litigation, *supra* note 56, at 9.

[64] *Id.*

[65] *Id.*

[66] *Id.* at 10–11.

B. First Amendment *Lochner*ism and Free Speech in a Networked World

Clearview's defense is part of the broader trend of companies claiming—and courts ruling—that various corporate activities are protected by the First Amendment, which in part prohibits governments from abridging the "freedom of speech."[67] Scholars have likened the trend to the *Lochner* era in the early 1900s, where the Supreme Court struck down myriad commercial regulations under broad theories of substantive due process.[68] The idea, as Professor Oren Bracha sums it up, is that "any coercive interference [with corporate activity] . . . abridges speech and is thus prohibited by the First Amendment."[69] Some predict that the current Supreme Court is on a path towards striking down everything from data privacy laws to securities and advertising regulations as part of a new "First Amendment *Lochner*ism" era.[70]

Data collection and processing has joined the pantheon of First Amendment *Lochner*ism in part due to the Supreme Court's 2011 decision in *Sorrell v. IMS Health*, where the Court invalidated a Vermont privacy law.[71] The law prohibited the sale, disclosure, and use of prescriber-identifying information (PII) without consent.[72] Pharmacies commonly sold information about which doctors prescribed which drugs to data miners.[73] Marketers of drugs would buy this PII from the data miners in order to determine the

[67] U.S. Const. amend. I. *See, e.g.*, Citizens United v. FEC*,* 558 U.S. 310, 337 (2010) (striking down a law that criminalized corporate election advocacy or "broadcast [of] electioneering communications within 30 days of a primary election and 60 days of a general election"); *see also* Plaintiffs' Motion for Judgment on the Pleadings at 10, ACA Connects v. Frey, No. 1:20-cv-00055-LEW (Dist. Me. 2020) [hereinafter ACA Connects Motion] (arguing that internet service providers' use of "consumer information to communicate with their customers, to market and advertise their products, and to facilitate geographically targeted public service announcements" is protected speech, and as such a Maine privacy law is unconstitutional as applied to the plaintiffs).

[68] *See* Lochner v. New York, 198 U.S. 45, 64 (1905) (striking down a state labor law limiting maximum number of weekly work hours as a violation of the Fourteenth Amendment's guarantee of due process).

[69] Oren Bracha, *The Folklore of Informationalism: The Case of Search Engine Speech*, 82 FORDHAM L. REV. 1629, 1639 (2014).

[70] *See generally* Amanda Shanor, *The New* Lochner, 2016 WISC. L REV. 133 (2016); Jeremy K. Kessler, *The Early Years of First Amendment Lochernism*, 116 COLUM. L. REV. 1915 (2016); Jeremy K. Kessler & David Pozen, *The Search for an Egalitarian First Amendment*, 118 COLUM. L. REV. 1953, 1961–77 (2018); Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1529 (2015); Bracha, *supra* note 69, at 1638–40.

[71] *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 570 (2011).

[72] *Id.*

[73] *See id.* at 558.

prescribing habits of the doctors to whom they sold medications.[74] Vermont's law required the consent of the prescribing doctor in exchange for collection and use of the identifying information.[75] But the Supreme Court invalidated the law on the grounds that it targeted some speakers (pharmaceutical manufacturers), and not others (for example, educational entities were exempted), and placed limits on the use of the PII (it could not be used for marketing).[76] As such the Court held that the law was a content- and viewpoint-based restriction on speech subject to strict scrutiny, which it did not withstand.[77]

Notably, however, Justice Anthony Kennedy's majority opinion also contained dicta proposing that "the creation and dissemination of information are speech within the meaning of First Amendment."[78] Vermont had argued that PII is not speech within the meaning of the First Amendment.[79] Justice Kennedy did not affirmatively reach this argument, holding instead that the law violated the First Amendment because it was a speaker-based restriction, even assuming the underlying content was not protected.[80] But Justice Kennedy nevertheless posited that there is a "strong argument that [PII] is speech for First Amendment purposes" because facts (embodied in data) form the basis for speech and are essential to advancing human knowledge.[81]

Again, there is every indication that this passage is dicta,[82] but subsequent litigants, including Clearview, have interpreted it to stand for the proposition that creating or disclosing data is protected speech.[83] The implication here is that *all* information processing could be deemed protected speech and, therefore, any regulation of it would be subject to constitutional challenge. This may strike some as odd, even radical. This is perhaps because it is an argument raised by a company in litigation seeking to escape liability. The First Amendment is a creature of litigation in that its rights are defined

[74] *Id.*
[75] *Id.* at 558–59.
[76] *Id.* at 571.
[77] *Id.*
[78] *Id.* at 570.
[79] *Id.*
[80] *See id.* at 571.
[81] *Id.*
[82] *See* Richards, *supra* note 70, at 1520–23 (reiterating that because Vermont's law was a viewpoint-based restriction, it did not really matter whether the underlying activity was actually protected speech; the better way to read the holding of *Sorrell* is that it merely strikes down a regulation targeting some potential speakers and not others—as opposed to the incredibly broad reading that all use of data is speech); *see also* G.S. Hans, *No Exit: Ten Years of "Privacy vs. Speech" Post-Sorrell*, 65 WASH. UNIV. J. L. & POL. 19, 24–25 (2021) (characterizing the passage as dicta).
[83] *See* Def.'s Mot. to Dismiss at 16, Clearview BIPA Litigation, *supra* note 56; ACA Connects Mot., *supra* note 67.

according to who brings which lawsuits at which time in history. In other words, the reach of the amendment is defined by the interests of litigants in individual cases. This has caused Professor Frederick Schauer to warn against "First Amendment opportunism."[84] Dissenting in *Sorrell*, Justice Stephen Breyer offered a dire warning:

> At best the Court opens a Pandora's Box of First Amendment challenges to many ordinary regulatory practices that may only incidentally affect a commercial message . . . . At worst, it reawakens *Lochner*'s pre-New Deal threat of substituting judicial for democratic decision-making where ordinary economic regulation is at issue.[85]

As Professor G.S. Hans recently pointed out, the Supreme Court has not meaningfully addressed the intersection between privacy regulation and the First Amendment since *Sorrell*.[86] And given Clearview's hiring of high-powered lawyers like Floyd Abrams, attention from well-known amici, and its statements to the press, the company seems poised to seek endorsement of the "data equals speech" argument in the high court.

In light of this impending inflection point, this Note offers a way to assess the Clearview case (and others like it) at the coverage stage of the First Amendment inquiry, without assuming privacy laws like BIPA regulate covered speech. The next Part describes First Amendment coverage doctrine and offers an updated framework that assesses the systemic effects of purported speech and how they relate to recognized First Amendment principles. Part IV applies that framework to Clearview AI's faceprinting—the algorithmic measurement of human facial geometry in service of law enforcement surveillance.[87]

[84] *See* Frederick Schauer, *The Politics and Incentives of First Amendment Coverage*, 56 WM. & MARY L. REV. 1613, 1627 (2015); *see also* Amanda Shanor, *First Amendment Coverage*, NYU L. REV. 318, 325 (2018) ("Coverage is a sociological concept: It is not the theoretical or philosophical scope of the right of free speech, but what litigants and courts in a given historical moment view as within, or plausibly within, the scope of that right. It is the range of activities whose regulation strikes legal actors at the constitutional moment.").

[85] *Sorrell*, *supra* note 71, at 602–03 (internal citations omitted).

[86] Hans, *supra* note 82.

[87] The inquiry is defined so narrowly because that is the exact activity BIPA regulates, and so the only activity on Clearview's part to which the First Amendment could apply here. Clearview's tool also scrapes the web for photographs. But BIPA does not regulate web scraping in itself, so whether the First Amendment is implicated in scraping is irrelevant. BIPA regulates collection, processing, and sale of biometric information.

III. FIRST AMENDMENT COVERAGE

A. Coverage vs. Protection

The First Amendment protects the people from laws and regulations that abridge the freedom of speech.[88] Courts apply different tiers of scrutiny when determining whether a government regulation violates the First Amendment, depending how burdensome the law is upon speech. This is the level of "protection" speech receives. For example, commercial regulations that only incidentally impinge upon protected speech receive intermediate scrutiny.[89] However, if a regulation directly targets speech based on its content or viewpoint, the law may stand only if the government proves it is "narrowly tailored to serve compelling state interests."[90] This is strict scrutiny.[91]

Yet not all "speech" in the literal form of the word implicates the First Amendment. For instance, there are numerous traditional, judge-made exceptions to First Amendment protection, such as obscene speech,[92] libel,[93] and fighting words[94]—words and phrases that may have expressive content, but the Supreme Court nonetheless deems unprotected.[95] The Court has cautioned against formally recognizing other exceptions.[96] But beyond those categorical exclusions, much speech still falls within the purview of regulation and is not thought to raise a First Amendment issue. Commonly invoked examples include agreements not to compete (antitrust), securities fraud, and bedrock principles of contract law.[97] Put simply, we do not have a First Amendment right to breach contracts, perpetrate fraud, or engage in anticompetitive business practices. In any First Amendment case, therefore, the threshold question is whether a given practice triggers First Amendment protection at all—whether it is covered. Scholars have observed that the

[88] *See* U.S. Const., amend. I.

[89] United States v. O'Brien, 391 U.S. 367, 377 (1968).

[90] Reed v. Town of Gilbert, 576 U.S. 155, 163 (2015).

[91] *See id.*

[92] Roth v. United States, 354 U.S. 476, 485 (1957).

[93] N.Y. Times Co. v. Sullivan, 376 U.S. 254 (1964).

[94] Chaplinksy v. New Hampshire, 315 U.S. 568 (1942).

[95] *See* United States v. Stevens, 559 U.S 460, 468–69; *see also* Tim Wu, *Machine Speech*, 161 U. PA. L. REV. 1495, 1509 (2013) (describing these examples as "formal exclusions").

[96] *See* Brown v. Ent. Merchants Ass'n, 564 U.S. 786, 791 (2011) (affirming that "new categories of unprotected speech may not be added to the list by a legislature that concludes certain speech is too harmful to be tolerated").

[97] *See* Schauer, *supra* note 84, at 1619; Richards, *supra* note 70, at 1515–16 (discussing stalking, eavesdropping, wiretapping, breaking client confidentiality, and others).

doctrine concerning this "dark matter"[98] of uncovered speech is in flux and often not even acknowledged by judges resolving First Amendment cases.[99]

The traditional test employed by the Supreme Court for coverage fails to account for the plethora of speech practices that do not trigger the amendment's protection. It comes from *Spence v. Washington*, and asks whether the activity at issue displays "an intent to convey a particularized message," and "in the surrounding circumstances the likelihood was great that the message would be understood by those who viewed it."[100] In this case, the Supreme Court held that a student hanging a flag with a peace sign taped onto it in protest of the Vietnam War was protected.[101]

As Robert Post has illustrated, however, neither prong of the *Spence* test states a sufficient condition for triggering the First Amendment because in any given instance, social context is constitutive of meaning.[102] One of Post's more evocative examples demonstrating this is the bathroom urinal. A urinal in a bathroom does not implicate the First Amendment even though it communicates a message and those who see it understand what it's for.[103] A urinal placed in an art show,[104] however, is much more likely to implicate the First Amendment. What has changed? The social space, its purpose, and its connection to First Amendment values. In other words, concluding that provocative art has more claim to protection than a urinal in a bathroom necessitates some sort of judgment about social context and the values served by the First Amendment.

This insight has led scholars to conclude that "[t]he only satisfactory way of answering the [coverage] question, for whose resolution no clear guidance exists in the case law, is through normative analysis."[105] When deciding which types of speech and conduct are to win protection, it is necessary to consider the values and purposes served by the amendment. Courts and scholars alike have recognized three normative values that pertain to the First Amendment: democratic governance, the marketplace of ideas, and individual autonomy.[106] Democratic governance conceives of the First Amendment as a tool with which society may check public officials and debate

[98] Bracha, *supra* note 69, at 1659.

[99] *See id.*; Robert Post, *Recuperating First Amendment Doctrine*, 47 STAN. L. REV. 1249, 1250 (1995); Shanor, *supra* note 84, at 341–43.

[100] 418 U.S. 405, 410–11 (1974).

[101] *Id.* at 415.

[102] *See* Post, *supra* note 99, at 1254.

[103] *Id.*

[104] This seems to be a reference to Marcel Duchamp's "Fountain." Marcel Duchamp, *Fountain* (1917).

[105] Bracha, *supra* note 69, at 1654.

[106] *See id.* at 1665 (cataloging various scholarly works).

the social and political issues of the day.[107] The marketplace of ideas theory posits that truth-seeking is best accomplished by the open flow of ideas.[108] The marketplace theory, however, has been subject to widespread criticism, in part on the ground that not all speakers have equal ability to have their ideas heard.[109] Individual autonomy theory, possibly the broadest conception of the amendment's purpose, proposes that the First Amendment protects an individual's ability to craft their identity—to define who they are by receiving and creating new ideas—because such freedom is intimately bound up with notions of liberty and self-rule.[110] Yet no single theory is itself sufficient to explain why we view some speech as covered, but not other speech; there is no one-size-fits-all normative theory to describe the Supreme Court's coverage jurisprudence.[111]

B. Assessing Systemic Effects at the Coverage Stage

As mentioned in Part IIA above, the issue of whether Clearview's faceprinting is covered by the First Amendment has been largely ignored in its BIPA litigation thus far. Part IIB likewise illustrated why this is concerning: it could be a harbinger of First Amendment *Lochner*ism applied to the digital world at a time when technology companies and governments assert increasing control over public life through surveillance. The prospect of a company like Clearview being immune from a regulation such as BIPA is alarming. This subpart builds upon recent scholarship to provide a fuller coverage analysis for a case like Clearview's: in considering coverage, courts should analyze the potential *systemic effects* of the activity in question, and what relation those effects bear to recognized First Amendment values.

[107] *See Sullivan*, 376 U.S. at 275 ("The right of free public discussion of the stewardship of public officials was thus, in Madison's view, a fundamental principle of the American form of government."); Alexander Meiklejohn, *Free Speech and its Relation to Self-Government*, 93–94 (1948) ("[T]he principle of the freedom of speech is derived, not from some supposed 'Natural Right,' but from the necessities of self-government by universal suffrage . . . .").

[108] *See* Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) ("There is no such thing as a false idea. However pernicious an opinion may seem, we depend for its correction not on the conscience of judges and juries but on the competition of other ideas . . . . [T]he ultimate good desired is better reached by free trade in ideas—that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out.") (internal citations omitted).

[109] *See, e.g.*, Mary Anne Franks, *The Free Speech Black Hole: Can The Internet Escape the Gravitational Pull of the First Amendment?*, COLUM. UNIV. KNIGHT FIRST AM. INST. (Aug. 21, 2019), https://knightcolumbia.org/content/the-free-speech-black-hole-can-the-internet-escape-the-gravitational-pull-of-the-first-amendment [https://perma.cc/NHC4-MRNB].

[110] *See* C. Edwin Baker, *Autonomy and Free Speech*, 27 CONST. COMMENT. 251 (2011).

[111] Post, *supra* note 99, at 1272.

Like Schauer and Post, more recent scholarship has highlighted the necessity of making normative judgments about social context before determining whether a given activity is covered. For example, Professor Neil Richards has proposed a sliding-scale approach: arguments for protection are stronger when the activity involves publication in news media, and weaker in other contexts involving, say, bankers, lawyers, doctors, etc., whose speech rights may be more limited due to confidentiality duties.[112]

On the free speech maximalism side of the coin, Professor Jane Bambauer, co-author of an amicus brief in support of Clearview AI,[113] has argued that information in general is subject to protection because of what she calls a "right to create knowledge" inherent in the First Amendment.[114] But for judicially enumerated exceptions, the First Amendment would extend to virtually any communication of information. However, there are problems with this approach that have been well-covered in the literature.[115] In short, per Neil Richards's formulation, "[i]f our lives become digital, but data is speech, regulation of many kinds of social problems will become impossible." [116] Everything humans do could theoretically be deemed expressive, and it does not serve democracy to make every law passed by an elected legislature subject to scrutiny by judges simply because they impinge upon conduct that could be termed expressive.[117]

Others have advanced more granular theories of coverage. Amanda Shanor posits that the First Amendment should not extend "when there is a common norm about the social effect of the activity or when the court decides

[112] Richards, *supra* note 70, at 1516 (making the point that the privacy torts advocated by Warren and Brandeis would likely run afoul of the First Amendment because they merely seek to prevent publication of gossip).

[113] Br. of Amici First Amendment Clinic at Duke Law and Professors of Law Eugene Volokh and Jane Bambauer in Support of Def.'s Mot. to Dismiss, Clearview BIPA Litigation, *supra* note 56.

[114] Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 86 (2014).

[115] *See, e.g.*, Wu, *supra* note 95, at 1508 ("A fully inclusive theory of the First Amendment would need to treat as speech forms of communication utterly devoid of ideas or content."); *see also* Richards, *supra* note 70, at 1524; Shanor, *supra* note 84, at 359–60; Bracha, *supra* note 69, at 1639–40. For a defense of the maximalist position in light of First Amendment *Lochner*ism critiques, see Jane Bambauer, *Information Libertarianism*, 105 CAL. L. REV. 335 (2017).

[116] Richards, *supra* note 70, at 1531.

[117] *Id.* at 1528; *see also* Cass R. Sunstein, *Pornography and the First Amendment*, 1986 DUKE L. J. 589, 605 (1986) ("But it would be difficult to imagine a sensible system of free expression that did not distinguish among categories of speech in accordance with their importance to the underlying purposes of the free speech guarantee. A system that granted absolute protection to speech would be unduly mechanical, treading unjustifiably on important values and goals: consider laws forbidding threats, bribes, misleading commercial speech, and conspiracies.").

there should be such a norm."[118] For example, because we are sufficiently familiar with harms that ensue when people break promises, we can confidently say that certain speech practices regulated by the common law of contracts do not trigger First Amendment protection.[119] Oren Bracha argues that search engine results are not covered, assessing the connection or lack thereof between search results and traditional normative justifications for speech: "a particular regulation targeting a specific practice is outside the coverage of the First Amendment when the speech practice, understood in light of the specifics of the social interactions involved, has little or no significance for freedom of speech values."[120] While these two assessments are different in important respects, when taken together they recognize the importance of the effects of the speech practice and its social context.

Blending the two, I propose that courts should inquire into potential *systemic* effects of the activity in question, and whether those effects connect to free speech values such as deliberative democracy and autonomy. "Systemic" in this sense means "fundamental to a predominant social, economic, or political practice."[121] Like Shanor, this inquiry accounts for the social effects of the activity, and like Bracha, it asks what connection those effects bear to recognized free speech values. The *Spence* test, Bracha, and Shanor, however, assume an exchange between one speaker and one listener or group of listeners when determining whether something should be deemed protected speech. Shanor, for instance, focuses on "how a speaker will affect the behavior of or harm a listener or audience."[122] But this is too narrow. Any analysis of the social context in which an activity occurs is incomplete without inquiry into its potential systemic implications: the societal impacts of the activity in question and its potential effects on fundamental institutions.

Take a lawyer or doctor, for instance. Likely no judge in the country would entertain the notion that these professionals have a First Amendment right to divulge client or patient confidences. People would lack trust that they could safely share sensitive information to their providers, and the legal and healthcare systems would crash. We may view these examples as places where certain *social contexts*, and the systemic effects of potentially harmful speech,

[118] Shanor, *supra* note 84, at 346.
[119] *See id.*
[120] Bracha, *supra* note 69, at 1666.
[121] *Systemic*, MERRIAM-WEBSTER ONLINE DICTIONARY, https://www.merriam-webster.com/dictionary/systemic (last visited Oct. 25, 2021) [https://perma.cc/KN3G-ZRGB].
[122] Shanor, *supra* note 84, at 344.

serve to limit the reach of the First Amendment.[123] This proposal would give judges room to ask broader questions about the effects of "speech."

To be sure, judges already ask these questions, explicitly and implicitly. Language in Supreme Court opinions provides a precedential basis for assessing systemic effects. In the context of the traditional categorical exceptions to coverage, the Supreme Court has excluded speech from protection based on assumed systemic harms.[124] The classic quote illustrating this point comes from *Chaplinsky v. New Hampshire*, where the Court declined to extend protection to fighting words: "such utterances are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality."[125] In that case, the exclusion of the phrase "damn Fascist" from First Amendment protection was to prevent risks of "breach[es] of the peace."[126] An early case excluding obscene speech from protection similarly asserted that obscene speech lacks any semblance of "redeeming social importance."[127] *Watts v. United States* recognized the nation's "overwhelming" interest in protecting the President from threats of violence, and on that basis held that the statute criminalizing such actions did not violate the First Amendment.[128] The Court in *Virginia v. Black* implicitly reasoned that true threats—in that case, the burning of a cross with intent to intimidate—should not be accorded protection because of systemic societal harms that flow from threats of violence.[129]

[123] This may remind some readers of Jack Balkin's proposal that digital platforms be regarded as "information fiduciaries." *See generally* Jack Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149 (2018). Here, by contrast, I am discussing the scope of rights of those companies as speakers, as opposed to the duties owed to other speakers by those platforms.

[124] *See* Sunstein, *supra* note 117, at 615 ("Analysis of suppression of speech advocating the immediate and violent overthrow of the government would be similar: the government is attempting to eradicate a harm, not attempting to impose a particular point of view. Bans on false or misleading commercial speech, cigarette advertising, or casino gambling are analyzed in substantially the same way. In the obscenity context, the reasoning is more obscure, but the central point remains: in some contexts, statutes that appear to be viewpoint-based are justified and accepted because of the harms involved. The harms are so obvious and immediate that claims that the government is attempting to silence one position in a 'debate' do not have time even to register.").

[125] *Chaplinsky*, 315 U.S. at 572.

[126] *Id.*

[127] *Roth*, 354 U.S. at 484.

[128] Watts v. United States, 394 U.S. 705, 707 (1969).

[129] *See* Virginia v. Black, 538 U.S. 343, 360 (2003) ("Rather, a prohibition on true threats 'protect[s] individuals from the fear of violence' and 'from the disruption that fear engenders,' in addition to protecting people 'from the possibility that the threatened violence will occur.' Intimidation in the constitutionally proscribable sense of the word is a type of

This is not to say that the Supreme Court's "limited categorical approach"[130] should be expanded, only that systemic effects of purported speech activities have played a role in the Court's reasoning regarding coverage over time. Nor is this limited to the categorical exclusions; the Court has employed similar reasoning in national security cases.[131] For example, in *Holder v. Humanitarian Law Project*, the Court declined to accept criminal defendants' arguments that funding and teaching international law principles to designated terrorist organizations amounted to protected speech.[132] Instead, the Court held that the government's prosecution of the defendants' activities under the material support statute did not raise a constitutional concern.[133] In doing so, the Court linked the funding and teaching to the terrorist activities that presumably follow, recognizing terrorism's systemic harms. For example, "training and advising a designated foreign terrorist organization on how to take advantage of international entities might benefit that organization in a way that facilitates its terrorist activities,"[134] and "[p]roviding foreign terrorist groups with material support in any form also furthers terrorism by straining the United States' relationships with its allies and undermining cooperative efforts between nations to prevent terrorist attacks."[135]

In the categorical exclusion and national security contexts, therefore, speech may be excluded from coverage based on the systemic effects the Court deems likely to follow from the speech practice. One might question why we need a new test, or a new factor to add to the *Spence* test. But as illustrated above, the Court already engages in systemic effects analysis, if by implication at times. This proposal seeks to make that inquiry explicit and consistent. As Bracha and others explain, any one normative speech theory alone is insufficient to answer all coverage questions.[136] Adding a broader layer that considers what the activity does in the world makes the analysis more holistic.

This approach also makes sense in a world where litigants argue that computer algorithms themselves, or their outputs, are speech. It is not easy to define who is the listener. After all, the listener could just be a machine.

true threat, where a speaker directs a threat to a person or group of persons with the intent of placing the victim in fear of bodily harm or death.") (internal citations omitted).

[130] R.A.V. v. City of St. Paul, 505 U.S. 377, 383 (1992).

[131] *See* Cass R. Sunstein, *Islamic State's Challenge to Free Speech*, BLOOMBERG (Nov. 23, 2015), https://www.bloomberg.com/opinion/articles/2015-11-23/islamic-state-s-challenge-to-free-speech [https://perma.cc/T3EW-54LK].

[132] Holder v. Humanitarian L. Project, 561 U.S. 1, 40 (2010); *see also* Shanor, *supra* note 84, at 336 (analyzing other material support cases where courts have declined to find a First Amendment concern in the criminal defendants' expression).

[133] *Humanitarian L. Project*, 561 U.S. at 40.

[134] *Id.* at 38.

[135] *Id.* at 32.

[136] Bracha, *supra* note 69, at 1665.

Further, because systems like Clearview's that employ neural networks are able to quickly process massive amounts of data and make decisions that affect a vast number of people, the effects of operating these computer programs may often be systemic in nature.[137] Indeed, we are becoming increasingly aware of the systemic effects of algorithmic decision-making across society in the context of hiring, behavioral advertisement targeting, and more.[138] Even though the judge in Clearview's state court litigation did not hold BIPA unconstitutional, it is no less necessary to consider broader societal effects just because a regulation like BIPA survived Clearview's First Amendment defense in one instance. The holding that Clearview's faceprinting is protected speech, but that BIPA withstands intermediate scrutiny, does not allay the fears espoused by Justice Breyer in *Sorrell*.

In sum, because the traditional tests for coverage are unsatisfying, courts can and should assess the potential systemic effects that a practice has on society broadly, and whether the effects bear any connection to First Amendment principles. The next part will apply this to Clearview AI's faceprinting.

IV. THE SYSTEMIC THREATS TO EXPRESSIVE AND ASSOCIATIONAL LIBERTIES POSED BY FACEPRINTING IN SERVICE OF POLICE SURVEILLANCE

In assessing the systemic implications of Clearview's faceprinting, we must acknowledge that, at this time, it is a law enforcement surveillance tool. One need look no further than the company's website to confirm this: banners reading "Supporting U.S. Law Enforcement and Government Agencies," and "Trusted By Law Enforcement" can be found on the homepage.[139] Thousands of agencies have at least tested the search engine,[140] and leaked emails from some have revealed close working relationships between the company and governments.[141] And as Elizabeth Joh points out, widespread government

[137] *See* Kinjal Dave, *Systemic Algorithmic Harms*, DATA & SOC'Y (May 31, 2019), https://points.datasociety.net/systemic-algorithmic-harms-e00f99e72c42 [https://perma.cc/U9AM-VVVA].

[138] *See* Miranda Bogen, *All the Ways Hiring Algorithms Can Introduce Bias,* HARV. BUS. REV. (May 6, 2019), https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias [https://perma.cc/Y8ED-9HBH]; Julia Powles, *The Seductive Diversion of 'Solving' Bias in Artificial Intelligence*, ONEZERO (Dec. 7, 2018), https://onezero.medium.com/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53 [https://perma.cc/M3GY-PWEL].

[139] CLEARVIEW.AI, https://clearview.ai/ (last visited Oct. 31, 2021).

[140] *See* Mac et al., *supra* note 45.

[141] Ryan-Mosley, *supra* note 51. In the case of the NYPD, Clearview helped many officers install the software on their personal devices, communicating through personal email. *Id.*

adoption of privately controlled tools can give private companies massive influence over public law enforcement policy.[142] In any given use case, Clearview's software exercises incredible power over the investigative process. Police customers are likely unaware of exactly how photo matches are scraped and returned, as well as the reliability of the facial measurements;[143] and yet when there is a match returned, the police immediately have the identity of a suspect—possibly the wrong one.[144] This not to say that Clearview's activity should be considered state action. But the fact that Clearview's sole function is to offer the state a surveillance tool is relevant when assessing its algorithmic output's effects and connection to First Amendment values.

As a tool that may enable remote biometric identification of any citizen with a social media account by law enforcement, Clearview's FRT raises the specter of systemic impacts upon society. Clearview's faceprinting threatens anonymous political speech and intellectual privacy, which, as recognized in Supreme Court precedent and both legal and social science literature, serve core First Amendment ideals. A critical look at the wider social context in which Clearview operates reveals that, instead of furthering free speech values, Clearview's faceprinting undermines them. As such, Clearview's faceprinting has a weak claim to First Amendment protection.

A. Deliberative Democracy and Anonymous Political Speech

Clearview's faceprinting undermines the public's capacity to remain unidentified when engaging in a core First Amendment activity: political speech. The line of Supreme Court cases regarding First Amendment privacy makes clear that the government may not compel a person engaging in political speech or association to give over their identity.[145] For instance, in *McIntyre v. Ohio Elections Commission*, the Supreme Court recognized the importance of public anonymity to political expression.[146] Striking down an Ohio law used to fine someone who had distributed anonymous leaflets regarding a proposed tax levy, the Court recognized anonymity as "a shield

[142] *See generally* Joh, *supra* note 2.

[143] *See* Garvie et al., *supra* note 18 ("The mathematical machinery behind a face recognition algorithm can include millions of variables that are optimized in the process of training. This intricacy is what gives an algorithm the capacity to learn, but it also makes it very difficult for a human to examine an algorithm or generalize about its behavior").

[144] *See* Hill, *supra* note 17.

[145] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995); Talley v. California, 362 U.S. 60, 65 (1960) (striking down state law mandating printing of names on distributed pamphlets).

[146] *McIntyre*, 514 U.S. at 357.

from tyranny of the majority."[147] In *N.A.A.C.P v. Alabama*, the Court invalidated an Alabama state court order requiring the N.A.A.C.P. to produce lists of its participating members.[148] In doing so, it recognized that "[i]nviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."[149] Anonymous political speech, therefore, is connected to the deliberative democracy theory of the First Amendment.

Clearview's faceprinting at the behest of law enforcement presents a clear threat to anonymity. Assuming efficacy, Clearview's tool automatically gives the government the identity of almost anyone it chooses to surveil who has a social media account, as well as whatever other information can be derived from the person's profiles. It represents a loss of "practical obscurity"[150] on a grand scale. The risks that this poses to political expression are not theoretical. There is a long history in the United States of law enforcement surveillance of minority viewpoints, often along racial lines,[151] and this conduct continues today. For example, the Department of Justice (DOJ) recently authorized its Drug Enforcement Agency (DEA) to "conduct covert surveillance" on any individual participating in a protest over the death of George Floyd.[152] Police in Florida flew surveillance drones over a press conference given by an attorney representing families of Black teens killed by law enforcement.[153] One police department authorized FRT searches for "intelligence" purposes at Black Lives Matter protests without any evidence

[147] *Id.*

[148] N.A.A.C.P. v. Alabama, 357 U.S. 449, 466 (1958).

[149] *Id.* at 462.

[150] *See generally* Evan Selinger & Woodrow Hartzog, *Obscurity and Privacy*, ROUTLEDGE COMPANION TO PHIL. OF TECH. (2014).

[151] *See* Alvaro M. Bedoya, *The Color of Surveillance*, SLATE (Jan. 18, 2016), https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html [https://perma.cc/YUC3-3PGD]; 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/7NQS-ACJ6].

[152] Jason Leopold & Anthony Cormier, *The DEA Has Been Given Permission To Investigate People Protesting George Floyd's Death*, BUZZFEED NEWS (June 3, 2020), https://www.buzzfeednews.com/article/jasonleopold/george-floyd-police-brutality-protests-government [https://perma.cc/H4JZ-FHY6].

[153] Joseph Cox, *Florida Cops Flew Spy Plane Above Press Conference for Black Teens Killed by Police*, VICE (Apr. 26, 2021), https://www.vice.com/en/article/qj8pbp/florida-spy-plane-ben-crumps-aj-crooms-sincere-pierce [https://perma.cc/LFV9-882Z]; *see also* Benjamin Powers, *Eyes Over Baltimore: How Police Use Military Technology to Secretly Track You*, ROLLING STONE (Jan. 6, 2017), https://www.rollingstone.com/culture/culture-features/eyes-over-baltimore-how-police-use-military-technology-to-secretly-track-you-126885 [https://perma.cc/YR6B-CTPL].

of criminal wrongdoing.[154] Against this backdrop, Clearview's faceprinting can hardly be seen to further First Amendment values. Its faceprinting more likely does harm to our capacity for deliberative democracy.

B. Autonomy and Intellectual Privacy

On a broader scale, the type of surveillance enabled by Clearview could contribute to chilling effects, such as social conformity and subversion of individual creativity and expression, both online and in the physical world. This is at odds with the autonomy conception of the First Amendment. One way in which it may accomplish this is by invading one's "intellectual privacy."[155] Coined by Neil Richards, intellectual privacy is "the ability . . . to develop ideas and beliefs away from the unwanted gaze or interference of others," which he posits is essential to free expression.[156] While the Supreme Court has not affirmatively recognized chilling effects as judicially cognizable injuries under the First Amendment,[157] it has recognized the importance of freedom of thought and anonymous association.[158] In the Fourth Amendment context, the Court has begun to reckon with the effects of digital information flows on liberty, characterizing certain uses of technology to track criminal suspects as unreasonable "searches" or "seizures" that violate defendants' Fourth Amendment rights.[159] Indeed, as the Court has famously pronounced,

[154] Joanne Cavanaugh Simpson & Marc Freeman, *South Florida police quietly ran facial recognition scans to identify peaceful protestors. Is that legal*? S. FLA. SUN SENTINEL (June 26, 2021), https://www.sunsentinel.com/local/broward/fl-ne-facial-recognition-protests-20210626-7sll5uuaqfbeba32rndlv3xwxi-htmlstory.html [https://perma.cc/63H4-Z4NG].
[155] Neil Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008).
[156] *Id.* at 389.
[157] Laird v. Tatum, 408 U.S. 1, 13–14 (1972) (holding that plaintiffs had no standing to challenge chilling effects from mere knowledge of Army surveillance program); Donohoe v. Duling, 465 F.2d 196, 202 (4th Cir. 1972) (ruling that plaintiffs had no standing to challenge police surveillance program in the absence of testimony establishing that a person's free expression or association rights had actually been chilled).
[158] *See* Stanley v. Georgia, 394 U.S. 557, 564–65 (1969) ("[The] right to receive information and ideas . . . is fundamental to our free society . . . . If the First Amendment means anything, it means that a State has no . . . power to control men's minds."); *N.A.A.C.P.*, 357 U.S. at 462 ("compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as [other forms of censorship].").
[159] *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("[T]he time-stamped data [at issue] provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.' These location records 'hold for many Americans the 'privacies of life.'") (internal citations omitted); Riley v. California, 573 U.S. 373, 386 (2014) (holding unconstitutional a warrantless search of the digital contents of a cell phone); United States v. Jones, 565 U.S. 400, 404 (2012) (holding that police use of a Global Positioning Device to

"[i]f there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion . . . ."[160]

Again assuming accuracy, Clearview's FRT gives the government the ability to identify anyone in public if that person appears in photos on a social media account. Not only can a Clearview user identify someone as they move through a public space equipped with a surveillance camera, but they can also access that person's social media, or the profile in which the subject's picture appears. This could lead to chilling effects both in the physical world and online.

On one hand, people may not wish to be identified in quasi-public places where they access or divulge sensitive information—for example, at AA meetings, abortion clinics, or libraries. Even if not engaging in a "sensitive" activity, mere awareness of being watched can lead people to conform their behavior to group norms. In a well-known experiment conducted by Gregory White and Philip Zimbardo, for example, student responses to whether they believed marijuana should be legalized varied widely depending on whether or not the subjects were told they were being videotaped.[161] Students molded their behaviors to what they perceived to be majoritarian beliefs regardless of their own perception of what was right. Citing these and other studies, Margot Kaminski and Shane Witnov contend that "widespread surveillance, or even the belief in it, is damaging to the development of diverse viewpoints, without any additional clear threat of injury or retaliation."[162] With the capacity to identify anyone in its dataset of billions of photographs, Clearview's faceprinting algorithm allows governments to engage in surveillance that could change individual behavior on a massive scale.

The ease with which Clearview's search engine can return personal information on a person's social media page is significant as well. For example, when the FRT technology is paired with a profile picture taken from LinkedIn, the government can not only learn an individual's name, but also the person's occupation and location of work. If the subject's Facebook or Twitter profile is public, then the police may come to know the person even more intimately by sifting through their photos and digital interactions. Such massive amounts

track movements of a vehicle for 28 days was a search within the meaning of the Fourth Amendment).

[160] W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 642 (1943).

[161] Gregory L. White & Philip G. Zimbardo, *The Effects of Threat of Surveillance and Actual Surveillance on Expressed Opinions Toward Marijuana*, 111 J. SOC. PSYCHOL. 49, 59 (1980).

[162] Margot Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 RICH. L. REV. 465, 499 (2014).

of personal information in the hands of law enforcement could similarly chill behavior online.

In a 2015 study on the effects of data breaches on users' subsequent online activity, 45% of respondents who had experienced a breach of personal information said privacy concerns deterred them from "conducting financial transactions, buying goods or services, posting on social networks, or expressing opinions on controversial or political issues via the Internet . . . ."[163] While this study accounted for leaks of personal information to purveyors of data breaches and not to the government, to the extent one mistrusts law enforcement, the same concerns would seem to be present. In addition, one 2016 study assessed the extent to which concerns about government surveillance in the wake of the Snowden revelations caused Internet users to refrain from accessing information about sensitive topics on Wikipedia.[164] The study found a statistically significant drop in Internet traffic to pages deemed sensitive directly following the leaks, as well as changes to long-term viewing trends, which indicated both immediate and long-term chilling effects.[165] Together these studies show that knowledge of online surveillance can cause users to change their online behavior.

In sum, pervasive surveillance that Clearview enables harms individual autonomy—a core free speech value. Professor Bambauer recognizes this as well, noting that "[i]f we had no control at all over who could observe us, when, or why, our ability to act authentically would be constrained."[166] While Bambauer goes on to contend that these limitations should be addressed at the scrutiny and not the coverage stage, this argument overlooks the power that the First Amendment confers upon activities deemed protected. Once an activity is protected by the First Amendment, no matter the applicable level of scrutiny, regulation of the activity is much more likely to be struck down by a court.

One might wonder whether a computer compilation of facial measurements should be entitled to First Amendment protection because, according to Justice Kennedy in *Sorrell*, "facts . . . are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs."[167] However, instead of adopting the maximalist

[163] Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities,* NTIA (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities [https://perma.cc/5CWB-39K5].

[164] Jonathon Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, BERKELEY L. TECH. J. 117, 123–24 (2016).

[165] *Id.*

[166] Bambauer, *supra* note 114, at 105.

[167] *Sorrell*, *supra* note 71, at 570.

position that almost any information is speech, we should ask better questions about the social context of a given practice and its connection to free speech values. The need for this sort of inquiry is exemplified by the proceedings in Clearview's state court litigation, where the parties and amici almost completely ignored the coverage question. The ACLU did argue that faceprinting is not protected because it is merely functional and not expressive; yet courts have protected search engine results and source code despite the seemingly functional nature of those practices.[168] As Part IV has argued, the better way to resolve the matter is by acknowledging that the systemic effects of this particular FRT do harm to our capacity for deliberative democracy and autonomy.

V. CONCLUSION

This Note first aims to situate coverage as a central component of any First Amendment inquiry and argues that a broader view of social context is needed when determining whether coverage extends to a given activity. Courts can and should consider a purported speech activity's *systemic effects*, as well as whether or not they further free speech values. This allows for a fuller assessment of social context in an age where networked information transmission increasingly pervades normal life.

One particular use of FRT—Clearview's faceprinting—should be excluded from coverage. Specifically, BIPA should not be subject to First Amendment scrutiny in the Clearview case because it does not regulate speech covered by the First Amendment. The faceprinting is not covered because its systemic effects not only bear little connection to First Amendment values, but actually serve to undermine them by subverting our capacity for deliberative democracy and autonomy.

As Alexander Meiklejohn explains in a prominent essay, in adopting the First Amendment, the American people "forbade their legislative agents to use, for the protection of the nation, any limitation of the religious or political freedom of the people from whom their legislative authority was derived."[169] Irrespective of any discrete "speech" right, the amendment was fundamentally concerned with creating a society where government could not impose upon expressive freedom by instituting orthodoxic rule in the name of security.[170]

[168] *See, e.g.*, Jian Zhang v. Baidu.com Inc., 10 F. Supp. 3d 433, 439–40 (S.D.N.Y. 2014) (protecting search engine results); Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426, 1435 (N.D. Cal. 1996) ("[T]he functionality of a [coding] language does not make it any less like speech.").

[169] Alexander Meiklejohn, *What Does the First Amendment Mean?*, 20 U. CHI. L. REV. 461, 464 (1953).

[170] *See id.*

If measurement of facial geometry in service of surveillance is to win First Amendment coverage, the normative justifications must be strong. As this Note has attempted to show, the opposite is true.