Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 32 *XXXII*
Number 4

Article 4

2022

Face the Facts, or Is the Face a Fact?: Biometric Privacy in Publicly Available Data

Daniel Levin

Face the Facts, or Is the Face a Fact?: Biometric Privacy in Publicly Available Data

Cover Page Footnote

* J.D. Candidate, Fordham University School of Law, 2022; B.A., Political Science and Women's & Gender Studies, Rutgers University, 2018. I would like to extend my sincerest gratitude to Olivier Sylvain and Fordham Intellectual Property, Media & Entertainment Law Journal, who oversaw this work's trajectory and provided invaluable insights along the way. I am also indebted to my colleagues' genius at the Electronic Frontier Foundation, Future of Privacy Forum, and Meta's Oversight Board for molding my ever-enduring exercise in thinking.

Face the Facts, or Is the Face a Fact?: Biometric Privacy in Publicly Available Data

Daniel Levin*

Recent advances in biometric technologies have caused a stir among the privacy community. Specifically, facial recognition technologies facilitated through data scraping practices have called into question the basic precepts we had around exercising biometric privacy. Yet, in spite of emerging case law on the permissibility of data scraping, comparatively little attention has been given to the privacy implications endemic to such practices.

On the one hand, privacy proponents espouse the view that manipulating publicly available data from, for example, our social media profiles, derogates from users' expectations around the kind of data they share with platforms (and the obligations such platforms have for protecting users from illicit uses of that data). On the other hand, free speech absolutists take the stance that, to the extent that biometric data is readily apparent in publicly available data, any restrictions on its secondary uses are prior restraints on speech.

This Note proposes that these principles underlying privacy and free speech are compatible. Wholesale bans on biometric technologies misapprehend their legitimate uses for actually preserving privacy. Despite the overwhelming dearth of protections for biometric privacy across the United States, current battles to preserve the few

* J.D. Candidate, Fordham University School of Law, 2022; B.A., Political Science and Women's & Gender Studies, Rutgers University, 2018. I would like to extend my sincerest gratitude to Olivier Sylvain and Fordham Intellectual Property, Media & Entertainment Law Journal, who oversaw this work's trajectory and provided invaluable insights along the way. I am also indebted to my colleagues' genius at the Electronic Frontier Foundation, Future of Privacy Forum, and Meta's Oversight Board for molding my ever-enduring exercise in thinking.

regulations on these data practices illuminate the emerging frontier for privacy and free speech debates.

As this Note concludes, existing regulations on biometric data practices withstand First Amendment scrutiny, and strike the appropriate balance between speech and privacy regulations.

INTRODUCTION

Facebook CEO Mark Zuckerberg ushered in the past decade with an omen: privacy is no longer a social norm.[1] Perhaps more a promise than a prophecy, Zuckerberg's declaration follows a now-

[1] Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, GUARDIAN (Jan. 10, 2010, 8:58 PM), https://www.theguardian.com/technology/2010/jan/11/facebook-privacy [https://perma.cc/RXY2-52RR].

familiar line among technology's giants. He may be right that we no longer take privacy for granted, but by no means was this inevitable. Nor does it follow that users idly capitulated to their privacy's deprivation. On the contrary, platforms disempower users from exercising entitlement over their privacy.[2] They play an indispensable role in shaping our privacy norms, employing covert language that gestures us toward greater disclosures and, by extension, greater insecurities.[3] At a more fundamental level, they contribute powerful interpretations toward otherwise amorphous concepts like "public"

---

[2] *See* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 42 (2018) ("Once design affects our perceptions, it begins to shape our behavior. Once it shapes our behavior, it can be used to control us because it shapes what we perceive as normal. And once norms are established, they are difficult to change."); Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROT. L. REV. 423, 426 (2018) (arguing that service providers use product design to constrain consumer choices).

[3] *See, e.g.*, Helen A.S. Popkin, *Privacy Is Dead on Facebook. Get Over It*., NBC NEWS (Jan. 13, 2010, 8:56 AM), https://www.nbcnews.com/id/wbna34825225 [https://perma.cc/D86R-KG7T] (citing Facebook's previous privacy guide, which provided, "Making connections—finding people you know, learning about people, searching for what people are saying about topics that interest you—is at the core of our product. This can only happen when people make their information available and choose to share more openly."); Anabel Pasarow, *How to Get More Matches on OKCupid, According to an Expert*, REFINERY29 (May 15, 2019, 3:55 PM), https://www.refinery29.com/en-us/okcupid-profile-questions-matches [https://perma.cc/KHE7-MK8W] ("When you add a new picture or a little anecdote, the algorithm treats you like a new user and shows you more people . . . . And the more questions you answer, the more you're improving your chances at making matches, so it's in your interest to answer more questions."); Mary Papenfuss, *Massive Tinder Photo Grab Is Latest Scary Warning to Be Careful What You Post*, HUFFPOST (Apr. 30, 2017, 4:41 AM), https://www.huffingtonpost.in/2017/04/30/massive-tinder-photo-grab-is-latest-scary-warning-to-be-careful_a_22063020/ [https://perma.cc/E6CQ-ESHS] (discussing compilation of a data set used to power a facial recognition program based on data scraped from Tinder); Natasha Singer & Aaron Krolik, *Grindr and OKCupid Spread Personal Details, Study Says*, N.Y. TIMES, https://www.nytimes.com/2020/01/13/technology/grindr-apps-dating-data-tracking.html [https://perma.cc/4WVS-ESJX] (Oct. 14, 2021) (discussing how dating websites solicit questions about recreational drug use, HIV status, and last STI testing date and market user responses to third parties); *Bumble Privacy Policy*, BUMBLE, https://bumble.com/privacy [https://perma.cc/7RUB-RBE6] ("We think our Users are awesome, and we want you to share how awesome you are with the world, so we have built certain features to enable this.…When using the Bumble App, you should assume that anything you post or submit on the App may be publicly-viewable and accessible, both by Users and non-users of the App.").

and "private" information.[4] Yet lay people—even unsuspecting youth—bear the brunt of these norm transformations, making for convenient scapegoats to shield these platforms from accountability.[5]

Against this backdrop, these norms situate a new tale for a new age. Contemporary facial recognition software relies on the breadth of information available on social media networks to generate surveillance technologies.[6] Using sophisticated algorithms, this software collects unprecedented levels of biometric data from our photographs, exceeding the amount of information available in either police departments' or the FBI's existing databases.[7]

---

[4] *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2008) ("Privacy…is a concept in disarray. Nobody can articulate what it means."); Woodrow Hartzog, *The Public Information Fallacy*, 99 B.U. L. REV. 459, 465 (2019) ("[N]obody knows what 'public' means, because it has no set definition in law or policy. Appeals to the public nature of information to justify surveillance and data practices are often just guesswork. At worst, appeals to the public nature of information and acts provide cover for unscrupulous and dangerous data practices and surveillance by making it seem as though there is some objective and established criteria for what constitutes public information. There is no such consensus.").

[5] Privacy norms are often reduced to generational divides. These arguments misconstrue norms' historicity, namely their ability to respond to and emerge from historical forces. This is to say: norms are neither accidental nor incidental; they are deliberate effects predicated on power asymmetries. *See, e.g.*, Emily Nussbaum, *Say Everything*, N.Y. MAG. (Feb. 2, 2007), https://nymag.com/news/features/27341/ (last visited Mar. 19, 2022) ("But in the past ten years, a new set of values has sneaked in to take its place, erecting another barrier between young and old. And as it did in the fifties, the older generation has responded with a disgusted, dismissive squawk. It goes something like this: *Kids today. They have no sense of shame. They have no sense of privacy. They are show-offs, fame whores, pornographic little loons who post their diaries, their phone numbers, their stupid poetry—for God's sake, their dirty photos!—online. They have virtual friends instead of real ones. They talk in illiterate instant messages. They are interested only in attention—and yet they have zero attention span, flitting like hummingbirds from one virtual stage to another*.").

[6] *See, e.g.*, Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, N.Y. TIMES, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/6GVW-UQKL] (Nov. 2, 2021).

[7] In its marketing materials, Clearview AI provides its prospective clients—typically law enforcement agencies—with a chart, demonstrating the extent of searchable photos in its database relative to other prominent agencies. Whereas the FBI contains 411 million searchable photos, Clearview's database contains three *billion* photos. *Id.*; *see also* David Kravets, *Smile, You're in the FBI Face-Recognition Database*, ARS TECHNICA (June 18, 2016, 3:50 PM), https://arstechnica.com/tech-policy/2016/06/smile-youre-in-the-fbi-face-recognition-database/ [https://perma.cc/R54E-CPTW].

The irony is uncanny. Emergent shifts in algorithmic development and machine learning enable companies to manipulate platforms' promises about the accessibility of public information to facilitate surveillance creep. By converting our faces into "facial geometries," these technologies reduce us to calculi that render us both known and knowable.[8] They function to the extent that gaps in privacy law weigh in favor of corporate actors' definitions of public information, allowing near-impenetrable analogies to Google's search features. Indeed, our industry giants reaped what they sowed, laying fertile grounds for more insidious forms of surveillance to pervade our day-to-day experiences and limit our options for refuge.[9] In short, we have internalized surveillance as a norm and quieted the possibility to exercise alternative subjectivities.[10]

Whereas the European Union has established a robust regulatory scheme, culminating with the passage of the General Data Protection Regulation in 2018, the United States remains bereft of any such federal protections. This deficit in protection enables companies to engage in privacy intrusions with relative impunity. For a while, this

---

[8] JOSEPH PUGLIESE, BIOMETRICS: BODIES, TECHNOLOGIES, BIOPOLITICS 112–13 (2010) ("In biometrics, [the] iterable and repeatable identity form can never be identical across each instance of its repetition . . . . In other words, the unique identity biometric of a subject is indissociably tied to iterability, as 'the logic that ties repetition to alterity.'…A subject's biometric 'root identity' is, however, in keeping with the rhetorical effects of this rhizomatic trope, always caught within a transversal movement of iterability that precludes the possibility of an authoritative self-identity not always already marked by difference.").

[9] The late French philosopher, Michel Foucault, provided an astute insight that foreshadowed the scale of mass surveillance today. *See generally* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1977). In *Discipline and Punish*, Foucault employed Jeremy Bentham's architectural design for a prison—popularly known today as the panopticon—to argue that surveillance disciplines us into docility. *Id.* at 184–85 ("The examination combines the techniques of an observing hierarchy and those of a normalizing judgement. It is a normalizing gaze, a surveillance that makes it possible to qualify, to classify and to punish. It establishes over individuals a visibility through which one differentiates them and judges them. That is why, in all the mechanisms of discipline, the examination is highly ritualized. In it are combined the ceremony of power and the form of the experiment, the deployment of force and the establishment of truth. At the heart of the procedures of discipline, it manifests the subjection of those who are perceived as objects and the objectification of those who are subjected. The superimposition of the power relations and knowledge relations assumes in the examination all its visible brilliance.").

[10] Foucault put the matter nicely when he said, "surveillance is permanent in its effects, even if it is discontinuous in its action." *Id.* at 201.

only benefitted companies directly because, as the FTC's enforcement mechanisms demonstrate, the law privileges privacy policies to determine whether companies fulfilled their contractual obligations. In other words, absent federal protections, privacy remains a self-governing regime that allays meaningful choice and enforces a regulative ideal that users can and do read privacy policies, evaluate available choices, and make informed decisions. The reality, to which many can anecdotally attest, is that users do not expend the time or energy to read, let alone understand, privacy policies. More critically, it seems dubious that reading and understanding how platforms collect data will inure to any substantive policy overhauls.[11]

Recognizing the inadequacy of federal protections, states began passing legislation that responded to legitimate concerns about companies' inconspicuous data collection.[12] One such exemplary piece of legislation is Illinois's Biometric Information Privacy Act ("BIPA").[13] BIPA requires that companies receive users' informed consent before processing their biometric data.[14] Unlike many other privacy laws, BIPA does not defer to state attorneys general to forward any litigation. It empowers individuals with a private right of action.[15] But, because BIPA operates within the notice-and-consent regime, it has the inverse effect of incentivizing companies to fabricate users' consent.[16]

---

11 *See* Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1500 (2019) ("[C]onsent regimes burden data subjects with all of the risks of understanding and self-protection while keeping the data machine humming. Consent does not scale without losing its legitimacy. The control that consent regimes promise us ends up being illusory and overwhelming. Even when companies are transparent, it doesn't lead to reform. Big tech platforms and shadowy advertising companies make their fortunes while the rest of us are watched, nudged, exploited, and exposed to data breaches and the manipulation of politics and elections.").

12 *See, e.g.*, TEX. BUS. & COM. CODE § 503.001 (2009); WASH. REV. CODE § 19.375.020 (2017); CAL. CIV. CODE § 1798.140(o)(1)(K)(2) (2018); 740 ILL. COMP. STAT. 14/1 (2008).

13 740 ILL. COMP. STAT. 14/1.

14 740 ILL. COMP. STAT. 14/15.

15 740 ILL. COMP. STAT. 14/20.

16 Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, *in* REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS 96, 103 (Amba Kak ed., 2020), https://ainowinstitute.org/regulatingbiometrics.pdf [https://perma.cc/2J6V-NR66] ("BIPA allows companies to exploit people as their consent is harvested through systems designed to have them hurriedly click 'I Agree' and get on with their busy lives.").

Platforms are now backpedaling their initial investments into privacy deprivation, motivated in part by the diminution of their control over users' public data.[17] In February, Google, YouTube, Venmo, and LinkedIn sent cease-and-desist letters to Clearview AI, alleging that the company violated their terms of use in derogation of their users' privacy expectations by collecting their photos.[18] However, these platforms structured the very norms that enabled Clearview to adopt its verbiage in the first place. Now, they not only struggle to reclaim their monopoly over our information from state regulations, but also from other companies like Clearview, who invert these platforms' promises to further their own ends.[19]

Consumer-focused privacy protections are fighting an uphill battle. Both platforms and their rivals are engrossed in efforts to assert dominion over our public information, deploying an array of legislative and judicial artillery. All the while, our privacy over information—and ourselves—suffers the fate of this attrition warfare. As consumers leverage BIPA against Clearview to redress considerable biometric privacy intrusions, the company elicits

---

[17] *See, e.g.*, Cory Doctorow, *Facebook Is Going After Its Critics in the Name of Privacy*, WIRED (Nov. 20, 2020, 8:00 AM), https://www.wired.com/story/facebook-is-going-after-its-critics-in-the-name-of-privacy/ [https://perma.cc/Q2JY-2QUH].

[18] *Google, YouTube, Venmo and LinkedIn Send Cease-and-Desist Letters to Facial Recognition App that Helps Law Enforcement*, CBS NEWS, https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/ [https://perma.cc/K78W-Z2BQ] (Feb. 5, 2020, 6:52 PM) [hereinafter *Companies' Cease-and-Desist Letters*].

[19] Consumer advocates argue that platforms' recent push for federal privacy laws are less concerned with privacy protections than they are with reinstating platforms' control over their own data collection processes. Their lobbying efforts aim to disempower users from private rights of action and pursue state law preemption in light of recent costly litigation. *See* Bennett Cyphers, *Big Tech's Disingenuous Push for a Federal Privacy Law*, ELEC. FRONTIER FOUND. (Sept. 18, 2019), https://www.eff.org/deeplinks/2019/09/big-techs-disingenuous-push-federal-privacy-law [https://perma.cc/E3WX-PRF2]; *see also* Issie Lapowsky, *Facebook's Plan for Privacy Laws? 'Co-creating' Them with Congress*, PROTOCOL (July 14, 2020), https://www.protocol.com/facebook-privacy-laws-white-paper [https://perma.cc/6YJT-X5D2] ("Facebook pushes for a light-touch approach to privacy regulation that involves maximum input from and flexibility for businesses . . . . It argues, for instance, that the best way to design privacy regulations is through 'policy co-creation,' in which governments and companies work together to prototype policies and test their viability before they're implemented. It makes a case for regulations that 'avoid or remove strict, one-size-fits-all design requirements,' opting instead for laws that 'regulate the process for making privacy design decisions, not the outcome of those processes.'").

constitutional interests to defend its practice, arguing that it has a First Amendment right to public information.[20] What it omits—quite crucially—is what it has a right to do in relationship with that information, and whether that information is truly public.[21] These questions concern more than intellectual fodder; they imagine technology's enduring force to shape legal inquiry.

This Note considers these issues in four parts. Part I provides a theoretical backdrop to privacy and situates overlaps and inconsistencies between privacy literature and its legal counterparts, drawing tensions between privacy norms and judicial interpretations of such norms. Part II describes existing legal infrastructures for data privacy enforcement in the United States and queries the adequacy of such enforcement mechanisms in light of tangible consumer privacy harms. Part III discusses Illinois's Biometric Information Privacy Act, using the legislation as a proxy for describing the importance of and limits to consumer self-help mechanisms to defend their biometric privacy against facial recognition technologies. Part IV analyzes First Amendment concerns relating to data privacy, concluding that biometric data collection exceeds the scope of First Amendment protections on legal and policy grounds.

---

[20] Alfred Ng, *Clearview AI Says the First Amendment Lets It Scrape the Internet. Lawyers Disagree*, CNET (Feb. 6, 2020, 12:13 PM), https://www.cnet.com/news/clearview-says-first-amendment-lets-it-scrape-the-internet-lawyers-disagree/ [https://perma.cc/Q35C-KCQJ].

[21] As this Note argues, the overemphasis on public information suggests a misguided precept about the First Amendment's jurisprudence. It may very well be that "data speaks," but the First Amendment does not protect speech as such; it protects speech relative to its content and context. For a descriptive account of whether data speaks, see Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 70 (2014) ("Data communicates. It tells a narrative just as effectively as prose, imagery, and music to those with the training to interpret it. Its style is dry, but this does not interfere with its ability to light up the mind. A database can be interpreted directly by a person with the help of a codebook, and it can also be translated into other more familiar forms of expression like maps, charts, graphs, and descriptive sentences. Lest there be any doubt about data's intimate connection to other forms of expression, one may recall that the very first form of writing was data: the accounting records of traders in ancient Mesopotamia. Data provided the building blocks of the rest of written language.").

I. PRIVACY NORMS, INVASIVE TECHNOLOGIES

Privacy scholarship carries a longstanding history in the United States. In 1890, Samuel Warren and Louis Brandeis published their seminal article, *The Right to Privacy*, which laid the foundation for modern privacy law.[22] Establishing privacy as "the right to be let alone,"[23] Warren and Brandeis mounted an assault against rampant intrusions by the press.[24] While their concerns may be read as universal, a more honest reading reveals their defense of a high-class sensibility.[25] By disclosing the province of their solitude, the press revealed more than the wealthy's lavish fineries; it offered a glimpse into precisely what made them like everyone else.[26]

Warren and Brandeis's lasting legacy is owed to more than their genius. *The Right to Privacy* set the stage for contemporary privacy issues. It alluded to an inversion of matters' relative importance, where the disclosure of otherwise trivial things garnered the public's attention.[27] For Warren and Brandeis, such disclosures do not merely respond to moral values and social standards; they also inform them.[28]

---

[22] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). *Cf.* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960) (laying the foundation for four privacy torts).

[23] Warren & Brandeis, *supra* note 22, at 195.

[24] *Id.* at 196 ("The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery.").

[25] *See* ARI WALDMAN, PRIVACY AS TRUST 16 (2018); Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 VAND. L. REV. 1295, 1301 (2010) ("Old norms of deference and respect seemed under assault, and there was great anxiety among elites keen on protecting their status, authority, and privacy.").

[26] Warren & Brandeis, *supra* note 22, at 196 ("To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle.").

[27] *Id.* ("In this, as in other branches of commerce, the supply creates the demand. Each crop of unseemly gossip, thus harvested, becomes the seed of more, and, in direct proportion to its circulation, results in a lowering of social standards and of morality. Even gossip apparently harmless, when widely and persistently circulated, is potent for evil. It both belittles and perverts. It belittles by inverting the relative importance of things, thus dwarfing the thoughts and aspirations of a people. When personal gossip attains the dignity of print, and crowds the space available for matters of real interest to the community, what wonder that the ignorant and thoughtless mistake its relative importance.").

[28] *Id*.

But Warren and Brandeis's conception of privacy—much like all conceptions of privacy—engendered particular norms.[29] Indeed, any meaningful engagement with privacy must not only ask what privacy *is*, but also what privacy *does*.[30] Competing understandings of privacy do not emerge for purely intellectual inquiry. Rather, they seek to enable certain rights for some at the expense of others.[31]

In her recent work, Susan Hazeldean identified a diversity of current philosophical conceptions of privacy.[32] Among them, she considered privacy as: a "right to be let alone";[33] a means to limit access to the self;[34] a safeguard of intimacy;[35] a right to control information;[36] a defense for personhood;[37] and protection for social networks.[38] In addition to Hazeldean's succinct yet comprehensive

---

29 *See* WALDMAN, *supra* note 25, at 16.

30 *See* Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1155 (2005) (noting that the right to privacy has been "poorly articulated" and "vaguely theorized," resulting in incoherent definitions of privacy).

31 *See generally* Susan V. Hazeldean, *Privacy as Pretext*, 104 CORNELL L. REV. 1719 (2019) (arguing that privacy has historically been used to justify unequal treatment of women and LGBTQ people). It helps to illustrate this historical element of privacy further. In *State v. Rhodes*, the court refused to indict a man for striking his wife several times without provocation, finding that courts should refrain from interfering with domestic affairs, including domestic violence. 61 N.C. 453, 454–55 (1868). The court recognized the sovereignty of the marital unit, calling it a "family government . . . as complete in itself as the State government is in itself." *Id.* at 456. In their reasoning, they determined that the "evils of ill temper" cannot compare with "the evils which would result from raising the curtain, and exposing to public curiosity and criticism, the nursery and the bed chamber." *Id.* at 457. They considered their ruling to favor neither husband nor wife, and to preserve the "modesty and purity" of the middle class, asking, "[w]hat could be more harassing to them, or injurious to society, than to draw a crowd around their seclusion?" *Id.* at 458. Although the case bears little significance today, it is useful to consider how courts have weaponized privacy to reify existing social norms and produce privacy winners and losers.

32 *See* Hazeldean, *supra* note 31, at 1721.

33 Warren & Brandeis, *supra* note 22, at 195.

34 Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423 (1980).

35 Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 280 (1977).

36 ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967); *see also id.* at 24–25 ("Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.").

37 J. Braxton Craven, Jr., *Personhood: The Right to Be Let Alone*, 1976 DUKE L.J. 699, 702 (1976).

38 Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 970 (2005).

list, privacy has also been popularly understood as contextual.[39] These theories of privacy function as more than abstract inquiries. They determine how we operate under given circumstances[40] and represent an affirmative commitment to self-determination; that is, they calculate the parameters of how we render ourselves both legible and intelligible to others.[41] But they also calibrate the extent of how we define ourselves to others.

In this sense, it may be untenable to consider how privacy preserves a unified "self." As Jeffrey Rosen wrote:

> Privacy protects us from being misdefined and judged out of context in . . . a world in which information can easily be confused with knowledge. True knowledge of another person is the culmination of a slow process of mutual revelation.[42]

We curate images of ourselves to show to others, but it seems doubtful that every person with whom we interact shares the same understanding of who we are. Our colleagues, friends, families, and lovers each conceptualize us based on their unique evaluations of our interactions with them and others, as well as our recreational interests and professional endeavors, to name a few.[43] To the extent that we

---

[39] SOLOVE, *supra* note 4, at 9; *see also id.* at 98 ("By understanding privacy as shaped by the norms of society, we can better see why privacy should not be understood solely as an individual right . . . . Instead, privacy protects the individual because of the benefits it confers on society.").

[40] WESTIN, *supra* note 36, at 7 ("Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.").

[41] *See* Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 989–1000 (2003) (discussing how privacy protections advance the interests of individual autonomy, democratic self-governance, and the marketplace of ideas).

[42] JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 8 (2000).

[43] *See* Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, 6 PHIL. & PUB. AFFS. 26, 30 (1976) ("One shares more of himself with a friend than with an employer, more with a life-long friend than with a casual friend, more with a lover than an acquaintance."). Reiman's construction of how we exercise discretion over who may know "more" about us offers a valuable contribution, though I argue that it misapprehends the prevailing qualitative nature of information-sharing. For example, modern dating applications have internal cultures that circumscribe their respective privacy norms. We would not ordinarily consider sharing romantic or sexual affinities part of our common parlance—at least among

are constituted through these social relations, it makes more sense to consider privacy as a precursor to defining and maintaining our "selves."[44]

Over a century ago, Warren and Brandeis foresaw the precise question that burdens the current privacy debate: to how much privacy are we entitled without interfering with the freedom of speech and expression? For them, the inversion of relative importance through publication in the press ascribed too much value to matters of a trivial nature. They wrote, "[w]hen personal gossip attains the dignity of print . . . no one can be surprised that it usurps the place of interest in brains capable of other things. Triviality destroys at once robustness of thought and delicacy of feeling."[45] In short, privacy enables the precondition for thinking, such that meaningful expression becomes possible.[46] Neil Richards popularly termed this phenomenon "intellectual privacy," arguing that "[t]he ability to freely make up our minds and to develop new ideas . . . depends upon a substantial measure of intellectual privacy."[47]

But there is also another component in Warren and Brandeis's argument that contributes to intellectual privacy. Thinking—or worrying—about a lack of privacy requires substantial mental expenditure. The time and energy spent thinking about whether we should speak could be invested into other life-enriching pursuits. The Supreme Court's recent decision in *Carpenter v. United States* echoed these concerns, determining that "pervasive, persistent surveillance even of noncontent communications information such as location

close friends and family—yet it may be precisely because we retain privacy from those friends and family that we divulge these things to potential suitors.

44 *See id.* at 39 ("*Privacy is a social ritual by means of which an individual's moral title to his existence is conferred.* Privacy is an essential part of the complex social practice by means of which the social group recognizes—and communicates to the individual—that his existence is his own . . . . [P]rivacy is necessary to the creation of *selves* out of human beings, since a self is[,] at least in part[,] a human being who regards his existence—his thoughts, his body, his actions—as his *own*.").

45 Warren & Brandeis, *supra* note 22, at 196.

46 *See* Jeffrey Rosen, *What Would Privacy Expert Louis Brandeis Make of the Digital Age?*, WASH. POST (Mar. 20, 2015), https://www.washingtonpost.com/opinions/clash-between-free-speech-and-privacy-in-the-digital-world/2015/03/20/bee390e6-c0f8-11e4-ad5c-3b8ce89f1b89_story.html [https://perma.cc/QZ6L-NZNC].

47 Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 389 (2008).

information can chill 'familial, political, professional, religious, and sexual associations.'"[48]

Carpenter reanimated the spirit of an unsuspecting guest: Louis Brandeis. The Court's concern against government surveillance harkened back to Brandeis's famed dissent in *Olmstead*.[49] There, he wrote:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.[50]

Although *Carpenter* and *Olmstead* concerned privacy's relationship to the Fourth Amendment, their discussions of privacy hold salience for contemporary debates over the First Amendment, as well.

Indeed, Brandeis's earlier preoccupation with privacy from the press presents a quandary for which he became equally reputed in defending freedom of speech.[51] Scholars credit Brandeis's concurrence in *Whitney v. California*[52] with forming modern First Amendment theory.[53] As he wrote, "[i]f there be time to expose through discussion the falsehood and fallacies, to avert the evil by the

---

48 Margot E. Kaminski & Scott Skinner-Thompson, *Free Speech Isn't a Free Pass for Privacy Violations*, SLATE (Mar. 9, 2020, 2:53 PM), https://slate.com/technology/2020/03/free-speech-privacy-clearview-ai-maine-isps.html [https://perma.cc/854S-7D5T] (quoting Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018)).

49 Olmstead v. United States, 277 U.S. 438, 471 (1928) (Brandeis, J., dissenting).

50 *Id.* at 478.

51 *See generally* Richards, *supra* note 25.

52 274 U.S. 357, 372 (1927) (Brandeis, J., concurring).

53 *See, e.g.*, NEIL M. RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 60 (2015); ANTHONY LEWIS, MAKE NO LAW: THE SULLIVAN CASE AND THE FIRST AMENDMENT 85 (2015); Vincent Blasi, *The First Amendment and the Ideal of Civic Courage: The Brandeis Opinion in* Whitney v. California, 29 WM. & MARY L. REV. 653, 668 (1988).

process of education, the remedy to be applied is more speech, not enforced silence."[54] For Brandeis, speech begets speech; it contributes to the marketplace of ideas where the possibility for truth can emerge. In view of his opinions in *Olmstead* and *Whitney*, it becomes clear that, for as much as Brandeis may have pinpointed the tension between privacy and the First Amendment, he could not have foreseen the conflict to define speech today, let alone its overlap with attendant privacy concerns.

As he noted in *Olmstead*, "in the application of a Constitution, our contemplation cannot be only of what has been, but of what may be."[55] By employing normative conventions around privacy, Brandeis gestured future decisions to consider the implications of permitting the law to enable certain privacy intrusions. He appealed to judicial foresight that begs inquiry into the nature of surveillance mechanisms and their coinciding privacy harms. However, while the law lags behind emerging norms, it simultaneously maintains or circumscribes others.[56] In this way, surveillance technology pursues the institutionalization of its norms through judicial action, giving legitimacy to its privacy intrusions. From this, we can understand courts' analyses of a "reasonable expectation of privacy" as a concession to surveillance technologies' dominion over ourselves. Their more pernicious effects will take hold by tethering norms to antiquated case law, construing new privacy intrusions into old constitutional mandates.[57] While companies abuse the law to their benefit, users' claims to their own personhood remain at stake.

II. THE LIMITS TO EXISTING PRIVACY ENFORCEMENT MECHANISMS

The United States relies on two primary privacy enforcement mechanisms. At the state level, state attorneys general occupy the confines of their particular jurisdictions and bring suits on behalf of aggrieved parties. At the federal level, the Federal Trade Commission ("FTC") polices companies' anticompetitive practices and

---

54 *Whitney*, 274 U.S. at 377.

55 *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting) (internal quotations omitted).

56 *See* Cass R. Sunstein, *On the Expressive Function of Law*, 144 U. PA. L. REV. 2021, 2022 (1996).

57 For a more thorough discussion of this trend, see *infra* Part IV.

ensures they fulfill their promises, typically enumerated in privacy policies. Neither entity addresses individual consumers' grievances, only their privacy incursions at large. With little means for individual redress, consumers are often disempowered from substantive changes in privacy law. This Part provides a brief overview of these concerns and pivots to the need for self-help mechanisms through private rights of action.

A. State Attorneys General

Dubbed the "people's privacy lawyers,"[58] state attorneys general ("AGs") investigate and litigate data security concerns relating to existing state and federal regulations.[59] Although state AGs are empowered to enforce state and federal privacy laws, they are limited to the laws—or safeguards—of their jurisdiction. In the earlier days, as Joel Reidenberg claimed, public enforcement looked to "data security as a proxy for wrongful disclosures of personal information."[60] In other words, rather than targeting a wrongful disclosure itself, state AGs only addressed the violation of companies' promises "to treat personal information with adequate security measures."[61] Their reliance on "creative, tertiary theories for privacy claims"—often the theory of "unfair trade practice"—failed to address underlying public wrongs, such as profiling and stereotyping individuals on the basis of such data and data breaches.[62]

Because of their narrow jurisdiction, though, state AGs enjoy more particular insights about local conditions than their federal counterparts.[63] Danielle Citron's account exalts states' specializations in discrete privacy realms.[64] Despite her allusion to Illinois's specialty in identity theft and data security, she made no explicit

---

58 Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 752 (2016).

59 *See id.* at 761.

60 Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 886 (2003).

61 *Id.* at 887.

62 *Id*. Using the New York AG as an example, Reidenberg noted an instance where the Attorney General attacked a student marketing company's data gathering practice rather than addressing that the company trafficked children's data. *Id.*

63 *See* Citron, *supra* note 58, at 786.

64 *See id.* at 786–90 (discussing individual states' sectorial expertise).

mention of any state's biometric privacy protections.[65] Rather than warrant their own expertise, biometrics fall within existing categories of data privacy and protection. Texas and Washington, for example, authorize their state AGs to enforce biometric privacy laws similar to how states enforce general data privacy rules.[66]

State AGs make for zealous consumer advocates, but they experience significant limitations to their effectiveness. For one, states have to share the burdens of litigation out of a dearth of resources.[67] With burden-sharing comes the risk of budget cuts or potential limits to their enforcement powers.[68] Industry lobbying efforts will not only pursue limiting state AGs substantive powers, but also their procedural powers through federal law preemption.[69] And, as federal lawmakers pursue slashing the FTC's budget, they complete a vicious cycle that may overwhelm already under-resourced offices.[70]

B. Federal Trade Commission

The FTC enforces federal data privacy legislation and develops policies that protect consumers from unfair and deceptive practices while preserving competition and legitimate business activity.[71] Established in 1914, the FTC began as a trust-busting agency to police anticompetitive practices.[72] In 1938, Congress passed a sweeping prohibition against "unfair and deceptive practices," turning the FTC into the largest proprietor for consumer protection.[73]

---

65 *See id.* at 788.

66 Hartzog, *supra* note 16, at 97.

67 Citron, *supra* note 58, at 796–97.

68 *Id.* at 797 (noting industry lobbying efforts to limit state attorneys general privacy and data security enforcement powers).

69 *See id.* at 798.

70 *See id.* at 800; *see also* Alex Kantrowitz, *Internal FTC Memo Announces Major Cuts Ahead of Tech Giant Action*, ONEZERO (Nov. 19, 2020), https://onezero.medium.com/internal-ftc-memo-announces-major-cuts-ahead-of-tech-giant-action-8edb84fa5c69 [https://perma.cc/R5UV-SX7J].

71 *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc [https://perma.cc/3FST-SEX5].

72 *Id.*

73 *Id.*

As commerce quickly turned to the internet in the 1990s, the FTC "expanded its focus on privacy to reflect the growing collection, use, and sharing of consumer data in the commercial marketplace."[74] Today, the FTC brings enforcement actions to "stop law violations and require companies to take steps to remediate the unlawful behavior," which mostly focus on protecting U.S. consumers, though they may also extend protection to foreign consumers, as well.[75] Specifically, Section 5 of the FTC Act prohibits "deceptive or unfair commercial practices."[76] A representation, omission, or practice is deceptive "if it is likely to mislead consumers acting reasonably under the circumstances and is material to consumers."[77] A practice is unfair if (1) it "causes or is likely to cause substantial injury"; (2) the injury is "not reasonably avoidable by consumers"; and (3) the injury is "not outweighed by benefits to consumers or competition."[78]

Apart from the FTC Act, the agency enforces other privacy laws, including protecting consumers' financial information, ability to opt out of commercial e-mail messages, and children's online privacy.[79] However, the FTC continues to experience significant limitations on its enforcement powers. For example, Section 5 does not allow the FTC to seek civil penalties for first-time offenses, which risks disabling the agency's enforcement ability in the event of an adverse

---

74 FED. TRADE COMM'N, FTC'S USE OF ITS AUTHORITIES TO PROTECT CONSUMER PRIVACY AND SECURITY 1 (2020), https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportprivacydatasecurity.pdf [https://perma.cc/RM9U-RDQE] [hereinafter FTC 2020 REPORT].

75 *Id.* at app. at 1. Notably, on July 24, 2019, the FTC and U.S. Department of Justice settled a claim against Facebook, alleging that the social media platform mispresented the extent of control users had over their personal information and failed to adequately safeguard such information. *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FED. TRADE COMM'N (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook [https://perma.cc/U9ND-36T2]. They also alleged that Facebook used users' phone numbers for targeted advertisements. *Id.* The case settled for $5 billion, becoming the largest penalty ever imposed on any company for violating consumers' privacy. *Id.*

76 FTC 2020 REPORT, *supra* note 74, at 1 (citing 15 U.S.C. § 1681).

77 *Id.* at 2 (citation omitted).

78 15 U.S.C. § 45(n).

79 FTC 2020 REPORT, *supra* note 74, at 5 (citations omitted).

determination.[80] Section 5 also excludes non-profits and common carriers from the agency's authority, even when these entities' acts implicate serious privacy concerns.[81] Finally, the agency lacks rule-making authority under the Administrative Procedure Act, stifling the agency's ability to make rules quickly.[82] As a result, the agency fills in its "regulatory gaps" with consent decrees, which provide a number of compliance requirements to specific companies.[83] These consent decrees have come to constitute a common law of privacy jurisprudence around unfair and deceptive practices.[84]

In assessing unfair and deceptive practices, the FTC adheres to the now-dominant legal regime for data privacy in the United States: notice-and-consent.[85] This regime requires websites and platforms notify users of their data practices—usually through their privacy policies—and that users agree to those terms to use their services.[86] Accordingly, the FTC looks to whether a company broke its promise to consumers rather than whether the company's data practice itself was either unfair or deceptive.[87]

By giving primacy to privacy policies, the agency recapitulates two critical issues in consumer data privacy. First, users seldom read privacy policies, let alone understand them.[88] In a study conducted by Carnegie Mellon University, researchers approximated that it would take an average person seventy-six full working days per year

---

80 *Id.* at 7.

81 *Id.* at 8.

82 *Id.* at 7.

83 JULIE COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 188 (2019).

84 *See generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

85 *See generally* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf [https://perma.cc/6XFM-AV39] [hereinafter FTC FAIR INFORMATION PRACTICES REPORT].

86 *Id.*

87 *See* Ari Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 129, 141–42 (2018) (discussing how the FTC's broken promises litigation is based on the "substantive disclosures" in a privacy policy).

88 *Cf.* Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39, 87 (2015) (concluding that privacy policies are ambiguous on key terms).

to read every privacy policy applicable to them.[89] In another survey, the Pew Research Center found that over half of internet users believe—incorrectly— that privacy policies ensure data confidentiality.[90] Because most users neither read nor understand privacy policies, their consent is often ill-informed.[91] It also risks undermining the FTC's requirement for websites to provide consumers with clear and conspicuous notice of their information practices.[92]

Second, and relatedly, the FTC defers to company's policy terms, which bear little input from key stakeholders, namely consumers. Consumers are often unable to exercise meaningful choice over websites' data practices, turning privacy policies into adhesion contracts.[93] However, the bulk of legal theories underlying contract law disfavor consumer protections. In the few instances where consumers alleged privacy harms spawning from privacy policies, their contract claims failed for lacking detrimental reliance, especially in light of their failure to read the policies themselves.[94] Because FTC enforcement actions only target these policies' terms, the agency reinforces power asymmetries between companies and consumers. Its status as our de facto privacy regulator is, at best, incomplete.[95]

---

[89] *See* Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, ATLANTIC (Mar. 1, 2012), https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851 [https://perma.cc/9YST-59LH]; *see also* Aleecia McDonald & Lorrie Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J. OF L. & POL'Y 540 (2008).

[90] Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RSCH. CTR. (Dec. 4, 2014), https://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/ [https://perma.cc/EA6J-VBWD].

[91] Daniel Susser, *Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworkers Aren't*, 9 J. INFO. POL'Y 148, 155–56 (2019).

[92] *See* FTC FAIR INFORMATION PRACTICES REPORT, *supra* note 85, at iii; *see also* Reidenberg et al., *supra* note 88, at 40 ("[A]mbiguous wording in typical privacy policies undermines the ability of privacy policies to effectively convey notice of data practices to the general public.").

[93] *See* Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP. 1, 14 (2009).

[94] Solove & Hartzog, *supra* note 84, at 596.

[95] *See* CHRIS J. HOOFNAGLE, FEDERAL TRADE COMMISSION AND PRIVACY LAW 119–23 (2016); Solove & Hartzog, *supra* note 84, at 599–600; Steven Hetcher, *The* De Facto *Federal Privacy Commission*, 19 J. MARSHALL J. COMPUT. & INFO. L. 109, 131 (2000).

C. *Inadequacies for Protecting Consumers*

State AGs and the FTC can only offer limited protections for consumer data privacy.[96] Their efforts largely operate within existing legal infrastructures captured by corporate interests in self-regulation. Where enforcement prevails, it falls short of providing individual victims with any real remedies.[97] As Woodrow Hartzog noted, building biometric privacy frameworks around concepts of transparency and informational self-determination feign the impression that consumers harness autonomy in their online interactions.[98] However, when platforms limit choice availability—or, worse, obscure choices that are otherwise available[99]—neither AGs nor the FTC can signal particular harms.[100] Our existing notice-and-consent regime turns informed consent into a platitude, allocating risk management to consumers whose choices are ill-defined and illusive.[101] Incumbent pressures to assimilate into contemporary social life

---

[96] *See* Ari Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 783–84 (2020) ("FTC commissioners and state AGs share one essential quality: they are charged with public governance and social welfare functions. But, in reality, many legal policy decisions are made by social groups far from those charged to protect citizens. Online platforms employ armies of content moderators to negotiate internal speech rules and make fair use determinations in copyright law. We outsource constitutional responsibilities to police officers, who make practical interpretations of search and seizure law in the moment. Catherine Crump argues that surveillance policy is made by vendors hired by the government. We are increasingly outsourcing judicial decision-making to mediators and arbitrators who hear evidence, consider legal arguments, and issue binding orders. And CPOs, lawyers, and compliance personnel create an internal 'company law' of privacy.") (internal citations omitted); *see also* Richards & Hartzog, *supra* note 11, at 1499 ("The FTC has made a heroic effort to be the top U.S. privacy cop, but it has been starved of the legal tools and financial resources it needs to do a proper job.").

[97] Reidenberg, *supra* note 60, at 878.

[98] Hartzog, *supra* note 16, at 102.

[99] For discussions of user interface designs that deceive users into making unintended, harmful choices, see Arunesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 PROC. ACM HUM.-COMPUT. INTERACTION, Nov. 2019, art. no. 81; *see also* Ari Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox*,*'* 31 CURRENT OP. PSYCHOLOGY 105 (2020).

[100] Hartzog, *supra* note 16, at 102 ("[B]y focusing on giving people control over their data and mandating procedural disclosure obligations, these frameworks fail to impose substantive limits on how far companies can encroach into our lives and how deeply these systems can be entrenched. Procedural transparency and consent regimes end up serving as a justification mechanism for all kinds of encroachments without any clear backstop to how vulnerable we can be made to these systems, so long as we consent.").

[101] *Id.* at 103.

online make regrettable choices inescapable and meaningful choices nearly impossible.[102]

We can situate the FTC's deference to privacy policies' terms within a larger legal infrastructure beholden to the wrong kinds of private interests. Principally concerned with stifled innovation and anticompetitive activity, the FTC maintains its legitimacy to the extent that it merely enforces companies' promises.[103] But privacy policies represent an "uncontract" that signifies a unilateral—and unequivocal—right to dispense users' information at will.[104] Importantly, whereas Shoshana Zuboff considered these phenomena beyond the scope of law,[105] legal scholars have argued that these agreements represent acts of legal entrepreneurship.[106] They rely on an oeuvre of antiquated corporate-protective norms that privilege unilateral contracts whose terms shy from consumers' entitlements to privacy and license extensive data appropriation.[107]

---

[102] Richards & Hartzog, *supra* note 11, at 1463 (likening the notice-and-consent regime to a "take-it-or-leave-it" approach).

[103] *See* Solove & Hartzog, *supra* note 84, at 604.

[104] *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 220–21 (2019) ("The uncontract is not a space of contractual relations but rather a unilateral execution that makes those relations unnecessary. The uncontract desocializes the contract, manufacturing certainty through the substitution of automated procedures for promises, dialogue, shared meaning, problem solving, dispute resolution, and trust: the expressions of solidarity and human agency that have been gradually institutionalized in the notion of 'contract' over the course of millennia. The uncontract bypasses all that social work in favor of compulsion, and it does so for the sake of more-lucrative prediction products that approximate observation and therefore guarantee outcomes.").

[105] *Shoshana Zuboff on the Age of Surveillance Capitalism*, CONTAGIOUS (Sept. 16, 2019), https://www.contagious.com/news-and-views/shoshana-zuboff-on-the-age-of-surveillance-capitalism [https://perma.cc/HEX8-LYPX] ("Law trails behind the market because the market moves into lawless space. That's the whole idea of: 'We took nature because there were no laws to protect nature because no one thought it could be taken.' There were no laws to protect private human experience because no one thought it could be taken.").

[106] *See, e.g.*, Julie Cohen, *Review of Zuboff's* The Age of Surveillance Capitalism, 17 SURVEILLANCE & SOC'Y 240, 241 (2019); Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460, 1465 (2020).

[107] *See* Cohen, *supra* note 106 ("Terms-of-use agreements are performative acts of consummation. Together with the technical protocols that structure interactions with platforms and other information services, they work to leverage ad hoc and contingent trade secrecy entitlements into de facto property arrangements.").

By turning our data into raw material for profit extraction, private companies engage in market analytics that form the logical extension of commodity fetishism.[108] They also embroil themselves in battles to maximally exploit the value in our personal data, all the while exposing us to extensive vulnerabilities.[109] Using predictive algorithms, these data analyses provide more than passive determinations; they provoke certain responses that divorce us from contexts that otherwise elicit human decisional conflicts in the first place. Put differently, recent analytics efforts pitch us contexts that ensure specific behavioral responses.

Inadequate legal infrastructures are part and parcel of the broader political economy that enables corporate actors to operate under the law.[110] As Ari Waldman argues, privacy law reaches its apex when judges, lawyers, and scholars defer to symbolic structures—appointing compliance officers, conducting data risk assessments and impact evaluations, and automating data breach notifications—as evidence of adherence to the law.[111] All the law does, then, is transfer regulatory monitoring to companies themselves, wedding a form of collaborative governance that shifts compliance enforcement out of regulators' hands. Symbolic compliance becomes compliance for its own sake; it permits regulators to avert their attention from companies' more deleterious practices. Without this trustworthy allegiance, consumers are forced to engage in legal self-help through private rights of action.

---

[108] ZUBOFF, *supra* note 104, at 8 ("Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioural data . . . [which] are declared as a proprietary behavioural surplus, fed into advanced manufacturing processes known as 'machine intelligence', and fabricated into prediction products that anticipate what you will do now, soon, and later.").

[109] *See supra* note 3 and accompanying text.

[110] *See* Kapczynski, *supra* note 106, at 1515 ("Our legal order, intertwined with the architecture of digital networks, has enabled the creation of vast new firms that wield new forms of surveillance and algorithmic power, but it also has delivered us a form of neoliberal capitalism that is inclined toward monopoly, concentrated power, and inequality. Most troubling are the developments in takings law, free speech law, and free trade law that are working to insulate growing private economic and surveillance power from democratic control.").

[111] *See* Waldman, *supra* note 96, at 815.

III. BIOMETRIC INFORMATION PRIVACY ACT: A HISTORY

Currently, there are no federal safeguards for biometric data.[112] In the absence of such protections, states are left to their own devices to determine adequate precautions and enforcement mechanisms for protecting such data, turning them into laboratories for "novel social and economic experiments without risk to the rest of the country."[113] As a result, the United States hosts a hodgepodge of inconsistent legal infrastructures, forcing government agencies and private entities to resort to self-regulation.[114] To put it into perspective, it is currently legal in forty-five states to use software to identify an individual using images taken without consent while the individual is in public.[115] The remaining five states—New York, California, Washington, Illinois, and Texas—ban using this software for commercial purposes.[116]

In 2008, Illinois became the first jurisdiction to offer comprehensive protection for biometric data. With its passage, BIPA[117] became the archetype for biometric privacy law.[118] BIPA regulates private actors' collection of biometric identifiers and information.[119] Under BIPA, a "biometric identifier" refers to a retina or iris scan,

---

112 *See* Carra Pope, Note, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, 26 J.L. & POL'Y 769, 770 (2018); *see also* Matt Laslo, *Hey Congress, How's That Privacy Bill Coming Along?*, WIRED (Nov. 29, 2019, 7:00 AM), https://www.wired.com/story/congress-privacy-bill-copra/ [https://perma.cc/2C5P-K64F] (describing the Senate-proposed Consumer Online Privacy Rights Act).

113 Susan Crawford, *Facial Recognition Laws Are (Literally) All Over the Map*, WIRED (Dec. 16, 2019, 8:00 AM), https://www.wired.com/story/facial-recognition-laws-are-literally-all-over-the-map/ [https://perma.cc/SEW6-DBSX] (quoting New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting)).

114 *Biometric Data and Privacy Laws (GDPR, CCPA/CPRA)*, THALES, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data [https://perma.cc/GY29-LJSS] (June 16, 2021).

115 *Id.*

116 *Id.*

117 740 ILL. COMP. STAT. 14/1 (2008).

118 Jane Bambauer, *Biometric Privacy Laws: How a Little-Known Illinois Law Made Facebook Illegal*, ANTONIN SCALIA L. SCH. PROGRAM ON ECON. & PRIV., https://pep.gmu.edu/wp-content/uploads/sites/28/2017/06/Biometric-Privacy-Laws-FINAL_really_6.20-.pdf [https://perma.cc/9UAL-XCG8].

119 740 ILL. COMP. STAT. 14/5(g).

fingerprint, voiceprint, or scan of one's hand or face geometry.[120] Before collecting biometric information, private entities must inform individuals in writing that their biometric information is being collected, and disclose the purpose and length of time for which such information is being obtained.[121] Companies must also receive written consent from consumers, authorizing the private entity to collect that data for any specified purposes.[122] Finally, BIPA prohibits the profiteering of biometric information[123] and mandates guidelines for destroying the information once its original purpose for collection expires.[124]

BIPA protects individuals from the "surreptitious and nonconsensual capture of their biometric identifiers, including faceprints."[125] In doing so, the legislature identified the especially precarious nature of biometric data.[126] As written in the statute:

> Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse [and] is at heightened risk for identity theft . . . .[127]

Senator Al Franken reiterated these concerns during the hearing of the Senate Judiciary Subcommittee on Privacy, Technology and the Law, where he discussed the implications of facial recognition technologies for privacy and civil liberties.[128] Specifically, he stated:

---

120 740 ILL. COMP. STAT. 14/10.

121 740 ILL. COMP. STAT. 14/15(b).

122 *Id.*

123 740 ILL. COMP. STAT. 14/15(c).

124 740 ILL. COMP. STAT. 14/15(a).

125 Elizabeth Montalbano, *ACLU Sues Clearview AI Over Faceprint Collection, Sale*, THREATPOST (May 29, 2020, 8:40 AM), https://threatpost.com/aclu-sues-clearview-ai-over-faceprint-collection-sale/156117/ (last visited Apr. 19, 2022) (quoting ACLU complaint against Clearview AI).

126 740 ILL. COMP. STAT. 14/5(c).

127 *Id.*

128 *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Priv., Tech. and the Law of the Comm. on the Judiciary*, 112th

> biometric information is already among the most sensitive of our private information, mainly because it is both unique and permanent. You can change your password. You can get a new credit card. But you cannot change your fingerprint, and you cannot change your face—unless, I guess, you go to a great deal of trouble.[129]

Unlike other forms of private data, biometrics are inherent to personhood.[130] They are, in short, our most immediate interface with the world. "Your face," as Senator Franken notes, "is a conduit to an incredible amount of information about you, and facial recognition technology can allow others to access all of that information from a distance, without your knowledge, and in about as much time as it takes to snap a photo."[131] That our faces may be subject to theft is no small tribulation. Nor does it amount to undue hysteria.[132] In 2019, the biggest known biometric data breach to date compromised a twenty-three gigabyte database containing nearly thirty-million records, including fingerprint and facial biometric data.[133] The

---

Cong. 1 (2012) (opening statement of Senator Al Franken) [hereinafter Hearing on FRT and Privacy].

[129] *Id.* Although Senator Franken does not explicitly name it, the relationship between facial recognition technology and facial reconstructive surgery has yielded considerable scholarship in recent years. For a more thorough discussion, see generally Kevin J. Zuo et al., *Facial Recognition Technology: A Primer for Plastic Surgeons*, 143 PLASTIC & RECONSTRUCTIVE SURGERY 1298 (2019).

[130] *See Hearing on FRT and Privacy*, *supra* note 128, at 1.

[131] *Id.*

[132] For a recent history of data breaches, see Rob Sobers, *98 Must-Know Data Breach Statistics for 2022*, VARONIS, https://www.varonis.com/blog/data-breach-statistics/ [https://perma.cc/GXB7-3GYD] (Apr. 16, 2021).

[133] Chaminda Hewage, *Stolen Fingerprints Could Spell the End of Biometric Security*, CONVERSATION (Aug. 20, 2019, 8:06 AM), https://theconversation.com/stolen-fingerprints-could-spell-the-end-of-biometric-security-heres-how-to-save-it-122001 [https://perma.cc/23AG-SNH2]. In their annual report on data breach trends, Experian correctly predicted that "attackers will zero in on biometric hacking," referring to the recent breach of Suprema's biometric identification system used by "5,700 organizations in [eighty-three] countries, including governments, banks, and the police." EXPERIAN, DATA BREACH INDUSTRY FORECAST 2020, at 8 (2020), https://www.experian.com/content/dam/marketing/na/assets/data-breach/white-papers/Experian-Data-Breach-Industry-Forecast-2020.pdf [https://perma.cc/E4NV-AXYG] [hereinafter 2020 DATA BREACH FORECAST]; Zak Doffman, *New Data Breach Has Exposed Millions of Fingerprint and Facial Recognition Records: Report*, FORBES (Aug. 15, 2019, 4:31 AM), https://www.forbes.com/

company left more than one-million people's biometric information unprotected on a publicly accessible database.[134] That same year, the Department of Homeland Security experienced not one, but two data breaches,[135] one of which resulted in 184,000 travelers' images from a facial recognition pilot pouring into the dark web.[136] The latent threat of a biometric data breach risks depriving us of more than financial or reputational well-being. In a holistic sense, it carries the possibility for individuals to operate in the world as someone other than themselves.[137]

Although BIPA lay dormant for its first few years, it became a prominent site for class action litigation since 2015, featuring suits against social media platforms alleging "improper collection of facial geometries in photographs without notice and consent."[138] The

sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/#551b9bbf46c6 (last visited Apr. 19, 2022).

134 *See* 2020 DATA BREACH FORECAST, *supra* note 133, at 8.

135 Chris Burt, *Breached CBP Contractor May Have Been Training Biometric Facial Recognition Algorithm*, BIOMETRIC UPDATE (June 11, 2019, 1:25 PM), https://www.biometricupdate.com/201906/breached-cbp-contractor-may-have-been-training-biometric-facial-recognition-algorithm [https://perma.cc/KQP7-EB4J].

136 Chris Burt, *CBP Biometric Pilot Data Breached from Perceptics Winds Up on Dark Web*, BIOMETRIC UPDATE (Sept. 25, 2020, 5:23 PM), https://www.biometricupdate.com/202009/cbp-biometric-pilot-data-breached-from-perceptics-winds-up-on-dark-web [https://perma.cc/58TD-E5CU].

137 *Hearing on FRT and Privacy*, *supra* note 128, at 1–2 ("But facial recognition creates acute privacy concerns that fingerprints do not. Once someone has your fingerprint, they can dust your house or your surroundings to figure out what you have touched. Once someone has your faceprint, they can get your name, they can find your social networking account, and they can find and track you in the street, in the stores that you visit, the Government buildings you enter, and the photos your friends post online.").

138 Steven Grimes & Eric Shinabarger, *Biometric Privacy Litigation: The Next Class Action Battleground*, BLOOMBERG L. (Jan. 9, 2018, 4:38 PM), https://news.bloomberglaw.com/business-and-practice/biometric-privacy-litigation-the-next-class-action-battleground/ [https://perma.cc/6AQU-SYYE] (citing Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, (N.D. Ill. 2015)). Given its pervasive use of facial recognition technologies, Facebook remains a popular target for BIPA litigation, accruing several lawsuits over the last five years. *See* Christopher Zara, *Facebook Keeps Getting Sued Over Face-Recognition Software, and Privacy Groups Say We Should Be Paying More Attention*, INT'L BUS. TIMES (Sept. 3, 2015, 3:49 PM), https://www.ibtimes.com/facebook-keeps-getting-sued-over-face-recognition-software-privacy-groups-say-we-2082166 (last visited Apr. 19, 2022); Jay Peters, *Facebook to Pay $550 Million to Settle Privacy Lawsuit Over Facial Recognition Tech*, VERGE (Jan. 29, 2020, 7:17 PM),

now-notorious piece of legislation provides a private right of action against alleged violators.[139] In 2019, the Illinois Supreme Court determined that plaintiffs only need to demonstrate a violation of their statutory rights, rather than an actual injury, to proceed in court.[140] The court recognized that "[t]o require individuals to wait until they have sustained some compensable injury beyond violation of their statutory rights before they may seek recourse . . . would be completely antithetical to the Act's preventative and deterrent purposes."[141]

A. Clearview AI and Biometric Data Collection

Facial recognition technology remains a principal target for BIPA litigation. In January 2020, Kashmir Hill revealed the technology's latest iteration in a now-notorious company, Clearview AI.[142] Operating out of a WeWork space, the New York-based startup drew acclaim for its refined facial recognition capacities, boasting investments from Peter Thiel, the famed venture capitalist behind PayPal, Palantir, and Facebook.[143] Before marketing to law enforcement agencies, its CEO, Hoan Ton-That, liaised with former Congressional candidate Paul Nehlen[144] for an "unconventional database" to conduct "extreme opposition research."[145] Now, Clearview contracts with over six-hundred law enforcement agencies.[146] Although the company claims—and its website represents—that

---

https://www.theverge.com/2020/1/29/21114358/facebook-550-million-settle-lawsuit-facial-recognition-technology-illinois (last visited Apr. 19, 2022).

139 740 ILL. COMP. STAT. 14/20.

140 *See* Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1207 (Ill. 2019); *see also* Patel v. Facebook, Inc., 932 F.3d 1264, 1274 (9th Cir. 2019) (holding that the collection and use of biometric data provided a concrete injury-in-fact sufficient to confer Article III standing). *But see* Matthew Boesler, *Google Wins Dismissal of Suit Over Facial Recognition Software*, BLOOMBERG (Dec. 29, 2018, 2:57 PM), https://www.bloomberg.com/news/articles/2018-12-29/google-wins-dismissal-of-suit-over-facial-recognition-software-jq9w1mws [https://perma.cc/ZG52-8QKG] (discussing plaintiffs' lack of concrete injuries violating their statutory rights under BIPA).

141 *See Rosenbach*, 129 N.E.3d at 1207.

142 Hill, *supra* note 6.

143 *Id.*

144 *Extremist Files: Paul Nehlen*, S. POVERTY L. CTR., https://www.splcenter.org/fighting-hate/extremist-files/individual/paul-nehlen [https://perma.cc/66QV-N92Z].

145 Hill, *supra* note 6.

146 *Id.*

their software is only for law enforcement use, a data breach in February 2020 unveiled its client list, including private retailers like Walmart, Kohl's, Best Buy, and Macy's.[147] Subsequent investigation demonstrated that private persons acting in their individual capacities also had their hands on the software.[148] In addition to conventional retail surveillance and employee intimidation, these persons used Clearview for illicit purposes, such as identifying their children's dates "within seconds."[149]

While facial recognition technology is not new, its improvements have been unprecedented. As Hill noted, police departments have employed these technologies for over twenty years, though they were powered by full-frontal, government-provided images, such as mug shots and driver's license photos.[150] What differentiates Clearview, though, is its breadth of available images and its algorithm's sophistication. Through a practice called "data scraping," or automated data harvesting, the company indexes a database of "publicly available" images from social media platforms, as well as employment, news, and educational sites.[151]

Clearview generates a searchable database of over three-billion images, sourcing biometric data from publicly available platforms like Facebook, Instagram, Twitter, YouTube, and Venmo.[152] After users upload an image, Clearview's algorithm relates the person's facial features to other images depicting the same individual.[153] Like other facial recognition technologies, its software reduces a person's facial anatomy to its component parts, extracting biometric information from the images to comprehend and determine a person's

---

147 Ryan Mac et al., *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA*, BUZZFEED NEWS, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement [https://perma.cc/WF7B-Q5F5] (Feb. 27, 2020, 3:43 PM).

148 Kashmir Hill, *Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*, N.Y. TIMES, https://www.nytimes.com/2020/03/05/technology/clearview-investors.html [https://perma.cc/3C3P-L58D] (Mar. 6, 2020).

149 *Id.*

150 Hill, *supra* note 6.

151 *Id.*; *see also generally* Benjamin Sobel, *A New Common Law of Web Scraping*, 25 LEWIS & CLARK L. REV. 147 (2021).

152 Hill, *supra* note 6.

153 *Id.*

identity.[154] As Ton-That explained, Clearview's facial recognition algorithm:

> convert[s] 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.[155]

Using vector analysis, the algorithm takes an image and understands it in terms of its quantitative metrics, particularly the face's measurements.[156] It does not necessarily understand it as a face, but

---

[154] Facial recognition technologies employ deep neural network learning mechanisms that enable greater accuracy in identification. In short, neural networks build from abstractions to particularities and, with enough data, they will be able to learn more about the specific divergencies in a training data set. Typical modern image processing nets are structured with low-level neurons being fed the direct pixels of an image, which then feeds their output. For example, this may involve relaying something like edges that were detected or colors that were found in the image to the next levels of neurons, which might be responsible for detecting shapes and patterns, and passing those outputs on to the next layers. Each layer builds up a more nuanced understanding of the image using the understanding of the previous layer's output. Training a network involves passing millions of images through it over the course of thousands of iterations, essentially rewarding the network when it is able to make any inferences about individuals in the dataset. So the low levels—the colors and textures, for instance—learn these abstract patterns first, and eventually, over time, the higher level neurons will no longer need to worry about the abstractions that have already been learned: they see one level of neurons telling them that this is a "brown image," another that says it is a "face," and another that gives it a shape, and the networks join these determinations to conclude that the image represents a particular person. For more information about facial recognition technologies and deep neural network learning, see Davide Castelvecchi, *Is Facial Recognition Too Biased to be Let Loose?*, NATURE (Nov. 18, 2020), https://www.nature.com/articles/d41586-020-03186-4 [https://perma.cc/7BHL-GPV6].

[155] Hill, *supra* note 6.

[156] *Joint Investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Comissioner of Alberta*, OFF. OF PRIV. COMM'R OF CAN. (Feb. 2, 2021), https://www.priv.gc.ca/en/opc-actions-and-

the measurements enable it to then recognize a pattern between images.[157] That pattern then apprehends a face, reproducing it as an amalgam of quantitative metrics.[158] The face is no longer more than the sum of its parts; it is a coordinate plane that renders signs and significations.[159]

These vector analyses may trouble normative and legal frameworks for data collection. Here, Ton-That draws an analogy to Google, which "downloads the whole Internet and then makes an index of all common keywords that point to the original page."[160] On a technical level, Ton-That would still need to store the vector data—the "keywords"—in order to search it. But he could process that data without ever storing the original image. Rather, he could store the metadata—the multitude of vectors—to conceive the image and produce a "composite [of the image]."[161]

Clearview's basic line is simple: components inherent to a public image are necessarily public, as well. After all, Clearview only extrapolates information from the public image. But, because Clearview does not return the image, its functionality bears distinguishment. Suppose you take an image of yourself next to a standard doorframe. By relating your depiction in the image to the standard doorframe, you can approximate your height. But doing so requires outside knowledge inputs; you would need to know the height of a standard doorframe. Assuming the photo lacks any other obscurities, you ascertain your height by analyzing the image's measurements, calculating the proportions of the measured image's heights,

---

decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/ [https://perma.cc/74NQ-9FK5].

157 *Id.*

158 *Id.*

159 GILLES DELEUZE & FELIX GUATTARI, A THOUSAND PLATEAUS 115 (Brian Massumi trans., Univ. of Minn. Press 2d ed. 1987) (1980) ("[T]he face crystallizes all redundancies, it emits and receives, releases and recaptures signifying signs. . . .The face is what gives the signifier substance; it is what fuels interpretation, and it is what changes, changes traits, when interpretation reimparts [the] signifier to its substance.").

160 This Week in Startups, *E1100: Clearview AI CEO Hoan Ton-That on Balancing Privacy & Security, Engaging with Controversy*, YOUTUBE (Aug. 25, 2020), https://www.youtube.com/watch?v=wNLK_f6m4e0 [https://perma.cc/8GE4-HULH].

161 *Id.*

combining outside information about the doorframe's height, and arriving at your own height.

However, algorithms cannot access this outside information on their own. No less than a person viewing the image, the doorframe's standard height is not readily apparent. Without that information, an algorithm can reconstruct the door and person in the image respectively, but cannot reconstruct an analysis that relates the person to the door. At best, algorithms give an approximate understanding of each represented object—the door and person—because the image reproduces you but is not actually you. And, whereas there are standard doorframes, such that you could input outside knowledge into the algorithm to reach more accurate results, faces are not standard; thus, the algorithm lacks a point of comparison other than the subject itself.

Ton-Thot simultaneously boasts his software's sophistication while recognizing the reality that every face is unique.[162] To take this position seriously, though, means no technology could ever identify every person with full precision unless it had data on every existing person; again, these technologies produce, at best, working approximations.[163] While facial recognition technologies have proven to identify people with greater accuracy than the human eye—a sensational selling point for these kinds of technologies—

---

[162] During their interview, Jason Calacanis asked Ton-Thot whether earlier developers had a blind spot to differentiating among races and ethnicities, or whether, for example, "all Irish people look the same?" *Id.* In response, Ton-Thot said, "[e]veryone's face is unique." *Id.* For this reason, he insisted that no races are more "unique" than others. *Id.* The problem, then, is that celebrity training data sets are not fully representative of the whole population. *Id.* But, absent considerable data on every individual, no amount of neural network processing will achieve full recognition capacities. *Id.*

[163] For discussions about bias in facial recognition technologies, see Natasha Singer & Cade Metz, *Many Facial-Recognition Systems Are Biased, Says U.S. Study*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html [https://perma.cc/HZ93-56XG]; Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEORGETOWN L. CTR. PRIV. & TECH. (May 16, 2019), https://www.flawedfacedata.com/ [https://perma.cc/Q4LW-TYLJ]; Steve Lohr, *Facial Recognition Is Accurate, If You're a White Guy*, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html [https://perma.cc/EM6L-P936]; SARAH MYERS WEST ET AL., DISCRIMINATING SYSTEMS: GENDER, RACE, AND POWER IN AI (2019); Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, *in* 81 PROCEEDINGS OF MACHINE LEARNING RESEARCH 77 (2018).

we should not expect otherwise. These facial recognition algorithms demonstrate that faces are reducible to numerical representations that are beyond the kind of comprehension the human eye performs. More likely, people perform qualitative analyses when they "recognize" others in the world, which explains why we are subject to misrecognition.[164] But just because computers perform quantitative analyses—measuring facial geometries, for instance—does not mean that they are less fallible. In fact, this is their limit: facial recognition technologies aspire toward unattainable precision and struggle to recognize meaningful differences.

Using these vector analyses for biometric data collection proves unsettling, if only because it appropriates its subjects' likenesses and transposes them from their image. Their translation becomes less about resemblance than relocation or displacement.[165] As cultural critic Homi Bhabha wrote:

> What is *within* photography that reaches *beyond* its limits in order to animate other desires . . . is its mode of signification, not its mimetic resemblance as image. By re-situating or re-locating photography in yet another representational or narrative medium . . . the subject gains another life, and the photographic image survives as itself, in a different form.[166]

Clearview exploits this feature of photography which was once only the province of thought: there is something in an image that is more

---

[164] *See* FACE PROCESSING: ADVANCED MODELING AND METHODS 8–9 (Wenyi Zhao & Rama Chellappa eds., 2006). *But see* Yana Welinder, *A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks*, 26 HARV. J.L. & TECH. 165, 170 (2012) ("While recognition is a natural human skill, the human brain can only memorize a limited number of faces. On the other hand, computers can process and remember a vast number of facial features to recognize many more people. But qualitatively, the human brain does a more complete job of recognizing faces than computers because it is able to combine visual recognition with other human senses.").

[165] *See* WALTER BENJAMIN, *The Translator's Task*, *in* ILLUMINATIONS 161 (Steven Rendall trans., 1969) ("[I]nstead of making itself resemble the meaning of the original, [a translation] must lovingly, and in detail, fashion in its own language a counterpart to the original's mode of intention, in order to make both of them as fragments of vessel, as fragments of a greater language.").

[166] *See generally* Homi Bhabha, *Beyond Photography*, *in* A LIVING MAN DECLARED DEAD AND OTHER CHAPTERS I-XVIII (2012).

than the image. The company argues that features internal to a public image are also public, including biometric data,[167] reanimating a central tension concerning whether individuals retain any privacy in public.[168]

B. Clearview AI's BIPA Litigation

Within four days of Hill's investigative report release, Illinois residents filed a class action against Clearview for violating their biometric privacy.[169] The company soon became ensnared in several class action lawsuits.[170] In *Mutnick*, the parties contended that Clearview circumvented various platforms' terms of use agreements to collect and obtain biometric data from users' profiles.[171] Its collection interfered with and violated users' contracts with these platforms, to which they entrusted their data.[172] Because they own their data servers, Clearview receives real-time access to user activity on their application, including ongoing criminal investigations.[173] As the *Mutnick* complaint alleged, "Clearview is enmeshed in the use of state power against individual American citizens and, further, has the unique opportunity to tip off and/or extort suspects."[174] In Hill's report, she mentioned that, after soliciting several police officers to run on a search on her, the company quickly called the officers to ask whether they were speaking to the media.[175]

Plaintiffs in both *Burke v. Clearview AI* and *ACLU v. Clearview AI* raised similar concerns. In *Burke*, the parties offered a parade of

---

167 *See Companies' Cease-and-Desist Letters*, *supra* note 18.

168 *See generally* Joel R. Reidenberg, *Privacy in Public*, 69 U. MIA. L. REV. 141 (2014); Hartzog, *supra* note 4.

169 *See* Class Action Complaint, Mutnick v. Clearview AI, Inc., No. 2020-cv-00512 (N.D. Ill. Jan. 22, 2020).

170 *See, e.g.*, *id.*; Memorandum Decision and Order Denying the Motion to Intervene and to Dismiss or, Alternatively, to Stay Cases or Transfer Venue, Burke v. Clearview AI, Inc., No. 2020-cv-03104 (S.D.N.Y. May 29, 2020); Complaint, ACLU v. Clearview AI, Inc., No. 9337839 (Ill. Cir. Ct. May 28, 2020).

171 Class Action Complaint, *supra* note 169, at 19.

172 *Id.*

173 *Id.* at 2.

174 *Id.*

175 Hill, *supra* note 6.

horribles.[176] Among them, they posed scenarios where the application empowered a rogue employee to stalk potential romantic partners, a foreign government to discover information to blackmail key individuals, or law enforcement agencies to pry into citizens' private lives without probable cause or reasonable suspicion.[177] In *ACLU*, the parties described that many private actors acquired the application free of charge for a thirty-day trial, relieving them of any contractual obligations with Clearview.[178] By February 2020, "people associated with 2,228 companies, law enforcement agencies, and other institutions had collectively performed nearly 500,000 searches of Clearview's faceprint database."[179]

All of the complaints alleged the same violation of BIPA: Clearview collected and sold the parties' biometric identifiers and information without users' consent.[180] Clearview also failed to provide a retention schedule for the maintenance of users' biometric data.[181] Two recent cases may serve as harbingers for Clearview's fate.

C. Privacy Harms, Tangible Harms

In *Rivera v. Google*, Google scanned images from its cloud-based service, Google Photos, to "locate[] [the plaintiff's] face and zero[] in on its unique contours to create a 'template' that maps and records her distinct facial measurements."[182] Google argued that the plaintiffs complaint about the use of their *photographs* fell outside of BIPA's scope for biometric identifiers.[183] It drew a distinction between photographic and in-person facial scans, contending that only the latter qualify as biometric identifiers.[184] However, the court

---

176 *See* Class Action Complaint at 3, Burke v. Clearview AI, Inc, No. 2020-cv-03104 (S.D. Cal. Feb. 27, 2020).

177 *Id.*

178 Complaint at 4, ACLU v. Clearview AI, No. 9337839 (Ill. Cir. Ct. May 28, 2020).

179 *Id.* (citing Mac et al., *supra* note 147).

180 Class Action Complaint at 11–12, Mutnick v. Clearview AI, Inc., No. 2020-cv-00512 (N.D. Ill. Jan. 22, 2020); Class Action Complaint at 18–19, *Burke*, No. 2020-cv-03104 (S.D. Cal. Feb. 27, 2020); Complaint at 31–32, *ACLU*, No. 9337839 (Ill. Cir. Ct. May 28, 2020).

181 *See, e.g.*, Complaint at 12, *Mutnick*, No. 2020-cv-00512 (N.D. Ill. Jan. 22, 2020).

182 Rivera v. Google Inc. (*Rivera I*), 238 F. Supp. 3d 1088, 1091 (N.D. Ill. 2017).

183 *Id.* at 1092.

184 *Id.* at 1095.

did not take the bait.[185] The court concluded, "if Google simply captured and stored the *photographs* and did not measure and generate scans of face geometry, then there would be no violation of the Act."[186] Its decision suggests that biometric data obtained from non-biometric sources, such as photographs, may still be considered a biometric identifier under BIPA.[187]

The following year, the Northern District of Illinois returned to the *Rivera* case and ultimately granted summary judgment for Google, finding that the plaintiffs lacked standing under Article III and failed to allege any concrete injuries relating to the collection of their biometric identifiers.[188] In 2019, though, the tides turned against corporate actors seeking to either dismiss cases or win summary judgment on standing grounds.[189] In *Patel v. Facebook*, the Ninth Circuit became the first appellate court to hold that biometric privacy violations under BIPA suffice to confer Article III standing.[190] There, the plaintiffs disputed Facebook's Tag Suggestions, which used facial recognition technology to identify potential subjects in users' photos. The court determined that Facebook's facial recognition technology could obtain information that is "detailed, encyclopedic, and effortlessly compiled," which would otherwise be near-impossible without such technology.[191] After generating face templates, companies can use them to identify and locate individuals with unprecedented precision.[192] The bare risk of such surveillance harms invades an individual's private affairs and concrete interests.[193]

---

185 *Id.*

186 *Id.* at 1097.

187 Erin Jane Illman, *Data Privacy Laws Targeting Biometric and Geolocation Technologies*, 73 BUS. LAW., Feb. 2019, at 191, 193.

188 *See* Rivera v. Google Inc. (*Rivera II*), 366 F. Supp. 3d 998, 1006 (N.D. Ill. 2018).

189 *See generally* Patel v. Facebook, 932 F.3d 1264 (9th Cir. 2019); Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197 (Ill. 2019).

190 *Patel*, 932 F.3d at 1275; *see also* Janice Lopez, *A Looming Dystopia? Facial Recognition Software Proliferates Privacy Concerns*, AM. UNIV. BUS. L. REV., https://aublr.org/2020/03/a-looming-dystopia-facial-recognition-software-proliferates-privacy-concerns/ [https://perma.cc/Q3ZA-8879].

191 *Patel*, 932 F.3d at 1273 (citing Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018)).

192 *Id.*

193 *Id.*

With the case prepared to proceed, Facebook settled the class action lawsuit for $550 million.[194] However, the district court worried that the judgment was under-compensatory.[195] In addition to raising the settlement to $650 million, Facebook changed its facial recognition settings to require users to opt-in to the setting.[196] As a result of Facebook's settlement, class action plaintiffs have set their eyes on BIPA class litigation.[197] But now that Facebook set the standard for valuing BIPA settlements, few defendants will be able to afford settling their claims, cornering them into litigation. With the case law increasingly weighing against them, facial recognition technologists, like Clearview, have one more avenue to pursue: undermine BIPA on constitutional grounds.

IV. THE FIRST AMENDMENT AND BIOMETRIC DATA COLLECTION

The First Amendment makes for a charming ally. Eugene Volokh, chief among its proponents, caused a stir among privacy academics when he professed that rights to information privacy are presumptively in conflict with the First Amendment.[198] He argues that contracts suffice to defend our privacy and assuage concerns over illicit disclosures.[199] However, consumers have few bargaining resources at their disposal relative to corporate actors. More often, they forfeit personal information without fully understanding the cumulative effects of such forfeitures.[200] Volokh's contract model

---

194 *See* Natasha Singer & Mike Isaac, *Facebook to Pay $550 Million to Settle Facial Recognition Suit*, N.Y. TIMES (Jan. 29, 2020), https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html [https://perma.cc/6NNF-98HV].

195 *See* David Oberly, *Impact of Facebook $650 Million Patel BIPA Settlement*, BIOMETRIC UPDATE (Aug. 20, 2020, 3:42 PM), https://www.biometricupdate.com/202008/impact-of-facebook-650-million-patel-bipa-settlement [https://perma.cc/L285-RMV5].

196 *Id.*

197 *Id.*

198 Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN L. REV. 1049, 1051 (2000) ("We already have a code of 'fair information practices,' and it is the First Amendment . . . .").

199 *Id.* at 1057–63.

200 *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1200 (2016).

contributes to a legacy where "the strong do what they can and the weak suffer what they must."

Volokh recognized a significant limit to the contract model and offered that customs should traverse certain contexts and imply contractual obligations.[201] However, implied obligations would only incentivize companies to provide explicit disclosures in their privacy policies that stipulate how they collect, store, use, and sell information. Jack Balkin offers a remedy to this issue, extending platforms' obligations to consumers under fiduciary theories.[202] For Balkin, consumers' relationships of trust and confidence with platforms give rise to their fiduciary duties not to use consumers' information to their detriment.[203]

Like doctor and lawyer contexts, asymmetries of knowledge and information should require platforms to protect our information and only use it to our benefit.[204] Yet companies frame this benefit in privacy policies in terms of enabling user personalization. These predictive schemes enshrine data collection practices as mutually beneficial, though they tread a fine line between accommodating and manipulating these experiences. Employing explicit language in privacy policies and prescribing fiduciary duties to platforms are only effective to the extent that we reckon with the nature of the benefit platforms are according us.

Neither Volokh's implied contract model nor Balkin's information fiduciary model adequately responds to third-party beneficiaries to our data disclosures and vulnerabilities online. Privacy policies only enumerate the obligations that parties in privity—platforms and their users—owe to each other. Any reciprocal benefit is confined to their discrete relationship. However, when privacy policies caution users that their disclosures are visible to the public, they give free rein to third-party observation and associated risks that data may be used in other contexts. Recent case law has

---

201 *See* Volokh, *supra* note 198, at 1057–58 ("In many contexts, people reasonably expect—because of custom, course of dealing with the other party, or all the other factors that are relevant to finding an implied contract—that part of what their contracting partner is promising is confidentiality.").

202 Balkin, *supra* note 200, at 1205–34.

203 *Id.* at 1208.

204 *See id.* at 1209, 1221.

complicated this further, suggesting that by revoking access to otherwise publicly available information, platforms risk generating information monopolies.[205]

The problem of data scrapers therefore elicits new First Amendment concerns in the digital sphere. In a recent interview, Clearview CEO Ton-That suggested that all the data contained in Clearview is "publicly available" on the internet.[206] Analogizing Clearview's facial recognition capacities to Google, he remarked, "it's like a Google search for faces. You put in a face, you get . . . a lead. It's like Googling someone's name."[207] Except Clearview's software operates differently than Google's. Any number of individuals may share your name, but no one shares your face.[208] Ton-That shies away from this meaningful technical difference with Google's "reverse image search."[209] Google's service analyzes an image to determine its unique features—its lines, colors, and textures, for example—to generate a query that matches the image to a database of billions of images.[210] Their algorithm returns search results containing matching or "visually similar" images.[211] Whereas Google's reverse image search returns the same image, Clearview returns the

---

[205] HiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1005 (9th Cir. 2019), *vacated* 141 S. Ct. 2752 (2021).

[206] *See* This Week in Startups, *supra* note 160.

[207] *Id.*

[208] In recent years, technologists have been working toward mitigating the "Evil Twin" dilemma, where facial recognition technology tends to have difficulty discerning between identical twins. *See* Jack Purcher, *Apple Advances Face ID to Be 'Twin Proof' Using Machine Learning, Subepidermal Imaging and More*, PATENTLY APPLE (Mar. 14, 2019, 8:48 AM), https://www.patentlyapple.com/patently-apple/2019/03/apple-advances-face-id-to-be-twin-proof-using-machine-learning-subepidermal-imaging-and-more.html [https://perma.cc/2QLJ-SHKL]. Subepidermal imaging of more discrete biometric components—such as blood vessels—provides one avenue for aiding such differentiation capacities. *Id.* ("Unlike some other facial features on the surface of the skin of a user's face, veins in the subepidermal layers of the face are typically unique to an individual and vein patterns are different between different individuals, even siblings or twins. Thus, assessment of the veins (and vein patterns) in the subepidermal layers of the face may be used to distinguish between siblings, twins, or other users with similar facial features on the surface of the face.").

[209] *Search with an Image*, GOOGLE, https://support.google.com/websearch/answer/1325808?p=searchbyimagepage&hl=en [https://perma.cc/XX6N-5L9M].

[210] *See* Google, *How Search by Image Works*, YOUTUBE (July 20, 2011), https://www.youtube.com/watch?v=keTZaJg0784 [https://perma.cc/FVR4-WHA2].

[211] *Id.*

same person. Their queries internalize different languages. Rather than apprehending the whole image, Clearview extracts the constitutive elements of the image, namely the biometric features internal to them, to render its analysis. This difference is not trivial.

Critics of the company's surveillance mechanisms bemoan an Orwellian future in sight, claiming that the company "might end privacy as we know it."[212] Dystopian fears over government-sanctioned surveillance abound, giving life to the adage "who watches the watchmen?" Existing case law may enable Clearview to exploit public information for its own benefit.[213] Without formal constraints on Clearview's data scraping practices, the company joins the ranks of other powerful corporate actors depreciating First Amendment values.[214]

---

[212] Hill, *supra* note 6.

[213] Petition for Writ of Certiorari at 28, hiQ Labs v. LinkedIn, Inc., 141 S. Ct. 2752 (2021) (No. 19-1116) ("Users do not expect, or consent to, the exploitation of their personal information in perpetuity by third parties that the users and the website owner did not authorize and whose interests are not aligned with the interests of the owners of that personal information.").

[214] *See* Julie E. Cohen, *The Zombie First Amendment*, 56 WM. & MARY L. REV. 1119, 1120 (2015) ("The contemporary First Amendment must be situated within a larger story about the realignment of information flows within circuits of power that serve emerging global interests, and to tell that story, one must look to disputes about the speech implications of private economic regulation. As a result of that struggle, free speech jurisprudence about information rights and harms is becoming what is best described as a zombie free speech jurisprudence: a body of doctrine robbed of its animating spirit of expressive equality and enslaved in the service of economic power."); *see also* Jameel Jaffer & Ramya Krishnan, *Clearview AI's First Amendment Theory Threatens Privacy—and Speech, Too*, SLATE (Nov. 17, 2020, 1:21 PM), https://slate.com/technology/2020/11/clearview-ai-first-amendment-illinois-lawsuit.html [https://perma.cc/U8F3-RGGA] ("Technology companies have learned that an effective way to protect lucrative business practices from regulation is to characterize those practices as free speech. Google has been arguing, with some success in the lower courts, that judges should deal with any effort to regulate its search engine in the same way they'd deal with efforts to censor the Wall Street Journal. In Maine, internet service providers are arguing that the First Amendment protects their right to use and sell their customers' sensitive data without their consent. Earlier this fall, President Donald Trump issued an executive order meant to shut down TikTok, the video-sharing platform. The company sued, arguing that the order violated the First Amendment because TikTok runs on code, and code is speech."); Balkin, *supra* note 200, at 1186 (discussing how the First Amendment has become "the most fertile source of constitutional defenses to business regulation"); Tim Wu, *The Right to Evade Regulation: How Corporations Hijacked the First Amendment*, NEW REPUBLIC (June 3, 2013),

With the Constitution as its battleground, Clearview asserts a free speech right to collect and disseminate publicly available photos.[215] Although this Note argues otherwise, such a practice may warrant constitutional protection,[216] if it was what Clearview's algorithm actually does. The software's sophistication exceeds the facial recognition capacities of similar programs run by the U.S. government and other Silicon Valley giants.[217] Given that Clearview defends its practice on First Amendment grounds,[218] the difference implicates a fundamental tension over whether people, rather than their images, are reducible to language—and, if so, whether others can lay claim to them. With BIPA on the table, it may also determine whether our biometric privacy is incompatible with the First Amendment.

A. Matter of Public Concern

The United States remains among the strongest proponents of free speech.[219] That right comes with an expansive, though limited, license to engage in speech. And, unsurprisingly, it carries a history contending over what qualifies *as* speech. Without exhausting many decades' worth of literature arguing that everything is speech, we

---

https://newrepublic.com/article/113294/how-corporations-hijacked-first-amendment-evade-regulation [https://perma.cc/4EJF-A4FF].

[215] Kashmir Hill, *Facial Recognition Start-Up Mounts a First Amendment Defense*, N.Y. TIMES, https://www.nytimes.com/2020/08/11/technology/clearview-floyd-abrams.html? [https://perma.cc/A3SR-TTT7] (Mar. 18, 2021).

[216] *See* Adam Schwartz, *Clearview's Face Surveillance Still Has No First Amendment Defense*, ELEC. FRONTIER FOUND. (July 13, 2021), https://www.eff.org/deeplinks/2021/07/clearviews-face-surveillance-still-has-no-first-amendment-defense [https://perma.cc/H339-3YF2].

[217] Hill, *supra* note 6 ("Its nationwide database of images is much larger, and unlike FACES [Florida's state-provided facial recognition tool], Clearview's algorithm doesn't require photos of people looking straight at the camera. 'With Clearview, you can use photos that aren't perfect,' Sergeant Ferrara said. 'A person can be wearing a hat or glasses, or it can be a profile shot or partial view of their face.'").

[218] Schwartz, *supra* note 216.

[219] *See* Richard Wike & Katie Simmons, *Global Support for Principle of Free Expression, but Opposition to Some Forms of Speech*, PEW RSCH. CTR. (Nov. 18, 2015), https://www.pewresearch.org/global/2015/11/18/global-support-for-principle-of-free-expression-but-opposition-to-some-forms-of-speech/ [https://perma.cc/4CND-W47A].

might say instead that "speech is everywhere."[220] But not all speech warrants a legal battle, let alone merits legal protection.

In its most popular iterations, unprotected speech may involve instances of incitement, obscenity, fighting words, threats, and falsely shouting "fire" in theatres.[221] Less obviously, there are product labeling requirements, securities disclosures and nondisclosures, and restraints on workplace speech.[222] In these latter circumstances, regulations over speech are so ubiquitous that they sublimate into our everyday norms for engaging and exercising speech.[223] Failing to appreciate their existence does not make them any less operative. Indeed, in the context of the First Amendment's privacy jurisprudence, these norms not only circumscribe what constitutes speech, but also define whether individuals are entitled to privacy over that speech.

In their *ACLU* amicus brief, the Electronic Frontier Foundation ("EFF") noted that the First Amendment protects not only expression, but also the necessary predicates that enable expression, including the collection and creation of information.[224] Emphasizing the right of listeners—the recipients of speech—the group drew an analogy to recording on-duty law enforcement officers.[225] As the Seventh Circuit found, "[t]he right to publish or broadcast an audio or audiovisual recording would be insecure, or largely ineffective, if the antecedent act of *making* the recording is wholly

---

220 RICHARDS, *supra* note 53, at 86.

221 *Id.*

222 *Id.*

223 Terming this phenomenon "First Amendment salience," Frederick Schauer argues that our understanding of the First Amendment is limited to those concerns which courts address. However, an overwhelming majority of speech regulations, such as those pertaining to antitrust or sexual harassment, receive little judicial scrutiny. Frederick Schauer, *The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience*, 117 HARV. L. REV. 1765, 1768 (2004).

224 Adam Schwartz & Andrew Crocker, *Clearview's Faceprinting is Not Sheltered from Biometric Privacy Litigation by the First Amendment*, ELEC. FRONTIER FOUND. (Nov. 5, 2020), https://www.eff.org/deeplinks/2020/11/clearviews-faceprinting-not-sheltered-biometric-privacy-litigation-first-amendment [https://perma.cc/EQ28-K3CT].

225 *Id.*; *see also* Marc Jonathan Blitz, *Constitutional Safeguards for Silent Experiments in Living: Libraries, the Right to Read, and a First Amendment Theory for an Unaccompanied Right to Receive Information*, 74 U. MO.-KAN. CITY L. REV. 799 (2006) (endorsing a First Amendment right to receive information).

unprotected."[226] On this basis, EFF concluded that Clearview's data collection was permitted.[227]

But the group missed a core tenet of First Amendment jurisprudence. Law enforcement officers acting in their official capacity are necessarily acting, ostensibly, in the public interest. They are accountable for on-duty conduct; their comportment is, in the jurisprudence's terms, "a matter of public concern."[228] The recording takes place in public and concerns public officials acting for the public. Indeed, speech does not harness the power to become of public concern on its own. It exists relative to the interests and intentions of its speakers and audience, and the general context in which it occurs. This context is often reduced to its spatial elements: speech occurred *in* public—therefore it must have been *for* the public.[229]

Here, the public is both a fiction of place and person. Part of this argument relies on the premise that the ability to curtail the "capture of public images" would "truncate recollection and discussion of matters experienced by the community, and [] effectively edit the community's memory."[230] But memory will exist irrespective of whether we are conscious of it. The issue is less about memory as such than on what terms we can control, manipulate, and prolong it. By conflating information access and collection—and confusing

---

226 ACLU of Ill. v. Alvarez, 679 F.3d 583, 595 (7th Cir. 2012); *see also* Seth F. Kreimer, *Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record*, 159 U. PA. L. REV. 335, 404 (2011) ("[W]e must distinguish between the capture and the distribution of images. The interest in avoiding outside observation depends primarily on the distribution of captured images. An invited observer who records images of her own interactions for her own future review has not subjected private occurrences to unconsented public examination. Recording the image preserves memories of the observer's own life, and in most situations it is implausible—and of dubious constitutionality—to imply an agreement to forgo her own memory.").

227 Brief of Amicus Curiae Electronic Frontier Foundation at 5, ACLU v. Clearview AI, Inc., No. 2020-CH-04353 (Ill. Cir. Ct. Nov. 5, 2020) [hereinafter EFF Amicus].

228 Bartnicki v. Vopper, 532 U.S. 514, 534 (2001).

229 *See, e.g.*, Kreimer, *supra* note 226, at 402; *see also* Bambauer, *supra* note 21, at 84–86 (arguing that the right to collect and create information implies a right to record in public). For further discussion of the right to record under the First Amendment, see Margot E. Kaminski, *Privacy and the Right to Record*, 97 B.U. L. REV. 167, 177–99 (2017).

230 Kreimer, *supra* note 226, at 402.

collection with recollection—the argument muddies the line between speech and conduct, which carry distinct legal protections.[231]

The Court struck this gentle balance in *Bartnicki v. Vopper*.[232] There, a teachers union engaged in collective bargaining negotiations with the school board.[233] These negotiations were contentious and received significant media attention.[234] Bartnicki, the union's chief negotiator, phoned the union's president to discuss the status of negotiations.[235] During the call, Bartnicki mentioned going to the board members' homes and "blow[ing] off their front porches."[236] An unidentified third party intercepted and recorded the call, later delivering the recording to union opponents.[237] The opponents then provided the tape to Vopper, a radio commentator, who broadcasted the recording.[238] After Bartnicki brought suit against Vopper for federal and state wiretapping violations, the Court was faced with a vexing dilemma: does the First Amendment protect subsequent disclosures of lawfully obtained information when the source of that information obtained the information unlawfully?[239]

The Court permitted the subsequent disclosure, finding that the relevant statute's "naked prohibition against disclosures is fairly characterized as a regulation of pure speech."[240] Accordingly, the statute could not suppress a law-abiding possessor of information's disclosure in order to deter a non-law-abiding third party's conduct.[241] This is particularly true where speech regulations sanction the publication of matters of public concern.[242] The Court went to great lengths to disclaim any endorsement of illicit information-

---

231 *See* Rice v. Paladin Enters., 128 F.3d 233, 243 (4th Cir. 1997) ("[S]peech which . . . is tantamount to legitimately proscribable nonexpressive conduct may itself be legitimately proscribed, punished, or regulated incidentally to the constitutional enforcement of generally applicable statutes.").

232 *Bartnicki*, 532 U.S. at 514.

233 *Id.* at 518.

234 *Id.*

235 *Id.*

236 *Id.* at 518–19.

237 *Id.*

238 *Id.* at 519.

239 *Id.* at 528.

240 *Id.* at 526.

241 *Id.* at 529–30.

242 *Id.* at 533–34.

gathering practices, reiterating that "[t]he essential thrust of the First Amendment is to prohibit improper restraints on the *voluntary* public expression of ideas; it shields the man who wants to speak or publish when others wish him to be quiet."[243]

Bartnicki is characteristic of the Court's general apprehension against sweeping privacy holdings.[244] Where the First Amendment conflicts with privacy rights, the Court is particular about limiting its holding to the instant facts, careful not to exceed the appropriate context and render a categorical deprivation of privacy.[245] In reaching its decision, the Court paid homage to Justice Brandeis, signaling that one of the costs associated with participation in public affairs is an attendant loss of privacy.[246]

Although *Bartnicki* remains good law, it stands out as a pariah. Writing ten years after the decision, one commentator noted, "[i]n no case reported to date has the holding in *Bartnicki* been applied to reach a similar conclusion in an analogous case."[247] However, the case remains clear for its proposition that regulations of matters of public concern deserve greater scrutiny than private matters.[248] As the Court discussed in *Snyder v. Phelps*, "speech concerning public affairs is more than self-expression; it is the essence of self-government."[249] Restricting speech on purely private matters does not implicate the same constitutional concerns.[250] Private matters depart from the First Amendment's essence to protect robust debate of public issues and enable a meaningful dialogue of ideas.[251]

Vesting facial recognition technologies in the hands of private developers plays a pivotal role in considering whether Clearview's

---

243 *Id.* at 532 n.20 (quoting Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 559 (1985)).

244 *Id.* at 529.

245 *See id.*

246 *Id.* at 534.

247 Eric Easton, *Ten Years After:* Bartnicki v. Vopper *as a Laboratory for First Amendment Advocacy and Analysis*, 50 U. LOUISVILLE L. REV. 287, 334 (2011).

248 *Cf.* Snyder v. Phelps, 562 U.S. 443, 452 (2011) ("[W]here matters of purely private significance are at issue, First Amendment protections are often less rigorous.").

249 *Id.* (quoting Garrison v. Louisiana, 379 U.S. 64, 74–75 (1964)).

250 *Id.*

251 *Id.* (citing Hustler Mag., Inc. v. Falwell, 485 U.S. 46, 56 (1988) (internal citations omitted)); *see also* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964).

data collection constitutes a matter of public concern. The company is, in the most immediate sense, primarily motivated to profit from their software. Their algorithm indiscriminately collects massive swaths of personal data, with little reason to believe that any particular individual whose data it collects engaged in matters of public concern.[252] The implication bears dire consequences on two fronts.

1. Algorithms as Subjects, Not Speech

Clearview interprets algorithms as speech rather than subjects. The Framers undoubtedly lacked the foresight to determine whether algorithms qualify as speech. But, at a more rudimentary level, they did establish the First Amendment to protect human speech.[253] The First Amendment has, in Tim Wu's view, "wandered far from its purposes when it is recruited to protect commercial automatons from regulatory scrutiny."[254] Though algorithms require initial human input, increasing sophistication in AI development and machine learning renders their code autonomous.[255] To the extent that courts imbue algorithms with what are foremost *human* rights,[256] they risk elevating self-sufficient (and, dare I say, self-conscious)[257] machines above ourselves.[258]

---

[252] *See* EFF Amicus, *supra* note 227, at 9; *cf.* Fla. Star v. B.J.F., 491 U.S. 524, 536 (1989) (holding that the First Amendment protected a newspaper's publication of a rape victim's name because it obtained the victim's name lawfully and, the nature of the information—a public criminal proceeding—ascribed its public significance).

[253] Tim Wu, *Free Speech for Computers?*, N.Y. TIMES (June 19, 2012), https://www.nytimes.com/2012/06/20/opinion/free-speech-for-computers.html [https://perma.cc/GJ3Y-D9NX].

[254] *Id.*

[255] *See, e.g.*, Bruce Schneier, *Autonomous Everything: How Algorithms Are Taking Over Our World*, LITERARY HUB (Oct. 1, 2018), https://lithub.com/autonomous-everything-how-algorithms-re-taking-over-our-world/ [https://perma.cc/4T5R-UX66].

[256] *See, e.g.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429, 445–50 (2d Cir. 2001) (holding that computer code and programs merit First Amendment protection); Junger v. Daley, 203 F.3d 481, 485 (6th Cir. 2000) (holding that the First Amendment protects encryption code).

[257] Christof Koch, *Will Machines Ever Become Conscious?*, SCI. AM. (Dec. 1, 2019), https://www.scientificamerican.com/article/will-machines-ever-become-conscious/ (last visited Apr. 19, 2022); Hugh Howey, *How to Build a Self-Conscious Machine*, WIRED (Oct. 4, 2017, 6:55 AM), https://www.wired.com/story/how-to-build-a-self-conscious-ai-machine/ [https://perma.cc/JV4D-LYUC].

[258] *See* Wu, *supra* note 253.

The First Amendment accords varying levels of protection to speech.[259] The preliminary inquiry latent and often taken for granted in these cases is whether a person conveys that speech. For example, in *Universal City Studios v. Corley*, the Second Circuit expressed that "[c]ommunication does not lose its constitutional protection as 'speech' simply because it is expressed in the language of computer code."[260] The court considered code like mathematical formulae and musical scores, whose symbolic notations may be "[in]comprehensible to the uninitiated" yet no less deserving of First Amendment protection.[261] If, for instance, someone wrote their novel entirely in binary code, the resulting inquiry would not ask whether the novel was in English.[262] But the argument does not concern whether language or its manifestation is protectible. Rather, it relates the speech to its subject.

Algorithms trouble precisely what makes us human because they appropriate our traditional categories of assimilation. We only understand each other by way of language, but as the Second Circuit seemed to suggest, all language is symbolic.[263] Indeed, in language, there are only differences.[264] For the first time, non-human subjects internalize our languages and communicate with our symbols. An algorithm, no less than a person, thinks; it registers meaning and reacts to linguistic stimuli. The Second Circuit's conclusion that code conveys information by virtue of its instructional nature therefore misplaces the importance of the speaker's agency in such conveyances.[265] Code may perform discrete functions that are

---

259 *See supra* notes 221–24 and accompanying text.

260 *See Corley*, 273 F.3d at 445.

261 *Id.*

262 *Id.* at 445–46.

263 *Id.*

264 FERDINAND DE SAUSSURE, *Identities, Realities, Values*, *in* COURSE IN GENERAL LINGUISTICS 107, 120 (Charles Bally & Albert Sechehaye eds., Wade Baskin trans., N.Y. Phil. Libr. 1959) (1916) ("Whether we take the signified or the signifier, language has neither ideas nor sounds that existed before the linguistic system, but only conceptual and phonic differences that have issued from the system. The idea or phonic substance that a sign contains is of less importance than the other signs that surround it.").

265 *Corley*, 273 F.3d at 447–48.

communicable to other developers, but algorithms employ code to address systematic inquiries. In other words, algorithms speak through code.[266]

2. Government Surveillance Insights

Clearview identifies its software as a research tool for law enforcement agencies.[267] However, there is a disjunction between its mass biometric data collection and its use of such data for law enforcement purposes. By touting its allegiance to law enforcement, Clearview plays into an age-old tradition of excusing privacy intrusions on the basis of public safety.[268] Underlying its practice, though, is a more insidious surveillance that not only harms our tangible privacy interests, but erodes our foundation for intimating others. While its technology is only one degree removed from the location-tracking surveillance found reprehensible in *Carpenter*, it recapitulates the Court's very concern that identifying and tracking people would reveal their "familial, political, professional, religious, and sexual associations."[269]

With respect to government surveillance, courts have been unwilling to take the bait.[270] In 2013, the Guardian released its seminal article detailing the National Security Agency's collaboration with Verizon to collect telephone records on an "ongoing, daily basis."[271]

---

[266] For an insightful discussion of whether algorithms speak and, if so, whether their speech is entitled to First Amendment protections, see Tim Wu, *Machine Speech*, 161 U. PA. L. REV. 1495, 1517–24 (2013).

[267] *Introducing Clearview AI 2.0*, CLEARVIEW AI, https://clearview.ai/ [https://perma.cc/56NZ-RNDT].

[268] *See* Jon Evans, *Personal Privacy vs. Public Security*, TECHCRUNCH (May 6, 2018, 9:00 AM), https://techcrunch.com/2018/05/06/personal-privacy-vs-public-security-fight/ [https://perma.cc/W753-QDHU].

[269] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (citing United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

[270] *See id.* at 2223; *see also* Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated sub nom*, Obama v. Klayman, 800 F.3d 599 (D.C. Cir. 2015); ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015).

[271] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 6:05 AM), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (last visited Apr. 19, 2022); *see also* Ewen Macaskill & Gabriel Dance, *NSA Files: Decoded*, GUARDIAN (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded [https://perma.cc/4RMF-GTSV].

The Snowden leaks, in common parlance, culminated in a lawsuit against the Obama administration for collecting millions of Americans' communication records "indiscriminately and in bulk—regardless of whether they are suspected of any wrongdoing."[272] Through its Bulk Telephony Metadata Program, the government created "an historical repository that permits retrospective analysis."[273] In its defense, the government asserted that the program served the "programmatic purpose of identifying unknown terrorist operatives and preventing terrorist attacks."[274] But the government failed to cite a single instance in which analysis of its data collection actually stopped an imminent attack.[275] The government hoped to appeal to an ideologically entrenched memory—or trauma—in the American psyche to justify large-scale privacy intrusions. Yet, as the court pronounced, Americans could very well combat terrorism in perpetuity.[276]

In *Klayman v. Obama*, the court limited its analysis to the Fourth Amendment, though the same program came under fire two years later.[277] While *Klayman* scrutinized the sheer volume of information available under the program, the Second Circuit focused instead on the quality of information.[278] The program enabled the government to receive metadata concerning every phone call made or received using Verizon for an indefinite period of time.[279] The court mentioned:

> The records demanded are not those of suspects under investigation, or of people or businesses that have contact with such subjects, or of people or businesses that have contact with others who are in contact with

---

272 *Klayman*, 957 F. Supp. 2d at 10.

273 *Id.* at 10, 15.

274 *Id.* at 39 (internal quotations omitted).

275 *Id.* at 40.

276 *Id.* at 32 ("[T]here is the very real prospect that the program will go on for as long as America is combatting terrorism, which realistically could be forever!").

277 *See* ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015).

278 *Id.* at 813.

279 *Id.*

> the subjects—they extend to every record that exists, and indeed to records that do not *yet* exist.[280]

Such a program not only implicates Fourth Amendment privacy rights, but First Amendment ones as well. Collecting data at this scale discourages associational privacies and substantially impairs the precursors to maintaining meaningful relationships.

Courts decline to address First Amendment privacy claims when the Fourth Amendment suffices to address the issue at bar.[281] But, in declining to grapple with the First Amendment implications, they surrender free speech to corporate actors. The First Amendment incurs Fourth Amendment privacy concerns because we lack adequate safeguards against data transfers to law enforcement agencies.[282] Corporate actors have every incentive to collaborate with law enforcement agencies; the government awards handsome contracts.[283] But collaborating with law enforcement agencies to protect against abstract threats fails to satisfy the nexus to determine whether the data collection itself is of public concern.[284] To hold otherwise

---

[280] *Id.* (emphasis in original).

[281] *See, e.g.*, *id.* The Second Circuit avoided reaching conclusions on any constitutional questions, though they appreciated that these concerns played an integral role in their decision and its consequences. *Id. See generally* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112 (2007).

[282] *But see* Molly Davis, *Utah Just Became a Leader in Digital Privacy*, WIRED (Mar. 22, 2019, 8:00 AM), https://www.wired.com/story/utah-digital-privacy-legislation/ [https://perma.cc/DV9X-9QSK] (discussing Utah's Electronic Information or Data Privacy Act, which requires law enforcement to obtain a warrant to access any electronic data held by third parties). While Fourth Amendment analyses are beyond the scope of this Note, I am inclined to suggest that First Amendment protections for corporate data collection and transfers to law enforcement agencies enable the government to circumvent procedural requirements for obtaining warrants and effectively swallow the Fourth Amendment's third-party doctrine.

[283] *See, e.g.*, Kim Lyons, *ICE Just Signed a Contract with Facial Recognition Company Clearview AI*, VERGE (Aug. 14, 2020, 3:19 PM), https://www.theverge.com/2020/8/14/21368930/clearview-ai-ice-contract-privacy-immigration (last visited Apr. 19, 2022); McKenzie Funk, *How ICE Picks Its Targets in the Surveillance Age*, N.Y. TIMES, https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html [https://perma.cc/69EY-6U2H] (June 7, 2021).

[284] Joel Reidenberg resolves the tension endemic to the First Amendment and privacy by proposing a "public significance filter." Rather than focus on the *observability* of information, namely that such information is accessible to the public, Reidenberg insists that courts should focus on the *nature* of the information to determine its public significance. *See* Reidenberg, *supra* note 168, at 155; *see also* Balkin, *supra* note 200, at

would shield corporate actors' profit motivations under the guise of public safety. More explicitly, it obscures "public safety" into a platitude for judicial appeasement.

B. Viewpoint Discrimination

Clearview continues to hang its hat on a baseless First Amendment line.[285] Its principal contention is that its application and computer code are protected speech. Citing a host of cases requiring strict scrutiny standards of review, Clearview seeks to undermine the legitimacy of privacy-based regulations by insisting that they discriminate against content.[286] But the more difficult question is determining whether its application speaks in the first place and, if so, whether it is Clearview that is speaking.[287]

Clearview—and even civil liberties groups like the EFF—insist that "code is speech."[288] At its core, the determination presupposes that all human manifestations of speech will continue, even in their functional capacities, as human speech. Even if courts adhere to this fiction, there are ample ways to reconceptualize the formula from "code is speech" to "code can be speech."

For example, just a year prior to its decision in *Corley*, the Second Circuit considered whether a software program that analyzes futures market transactions and immediately signals users to buy or sell futures contracts was protectible speech.[289] Because the program functioned as an automatic trading program, it did not serve any editorial or otherwise informative capacities.[290] To be sure, the court emphasized that language was involved in conveying the program's commands to its users but only "in an entirely mechanical

---

1205 ("[C]ertain kinds of information constitute matters of private concern not because of their *content*, but because of the *social relationships* that produce them.").

285 *See, e.g.*, State v. Clearview AI, Inc., No. 226-3-20 Cncv, slip op. at 9–10 (Vt. Super. Ct. Sept. 10, 2020).

286 *Id.* (citing Reed v. Town of Gilbert, 576 U.S. 155, 163 (2015)).

287 *Id.* at 12.

288 Schwartz & Crocker, *supra* note 224.

289 Commodity Futures Trading Comm'n v. Vartuli, 228 F.3d 94 (2d Cir. 2000).

290 *Id.* at 111.

way . . . to induce action without the intercession of the mind or the will of the recipient."[291]

The program related little to the heart of the First Amendment.[292] It failed to advance the pursuit of truth, the accommodation among interests, the achievement of social stability, the exposure and deterrence of abuses of authority, personal autonomy and personality development, and the functioning of a democracy.[293] It also misapprehended the locus of inquiry: the First Amendment does not protect speech in the abstract; it protects us against the government limiting our ability to speak about certain things.[294] Just as the First Amendment would not protect engaging in sexual harassment or asking someone to murder your spouse, so too are there necessary limits on software.[295] Government regulations relate to particular kinds of speech—here, particular kinds of code—because they orient toward particular objectives, which is to say, they target what speech does.[296]

---

[291] *Id*.

[292] *Id.*

[293] *See generally* Kent Greenawalt, *Free Speech Justifications*, 89 COLUM. L. REV. 119 (1989).

[294] *See* Neil Richards, *Apple's "Code = Speech" Mistake*, MIT TECH. REV. (Mar. 1, 2016), https://www.technologyreview.com/2016/03/01/161811/apples-code-speech-mistake [https://perma.cc/W2BS-P9RC] ("What matters, in the end, isn't the metaphysics of 'speechiness,' but whether a government regulation of an activity threatens the traditional values of free expression—political dissent, art, philosophy, and the practices of self-government."); *see also* Jaffer & Krishnan, *supra* note 214 ("[C]ourts have looked to the social meaning of the activity in question, asking, for instance, whether the activity belongs to a recognized medium of expression; whether it is intended to convey a message and whether that message is likely to be understood; and, perhaps most important, whether the activity has the effect of informing public discourse . . . .It has always mattered to courts, in other words, what an activity signifies, and what it is, and what it does.").

[295] Richards, *supra* note 294 ("Code = Speech is a fallacy because it would needlessly treat writing the code for a malicious virus as equivalent to writing an editorial in the *New York Times*."); *see also* Andrew Tutt, *Software Speech*, 65 STAN. L. REV. ONLINE 73, 77 (2012) ("Software is sometimes primarily concerned with conveying ideas of the kind and in a manner that one would recognize as familiar and essential to a free society. At other times, software functions much more like a means by which data is gathered, manipulated, and relayed to and by a user and therefore difficult to think of as akin to 'speech.' Software, in other words, should be considered not for what it *is* or even what it *says* but for what it means to society to treat it like speech.").

[296] Eugene Volokh presumes that data privacy laws, for instance, implicate First Amendment concerns and are generally impermissible. However, he only narrowly considered restrictions on the communication of information without considering the

Clearview's last-ditch effort relies on the Supreme Court's latest decision on the First Amendment and data privacy.[297] In response to concerns about brand-name drug marketing, Vermont passed legislation addressing widespread pharmaceutical detailing, a practice whereby manufacturers promote their drugs to physicians and solicit physicians' prescription practices.[298] This latter category, known as "prescriber-identifying information," enables detailers to better determine which physicians are more likely to prescribe their medicines and how to best market their medicines to those particular physicians.[299] Pharmacies regularly obtained this information as a matter of course and federal law, which they sold to data-mining firms.[300] These firms analyzed and leased their reports to manufacturers, informing their marketing techniques and enhancing their sales opportunities.[301] Vermont's legislation prohibited the sale of prescriber-identifying information for marketing purposes, absent the prescriber's consent.[302] The Court determined that Vermont's law enacted both content-based and speaker-based restrictions on the sale, disclosure, and use of prescriber-identifying information.[303]

Sweeping well beyond its caution in *Bartnicki*, the Court declared that information is speech.[304] In its view, facts are the beginning point for speech that is most essential to advance human knowledge and to conduct human affairs.[305] Facts are both formative to and constitutive of knowledge-production. Vermont's legislation

implications of data collection practices themselves. *See* Volokh, *supra* note 198, at 1050–51.

297 Ronald K. L. Collins, *Floyd Abrams' March in Postmodernity: Facial Recognition and the First Amendment*, FIRE (Aug. 19, 2020), https://www.thefire.org/first-amendment-267-floyd-abrams-march-into-postmodernity-facial-recognition-and-the-first-amendment/ [https://perma.cc/62T4-JKQK].

298 Sorrell v. IMS Health Inc., 564 U.S. 552, 557–58 (2011).

299 *Id.* at 558.

300 *Id.*

301 *Id.*

302 *Id.* at 558–59. Interestingly, Vermont—and *Sorrell*, by extension—use prescribers' privacy as a proxy for consumer harms. The Court addressed privacy harms in relation to prescribing physicians rather than affected patients, who actually bore the brunt of manufacturers' detailing successes. *See* Kaminski & Skinner-Thompson, *supra* note 48.

303 *Sorrell*, 564 U.S. at 563–64.

304 *Id.* at 570–71.

305 *Id.* at 570.

exceeded its intentions to protect privacy because it guarded against marketing, but not research, initiatives.[306] It permitted insurers, journalists, and even the state itself to use prescriber-identifying information, just not marketers.[307] Accordingly, the Act failed to advance confidentiality interests.[308] The decision effectively reduced privacy to a truism: privacy exists against everybody or nobody.[309] Divorcing it from its purposes, the Court refrained from the obvious contexts that require privacy and instead contributed to a political economy that materializes information flows to align with broader extralegal profit motivations.[310]

Though the Court's decision in *Sorrell v. IMS Health Inc.* signaled appropriate backlash, certain criticisms overstate its breadth and should give us pause to derive its implications for data privacy.[311] The First Amendment does not protect speech so much as it targets arbitrary restraints on the exercises thereof.[312] Though the Court pronounced that all information is speech, it was especially concerned with legislation incapacitating certain actors from

---

306 *Id.* at 573.

307 *Id.*

308 *Id.*

309 Determining whether privacy exists "against" or "with" the world equally contributes to a normative evaluation of how we conceive privacy as either an individuating or collectivizing force. Whereas the Court implies that privacy exists against the world, that is, as an antagonism enabling our solitude for and with ourselves, we may fare better to think that privacy contributes to conviviality—at least in the strict etymological sense—and cohabitation. For a broader discussion of privacy's positive elements, see Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1918–27 (2013) (arguing that privacy and regulation are compatible with and necessary for self-constitution and innovation).

310 *See* Cohen, *supra* note 214, at 1132 ("Both developments [in commercial speech jurisprudence and free speech rights of corporations generally] reflect an economic reality in which information has increasingly become untethered from industrial production to become a source of value in its own right, and in which powerful interests that profit from information-related activities have systematically resisted regulatory oversight."); *see also* Ashutosh Bhagwat, Sorrell v. IMS Health*: Details, Detailing, and the Death of Privacy*, 36 VT. L. REV. 855, 868 ("[*Sorrell*] governs all information disclosure. In other words, all sales or disclosures of information in the possession of the speaker constitute fully protected speech under the First Amendment.").

311 *See, e.g.*, Neil Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1521–22 (2015); Bhagwat, *supra* note 310, at 868.

312 *See supra* notes 221–24 and accompanying text.

engaging in speech.[313] Notwithstanding legitimate debate over whether corporate marketing should be entitled to heightened scrutiny, *Sorrell* is principally a case about speaker-based discrimination; it entitles corporate actors to engage in and benefit from the same speech as lay persons.[314]

Turning to Clearview, this helps clarify why the company's First Amendment arguments are a lost cause. BIPA provides an indiscriminate ban on nonconsensual biometric data collection. Out of an abundance of caution, the legislation prohibits data that is most integral to our ability to interface in the world. It appeals to growing public concern that major national corporations will manipulate our biometric data and render it insecure, putting us at heightened risk for irreparable forms of identity theft. But BIPA does not discriminate between permissible or impermissible purposes; nonconsensual biometric data collection is, in itself, the issue. Nor does it discriminate among actors. The Act prohibits "private entities"—including individuals and corporations alike—from engaging in such practices and requires them to comply with a host of requirements to secure biometric data. Competing First Amendment interests inform Illinois's legislation: it designates privacy as a precondition to free speech. As critics of facial recognition technologies recognize, surveillance not only encroaches on our privacy, but also undermines core civil liberties.[315] Absent from these criticisms, though, is the more dire possibility that biometric data will be used to undermine our autonomy to exercise subjectivity; it risks someone interfacing in the world as ourselves.[316]

---

313 *Sorrell*, 564 U.S. at 570–71.

314 *Id.* at 565.

315 *See, e.g.*, Jaffer & Krishnan, *supra* note 214 ("Facial recognition in particular is an immensely powerful form of surveillance whose abuse could fundamentally undermine civil liberties, including the liberties the First Amendment is meant to protect. Clearview's technology highlights these dangers. The company's app would allow anyone to identify the protesters who attended a particular political rally, or to identify the people who entered a particular house of worship or medical clinic."); *see also generally* Margot Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICHMOND L. REV. 465 (2015) (arguing that, in addition to chilling speech, surveillance induces conformity with majority opinions).

316 *See* Kashmir Hill & Jeremy White, *Designed to Deceive: Do These People Look Real to You?*, N.Y. TIMES (Nov. 21, 2020), https://www.nytimes.com/interactive/2020/11/21/science/artificial-intelligence-fake-people-faces.html [https://perma.cc/K9B8-6Q8W];

C. Data Collection Is Speech-Related Conduct

Perhaps more obvious is that regulating Clearview's data collection only incidentally burdens speech.[317] Regulating such practices merely targets "speech-related" conduct.[318] In *Hill*, Colorado passed a statute that made it unlawful to solicit or otherwise engage someone in oral protest outside of medical facilities.[319] However, it made no reference to the kinds of speech disallowed and did not infringe on the rights of willing listeners.[320] Rather, it mended the relationship between addressing a willing audience and protecting listeners from unwanted communication.[321] As the Court mentioned, the statute does not regulate speech so much as it regulates places where speech might occur, particularly when pedestrians do not consent to such approaches.[322]

Today, the Supreme Court maintains two distinct regimes respecting its speech-related conduct jurisprudence. On the one side, *Hill* permits content-neutral regulation in public places precisely

---

Pierluigi Paganini, *3D Models Based on Facebook Images Can Fool Facial Recognition Systems*, CYBER DEF. MAG. (Aug. 25, 2016), https://www.cyberdefensemagazine.com/3d-models-based-on-facebook-images-can-fool-facial-recognition-systems/ [https://perma.cc/8UF3-59BU].

317 *See* Balkin, *supra* note 200, at 1196 ("One might argue that data, when collected, collated, used, and sold in bulk, is not speech at all. Rather, it is a commodity, like widgets or soybeans. Vermont made this argument in *Sorrell*; although the Court did not decide the question, Justice Kennedy's majority opinion seemed skeptical."). *But see* Bambauer, *supra* note 21, at 63 ("[F]or all practical purposes, and in every context relevant to the current debates in information law, data is speech. Privacy regulations are rarely incidental burdens to knowledge. Instead, they are deliberately designed to disrupt knowledge creation.").

318 *See* Hill v. Colorado, 530 U.S. 703, 707 (2000). As Neil Richards argues, privacy laws seldom implicate First Amendment concerns because they relate to information-gathering practices rather than information itself. *See* Richards, *supra* note 30, at 1189.

319 *Hill*, 530 U.S. at 707–08.

320 *Id.* at 708.

321 *Id*. at 717 (quoting Am. Steel Foundries v. Tri-City Cent. Trades Council, 257 U.S. 184, 204 (1921)) ("We are a social people and the accosting by one of another in an inoffensive way and an offer by one to communicate and discuss information with a view to influencing the other's action are not regarded as aggression or a violation of that other's rights. If, however, the offer is declined, as it may rightfully be, then persistence, importunity, following and dogging become unjustifiable annoyance and obstruction which is likely soon to savor of intimidation. From all of this the person sought to be influenced has a right to be free, and his employer has a right to have him free.").

322 *Id.* at 719–20.

because it regulates a public place rather than conduct.[323] On the other side—and more recently—the Court has interrogated whether the First Amendment permits regulating speech in public. In *Snyder v. Phelps*, the Westboro Baptist Church protested a military funeral, garnishing signs that read a host of inflammatory, if not outright pejorative, slurs.[324] The plaintiffs alleged state law tort claims, including defamation, publicity given to private life, intentional infliction of emotional distress, intrusion upon seclusion, and civil conspiracy, but did not point to any legislative regulation.[325] In spite of the Church's grotesque speech, the Court held firmly to the principle that speech which offends ordinary sensibility deserves protection.[326] Of particular importance, the Court applauded the Church's compliance with public officials' instructions for staging their demonstration, but made no comment on the First Amendment implications of public officials delegating where protests can happen in the first place.[327] Nor did they expound on the differences between exercising First Amendment rights against common law causes of action as opposed to explicit regulations.

Taking *Hill* as its inspiration, Massachusetts enacted a similar statute that barred solicitations and counseling outside of abortion clinics.[328] Except, unlike the Colorado statute, Massachusetts outlawed knowingly standing on a public way within the clinics' vicinity.[329] Despite the law having the "inevitable effect" of restricting abortion-related speech, the Court determined that the otherwise facially neutral law does not become content-based by virtue of its

---

323 *Id.*

324 Snyder v. Phelps, 562 U.S. 443, 448 (2011).

325 *Id.* at 450.

326 *Id.* at 460–61 ("Westboro's funeral picketing is certainly hurtful and its contribution to public discourse may be negligible. But Westboro addressed matters of public import on public property, in a peaceful manner, in full compliance with the guidance of local officials. . . . Speech is powerful. It can stir people to action, move them to tears of both joy and sorrow, and—as it did here—inflict great pain. On the facts before us, we cannot react to that pain by punishing the speaker. As a Nation we have chosen a different course—to protect even hurtful speech on public issues to ensure that we do not stifle public debate.").

327 *Id.*

328 McCullen v. Coakley, 573 U.S. 464, 469–70 (2014).

329 *Id.*

disproportionate effect on certain kinds of speech.[330] Massachusetts failed to demonstrate that its law narrowly served governmental interests in preserving public safety because it banned standing, as opposed to soliciting, by the clinics.[331] The Court's decision can best be understood as differentiating between regulations against being in public versus doing something in public. The former disables a portion of a "traditional public forum," which curtails the possibility for speech to occur at all.[332] The latter, on the other hand, targets a relational action; it bars certain ways of conveying information to others within a given context rather than encroaching on its access to be in public and access information therein.

Clearview's facial recognition technology offends First Amendment jurisprudence, conflating access to data with its more insidious data-collection conduct. All the more so, corporate actors operating such technologies turn the internet into a microcosm for our world without appropriating its prevailing norms about privacy. We do not need new privacy norms to define our digital lives; the "real world" and "digital world" is a false dichotomy.[333] Our existing norms suffice to draw analogies to our digital lives and satisfy demands for our continued privacy. The internet reiterates a template for a world we already inhabit.[334] By infiltrating social media networks to

---

330 *Id.* at 480.

331 *Id.* at 494 ("Although respondents claim that Massachusetts 'tried other laws already on the books,' they identify not a single prosecution brought under those laws within at least the last 17 years." (citation omitted)).

332 *Id.* at 497.

333 In light of digital reconfigurations of norms surrounding in- and co-habitation, academics and artists have indulged new philosophical discussions about "worlding." For more thorough discussions of the concept, see Ian Cheng, *Worlding Raga: 2—What Is a World?*, RIBBONFARM (Mar. 5, 2019), https://www.ribbonfarm.com/2019/03/05/worlding-raga-2-what-is-a-world/ [https://perma.cc/24ZG-LQJJ]; Helen Palmer & Vicky Hunter, *Worlding*, NEW MATERIALISM (Mar. 16, 2018), https://newmaterialism.eu/almanac/w/worlding.html [https://perma.cc/6KXB-B87N].

334 In response to Google entering their property to photograph their home for Google Maps, a couple brought suit against the company for intrusion upon seclusion. Boring v. Google Inc., 362 Fed. App'x. 273, 276 (3d Cir. 2010). The court determined:

> "No person of ordinary sensibilities would be shamed, humiliated, or have suffered mentally as a result of a vehicle entering into his or her ungated driveway and photographing the view from there. . . . Thus, what really seems to be at the heart of the complaint is not Google's fleeting presence in the driveway, but the photographic image captured

collect biometric data, Clearview arguably trespasses its terrain in derogation of its terms of use.[335] It also collects beyond what is readily ascertainable in our public images, that is, it derives information and draws implications beyond the images taken as a whole.[336] Instead, its algorithm relates information internal to each image to recognize patterns and reach identification.[337] Until we receive adequate federal protections for our data, companies like Clearview will make every effort to manipulate courts to presume their data-collection practices falls under permissible speech and—more troublingly—that our faces are facts worth communicating.

CONCLUSION

In response to public scrutiny, facial recognition technologies are becoming increasingly taboo. Many jurisdictions have outright banned them.[338] Even several prominent corporate actors—some of

> at that time. The existence of that image, though, does not in itself rise to the level of an intrusion that could reasonably be called highly offensive. Significantly, the Borings do not allege that they themselves were viewed inside their home, which is a relevant factor in analyzing intrusion upon seclusion claims."

Id. at 279. Despite the Borings failure to redress their alleged privacy harms, the court recognized that Google may still have trespassed on their property. *Id.* at 283.

[335] Although his analysis is limited to the Computer Fraud and Abuse Act, Orin Kerr offers invaluable insights to the ongoing discussion around "computer trespass." *See generally* Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143 (2016).

[336] *See* discussion *supra* Part III.A.

[337] *See supra* note 154 and accompanying text.

[338] *See, e.g.*, Brianna Sacks et al., *Los Angeles Police Just Banned the Use of Commercial Facial Recognition*, BUZZFEED NEWS (Nov. 17, 2020, 6:08 PM), https://www.buzzfeednews.com/article/briannasacks/lapd-banned-commercial-facial-recognition-clearview [https://perma.cc/VKE3-S34P]; Kate Conger et al., *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html [https://perma.cc/75BY-4593]; Jay Peters, *Portland Passes Strongest Facial Recognition Ban in the U.S.*, VERGE (Sept. 9, 2020, 10:41 PM), https://www.theverge.com/2020/9/9/21429960/portland-passes-strongest-facial-recognition-ban-us-public-private-technology (last visited Apr. 19, 2022); Ali Tadayon, *Oakland Bans City Use of Facial Recognition Technology*, E. BAY TIMES, https://www.eastbaytimes.com/2019/07/16/oakland-bars-city-from-using-facial-recognition-technology/ [https://perma.cc/95ZS-QWN7] (July 17, 2019, 2:46 PM); Levi Sumagaysay, *Berkeley Bans Facial Recognition*, MERCURY NEWS (Oct. 16, 2019, 4:23 PM), https://www.mercurynews.com/2019/10/16/berkeley-bans-facial-recognition/ (last visited Apr. 19, 2022); Ally Jarmanning, *Boston*

whom previously employed such technologies—refrain from using them.[339] These technologies pose considerable threats to our ability to navigate the world devoid of concern that powerful actors, corporate and governmental ones alike, will further their control interests over and against our own. The problem is not that facial recognition technologies are neither refined nor accurate enough. Rather, it is that they risk exacerbating existing social ills and encouraging efficiencies that streamline the wrong processes.[340]

Our last decade was marked by perennial debates over corporate personhood. President Barack Obama and Senator Elizabeth Warren decried our inverted relationship to powerful companies in a single phrase: corporations are not people.[341] As data collection pervades our daily lives and tech giants reinscribe our privacy norms,[342] an overwhelming malaise gestures us towards nihilism. But the new decade has only excavated old issues. To rein in these excesses, we need more than comprehensive federal legislation; we must

---

Lawmakers Vote to Ban Use of Facial Recognition Technology by the City, NPR (June 24, 2020, 7:05 PM), https://www.npr.org/sections/live-updates-protests-for-racial-justice/2020/06/24/883107627/boston-lawmakers-vote-to-ban-use-of-facial-recognition-technology-by-the-city [https://perma.cc/C63V-5JRT].

339 *See, e.g.*, Jay Peters, *IBM Will No Longer Offer, Develop, or Research Facial Recognition Technology*, VERGE (June 8, 2020, 8:49 PM), https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software (last visited Apr. 19, 2022); Karen Weise & Natasha Singer, *Amazon Pauses Police Use of Its Facial Recognition Software*, N.Y. TIMES (June 10, 2020), https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html? [https://perma.cc/8GBF-ULRD]; Brad Smith, *Facial Recognition: It's Time for Action*, MICROSOFT (Dec. 6, 2018), https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/ [https://perma.cc/8LFT-RJSH].

340 *See generally* Margaret Hu, *Algorithmic Jim Crow*, 86 FORDHAM L. REV. 633 (2017); *see also* Woodrow Hartzog & Evan Selinger, *Facial Recognition Is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66 [https://perma.cc/HHZ2-ZLSA].

341 Kent Greenfield, *If Corporations Are People, They Should Act Like It*, ATLANTIC (Feb. 1, 2015), https://www.theatlantic.com/politics/archive/2015/02/if-corporations-are-people-they-should-act-like-it/385034/ [https://perma.cc/GK82-P74B] (alluding to Citizens United v. Fed. Elections Comm., 558 U.S. 310 (2010)). *But cf.* Fed. Commc'ns Comm. v. AT&T Inc., 562 U.S. 397, 409–10 (2011) (holding that corporations are not entitled to "personal privacy" from disclosing law enforcement information under the Freedom of Information Act).

342 *See* Matthew Tokson & Ari Waldman, *Social Norms in Fourth Amendment Law*, 120 MICH. L. REV. 265, 298–301 (2021).

fundamentally reorient the trajectory of our civil liberties back to the Constitution's human origin. Neither corporations nor computers promise salvation. If nothing else, the new decade will reckon with whether we are prepared to reclaim ourselves from our inventions and renew our humanity.