The Death of the Data Subject

Gordon Hull / UNC Charlotte / ghull@uncc.edu

Abstract. This paper situates the data privacy debate in the context of what I call the death of the data subject. My central claim is that concept of a rights-bearing data subject is being pulled in two contradictory directions at once, and that simultaneous attention to these is necessary to understand and resist the extractive practices of the data industry. Specifically, it is necessary to treat the problems facing the data subject structurally, rather than by narrowly attempting to vindicate its rights. On the one hand, the data industry argues that subjects of biometric identification lack legal standing to pursue claims in court, and Facebook recently denied that that its facial recognition software recognizes faces. On the other hand, industry takes consent to terms of service and arbitration clauses to create enforceable legal subject positions, while using promises of personalization to create a phenomenological subject that is unaware of the extent to which it is being manipulated. Data subjects thus have no legal existence when it is a matter of corporate liability, but legal accountability when it is a matter of their own liability. Successful reform should address the power asymmetries between individuals and data companies that enable this structural disempowerment.

Keywords. Privacy – Subjectivity – Big Data – Biometrics

According to a widespread narrative about information privacy, individuals choose to disclose information about themselves to various entities in return for something of value. Although it continues to form policy, the conceptual basis of this narrative has been widely criticized on both theoretical and practical grounds. In particular, people produce and release large amounts of information about themselves involuntarily and in a variety of ways that escape conceptualization as "consent." At the same time, information both from others and from the structures of social networks allows accurate inferences to be made about people without their disclosing their own information at all. In other words, this "notice and consent" model for protecting personal information is based on a model of judicial subjectivity that has collapsed under the weight of data generation and mining. That collapse has led to a large body of

innovative work attempting to conceptualize what privacy protects and how it might be more adequately conceptualized.[1]

In what follows, I situate the privacy debate in the context of what I will call the death of the data subject. My central claim is that concept of a rights-bearing data subject is being pulled in two contradictory directions at once, and that simultaneous attention to these is necessary to understand and resist the extractive practices of the data industry. Specifically, it is necessary to treat the problems facing the data subject structurally, rather than by narrowly attempting to vindicate its rights. In part 1, I offer a schematic outline of what I mean by the data subject and of these two opposing pressures on it. Part 2 focuses on efforts by industry to deny legal standing to subjects of biometric identification and on an effort by Facebook to deny that its facial recognition software recognizes faces. Part 3 argues that industry takes consent to terms of service and arbitration clauses to create enforceable legal subject positions, while using promises of personalization to create a phenomenological subject that is unaware of the extent to which it is being manipulated. Part 4 discusses what a progressive politics of privacy might look like in the context of this dissonance; rather than attempting to vindicate the rights of the data subject, law should address the constitutive power asymmetries between data subjects and data companies.

I. What is a Data Subject?

[1] The most influential such account may be Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Palo Alto: Stanford University Press, 2010). Other examples include Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge: Cambridge University Press, 2018). (conceptualizing privacy as an aspect of social trust) and Julie E. Cohen, "What Privacy is For," *Harvard Law Review* 126 (2013). (arguing that the liberal subject underpinning privacy debates is a construct).

Basic legal concepts and terms turn out both to be surprisingly difficult to specify in practice and to conceal differential power relations. Consider, for example, the concept of "author" or "creator" in intellectual property law. If popular imaginaries of authorship often involve notions of solitary creators drawn from literary romanticism, current legal constructions of authorship are primarily about assigning property entitlements. Furthermore, mainstream intellectual property jurisprudence is much more concerned with providing incentives to create than protecting the moral rights of "authors." Indeed, as "work for hire" doctrine underlines, the "author" of a work may not even be its creator. In this context, intellectual property law serves to modulate and foster specific kinds of social and economic relations outside the law itself. In particular, it works to foster certain kinds of subjectivity as it works to mediate individuals' creation and consumption of cultural goods.[2]

As Lawrence Lessig demonstrated, technological developments can also put pressure on legal concepts by revealing ambiguities latent in existing law.[3] For example, when the Fourth Amendment was framed, any search could be conceived both as an affront to the dignity of the person searched and as disruptive of their lives. The development of electronic surveillance separates these functions, allowing non-disruptive searching. As a result, it is necessary to revisit the imaginary behind the concept of "search" in order to understand what political values its limitation is designed to express. In this case, Lessig follows William Stuntz to argue that the Fourth and Fifth Amendments ought to be construed together as an effort to limit state power by

---

[2] For intellectual property law and power, see Gordon Hull, *The Biopolitics of Intellectual Property: Regulating Innovation and Personhood in the Information Age* (Cambridge: Cambridge University Press, 2020). For literary romanticism in IP, see James Boyle, *Shamans, Software and Spleens: Law and the Construction of the Information Society* (Cambridge, MA: Harvard University Press, 1997). and for works for hire, see *Community for Creative Non-Violence v. Reid*, 490 U.S. 730 (1989).

[3] Lawrence Lessig, *Code and other Laws of Cyberspace* (New York: Basic Books, 1999).

making it harder to prosecute certain crimes, as for example heresy in the seventeenth century.[4] Lessig's analysis thus suggests the importance of both the sociopolitical conditions in which legal concepts become salient and the specific power relations that those legal concepts work to create and sustain.

The rapid developments of data-driven economic relations and concomitant social practices are putting analogous pressure on privacy as a tort and on the conceptual understanding of subjectivity that implicitly underpins it. This view of subjectivity, broadly aligned with modern liberalism, imagines a stable reference point, acting causally on the world; although such a subject responds to things in the world, those things in the world are not generally taken to be constitutive of her subjectivity in a fundamental way. As the example of copyright makes clear, this latter model of subjectivity is common across any number of legal regimes.[5] In privacy, the paradigmatic case is in notice-and-consent regimes, which tend to model an agent – a data or privacy subject - who controls information about herself. These regimes trace back to the late nineteenth century, and complaints about unwanted intrusion by mass media.[6]

Current data collection practices work under the surface of these individuals, not just collecting information about them, but modifying them and treating them as malleable collections of points of information. In so doing, they make the liberal view of subjectivity an increasingly poor fit with current data practices; "data" is the space where this stable subjectivity

---

[4] William J. Stuntz, "The Substantive Origins of Criminal Procedure," *Yale Law Journal* 105 (1995).

[5] See also the discussion in Mala Chatterjee and Jeanne C. Fromer, "Minds, Machines, and the Law: The Case of Volition in Copyright Law," *Columbia Law Review* 119 (2019). and the critique in Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (New Haven: Yale University Press, 2012).

[6] Jennifer Rothman makes a compelling case that this data subject has survived in publicity law, which envisions someone who attempts to monetize a lack of privacy. As Rothman notes, the aggrandizement of protection for the subject of publicity law accompanies the impoverishment of protection of subjects who want to maintain their privacy. Jennifer E. Rothman, *The Right of Publicity: Privacy Reimagined for a Public World* (Cambridge. MA: Harvard University Press, 2018).

slips away and our identity is lost, because to locate any of us as data subjects – to identify what we do and are predictively likely to do – is not to locate a transcendental principle of organization, but to name a particular mixture of networks of data points. The promise of data-based targeting, whether by advertising or surveillance, is the singularity of its object. Unlike even previous advertising, which identified its targets by externally-imposed demographic categories and then by focus groups, the ideal target of a data-supported intervention is singular: a unique collection of nudge-able desires, different not only from other possible targets, but from itself at different times.[7] Every action the data subject takes, and every action by anyone else whose data goes into the assessment of that subject, subtly changes how the subject is assessed and targeted. Who I am for Google's ad servers at exactly this moment is not identical to who I will be in even a few minutes, even if I do absolutely nothing.

This data subject is dead in the sense that it lacks both stability and a sense in which it exists exogenously to the world in which it acts. There is no reductive principle at work to lend it these attributes; rather, there are only discrete moments of reduction. That is, there is no underlying substrate to render a subject coherent; instead, the data subject is reconstituted at every moment out of the data and actions that surround it. Because of this process of re-creation, there is no way to create a reference point outside of its actions. Instead, the subject is always constituted in order to lead to certain behaviors. The goal is not to know the data subject, but to move it to buy or retweet something. These endpoints are inherent to the subject's constitution. That the goal is to cause the data subject to do something underscores that, despite the death of

---

[7] For the move from demographic categories to focus groups, see Adam Arvidsson, "On the 'Pre-History of the Panoptic Sort:' Mobility in Market Research," *Surveillance and Society* 1, no. 4 (2004), http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3331. For the complexities behind the singularized data subject, and its non-constancy, see, *e.g.*, John Cheney-Lippold, *We Are Data: Algorithms and the Making of Our Digital Selves* (New York: NYU Press, 2017).

the data subject as a substance or causal principle, there is nonetheless an organizing political logic to it. Here, the concept of the data subject does real work in that it permits organizing an economy based on targeting.

This admittedly abstract characterization has legal implications. Data companies would very much like to avoid being constrained by existing legal regimes. As Julie Cohen has persuasively demonstrated, the combination of the wealth, novelty, and political savvy of these companies in the context of a more general neoliberalization of the economy has enabled a slow restructuring of the legal order to suit their interests.[8] In the specific case of the data subject, the goal is to avoid accountability to legal categories traditionally associated with liberal juridical subjects. Accordingly, companies like Facebook vehemently argue that their data subjects are not the same data subjects as contemplated by existing legal regimes. This strategy is particularly evident in litigation around facial recognition and other forms of biometric identification. At the same time, they will also argue that the data subject who "agrees" to terms of service is precisely the sort of stable agent contemplated by traditional legal regimes.

II. Biometric Identification: The Data Subject is Dead!

Biometric identification technology is an emerging privacy mess. Ethical concern with biometric technologies in general is longstanding, and recent research shows that people are generally quite uncomfortable with biometric identification outside of local security contexts (like unlocking a smart phone), and are willing to forego benefits to avoid it.[9] The core

---

[8] Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford: Oxford University Press, 2019). For a further development of this point, see also Ari Ezra Waldman, "Privacy, Practice, and Performance," *California Law Review* 110 (forthcoming) (2021).

[9] See, *e.g.*, Anton Alterman, "'A piece of yourself:' Ethical Issues in Biometric Identification," *Ethics and Information Technology* 5, no. 3 (2003), https://doi.org/10.1023/B:ETIN.0000006918.22060.1f. (arguing that

conceptual problem was noted several years ago by Woodrow Hartzog and Frederic Stutzman, who point out that identified photos and other biometric records are searchable, which "significantly erodes the protection of obscurity, and, consequently, threatens a user's privacy."[10] Machine identification automates and generalizes the process, thereby enabling the rapid creation of searchable records of the activities and records of people, often without their consent. Because an individual's biometric features remain both unique to them and constant over time, these records present the possibility of permanent individuation.[11] Such records "can reduce the cost of sorting, categorizing, discriminating, and denying opportunities, benefits, or needed support and treatment in furtherance of surveillance capitalism."[12]

Facial recognition is even more problematic because of a combination of the centrality of faces to social interaction, the wealth of data that can be mined from facial recognition systems, the comparatively low cost of their deployment (they require no direct physical contact), and a general lack of regulation.[13] Worse still, facial recognition systems perform poorly in identifying darker-skinned people, especially Black women, magnifying the risks to already minoritized

---

biometric identification instrumentalizes one's body and so fails on Kantian grounds, and that there should be a presumption against its use). For survey data, see Matthew B. Kugler, "From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms," *U.C. Irvine Law Review* 10 (2019).

[10] Woodrow Hartzog and Frederic Stutzman, "The Case for Online Obscurity," *California Law Review* 101, no. 1 (2013): 47.

[11] April Glaser, "Biometrics Are Coming, Along With Serious Security Concerns," *Wired*, March 9, 2016, https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/. (also noting that biometrics like faces and fingerprints are often publicly accessible, and so vulnerable to hacking, appropriation by law enforcement, etc.).

[12] Neil Richards and Woodrow Hartzog, "The Pathologies of Digital Consent," *Washington University Law Review* 96 (2019): 1485. If the data is breached, all of these risks are magnified and the resulting harms can drag on for years: see Daniel J. Solove and Danielle Keats Citron, "Risk and Anxiety: A Theory of Data-Breach Harms," *Texas Law Review* 96 (2018).

[13] Evan Selinger and Woodrow Hartzog, "The Inconsentability of Facial Surveilance," *Loyola Law Review* 66 (2019); Evan Selinger and Brenda Leong, "The Ethics of Facial Recognition Technology," in *The Oxford Handbook of Digital Ethics*, ed. Carissa Véliz (Oxford: Oxford University Press, forthcoming).

communities and magnifying social inequalities.[14] Efforts to fix this problem are often themselves problematic: even if accurate facial recognition is good in the abstract, there are good reasons for Black Americans to be skeptical of increased legibility to the state. Indeed, Black legibility has a long history as a technique of white supremacy.[15]

A few states have passed legislation to protect biometric information; the Biometric Information Privacy Act (BIPA) in Illinois is the most comprehensive.[16] The law establishes an opt-in, notice-and-consent procedure for private use of biometric information. It is a modest initial step, subject to the well-documented limitations to notice-and-consent privacy.[17] Nonetheless, it involves a subtly different imagination of privacy practice and its enforcement, and has as a result been vociferously opposed by the data industry. First, the regime is opt-in, not opt-out: unlike much current and proposed privacy legislation, BIPA does not presume data collection is legitimate unless someone objects. Second, uniquely among current biometric privacy laws, it establishes a private right of action. Individuals can sue under the statute, and do

---

[14] Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" (Proceedings of the 1st Conference on Fairness, Accountability and Transparency, New York, 2018).

[15] Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Durham, NC: Duke University Press, 2015).

[16] See Michael A. Rivera, "Face Off: An Examination of State Biometric Privacy Statutes and Data Harm Remedies," *Fordham Intellectual Property, Media & Entertainment Law Journal* 29, no. 2 (2019). (discussing the Texas, Washington and Illinois statutes, emphasizing various weaknesses in the regimes and noting that only Illinois involves a private right of action).

[17] Most generally, in line with the argument here, the formalization of consent makes power and information asymmetries invisible. For problems with notice-and-consent, see, *e.g.*, Daniel J. Solove, "Privacy Self-Management and the Consent Dilemma," *Harvard Law Review* 126 (2013); Alessandro Acquisti, Laura Brandimarte, and George Loewenstein, "Privacy and human behavior in the age of information," *Science* 347, no. 6221 (2015), https://doi.org/10.1126/science.aaa1465; Gordon Hull, "Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data," *Ethics and Information Technology* 17, no. 2 (2015), https://doi.org/10.1007/s10676-015-9363-z; Katherine J. Strandburg, "Free Fall: The Online Market's Consumer Preference Disconnect," *University of Chicago Legal Forum* 2013 (2013); Joshua A. T. Fairfield and Christoph Engel, "Privacy as a Public Good," *Duke Law Journal* 65 (2015); Cohen, *Between Truth and Power*., ch. 2; Richards and Hartzog, "The Pathologies of Digital Consent.". Rivera "Face Off." emphasizes the risks of private litigation in data breach suits; even in Illinois, these include the high cost of litigation and difficulty in getting class certification.

not need to wait for action by state attorneys general. The law thus explicitly recognizes the data subject implicit in the notice-and-consent imaginary and attempts to empower it to claim its rights. This is important because, as Ari Ezra Waldman has shown, when it remains implicit, this imaginary is often significantly reshaped in practice by corporate involvement in statutory implementation and enforcement.[18] As I will argue, the litigation strategy of Facebook shows the limits of BIPA's reformed imaginary; to the extent that that BIPA tries to empower a judicial subject, Facebook claims that such a subject does not exist.

BIPA presents a significant threat to Facebook because it regulates photo-tagging. As the 9th Circuit described the process:

> When a photo is uploaded, the technology scans the photo and detects whether it contains images of faces. If so, the technology extracts the various geometric data points that make a face unique, such as the distance between the eyes, nose, and ears, to create a face signature or map. The technology then compares the face signature to faces in Facebook's database of user face templates …. If there is a match between the face signature and the face template, Facebook may suggest tagging the person in the photo.[19]

A group of representative Illinois Facebook users sued the company and filed for class certification, citing Facebook's failure to obtain consent for any of this.

Facebook followed a two-pronged strategy in attempting to defeat this litigation. On the one hand, the company has argued that the interests protected by the law are not substantive; on the other hand, it has argued that its software does not actually recognize faces. Together, these exemplify a strategy premised on the death of the data subject: there is no juridical subject whose right to control her information is implicated, both because the data collection in question falls below a threshold for legal intelligibility, and because the software does not target such a subject

---

[18] Waldman, "Privacy, Practice, and Performance."
[19] *Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019), 1268.

in the first place. As I will indicate, this strategy eventually failed, but recent Supreme Court jurisprudence suggests that its likelihood of success is increasing, at least at the federal level.

1. Standing, Round 1: Is there a substantive interest in biometric privacy?

One way judicial subjectivity is operationalized is standing doctrine, and evidence that the data subject is dead would include its inability to obtain legal standing. Under Article III of the U.S. Constitution, someone has standing to bring a claim in (federal) court if they can successfully allege an injury that is "concrete, particularized, and actual or immanent; fairly traceable to the challenged action; and redressable by a favorable ruling."[20] Victims in data breach cases have had a difficult time with this threshold requirement, in part because courts tend to view the harms as distant or speculative.[21] Because it concerns similar interests, litigation over BIPA has substantially been a contest over standing.

The Facebook litigation is framed by *Rosenbach v. Six Flags* (2019), an Illinois Supreme Court case involving an amusement park that used thumbprints to identify customers who had bought a season pass, in order both to admit them quickly and to stop people from sharing passes. According to BIPA, if the company wants to collect such information, it has to inform customers in writing, and get their affirmative consent. Alexander Rosenbach's mother signed him up for a season pass to Six Flags online, in anticipation of a school field trip. Once he got there, Alexander was shuttled to a kiosk where the park completed the sign-up, which included thumbprinting him. The park did not provide the required documentation anywhere in the process, and his mother sued.

---

[20] *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013), 409.
[21] Solove and Citron, "Risk and Anxiety."

Six Flags' response was to deny that BIPA provided substantive privacy protections by arguing that, although they technically violated the statute, Rosenbach was nevertheless not "aggrieved" under the law since a mere procedural violation of the statute did not add up to an "actual injury or harm, apart from the statutory violation itself."[22] Indeed, federal courts often deny standing when a law establishes an entitlement to a procedural protection against a harm, rather than a substantive harm itself.[23] The question for BIPA, then, is whether a violation is procedural or substantive, and some early federal caselaw suggested that plaintiffs lacked standing when they failed to demonstrate an immanent privacy harm.[24]

The Illinois Supreme Court rejected this argument both on the merits and as a matter of statutory interpretation. On the merits, the Court notes that:

> When a private entity fails to adhere to the statutory procedures, as defendants are alleged to have done here, "the right of the individual to maintain [his or] her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized." This is no mere "technicality." The injury is real and significant. …. The situation is particularly concerning, in the legislature's judgment, because "[t]he full ramifications of biometric technology are not fully known."[25]

That is, the harm against which Rosenbach protects is a substantive one in the sense that Rosenbach has named an interest that is itself legally protectable, without showing of further

---

[22] *Rosenbach v. Six Flags Entertainment Corp.*, 129 N.E.3d 1197 (Sup. Ct. Illinois 2019), 1204. (¶22)

[23] For example, compare *Kearns v. Cuomo*, 2020 U.S. App. LEXIS 37384 (2nd Cir. 2020). (denying standing in a case where a tire dealer failed to assist a customer in registering new tires with the manufacturer, as required by the National Traffic and Motor Vehicle Safety Act of 1966) with *Aranda v. Caribbean Cruise Line, Inc.*, 202 F. Supp. 3d 850 (ND Illinois 2016). (refusing to rule against the plaintiff's standing on summary judgment in a case involving unwanted telemarketing, explaining that "Congress has identified that such unsolicited telephonic contact constitutes an intangible, concrete harm, and plaintiffs have alleged such concrete harms that they, themselves suffered" (858)).

[24] See *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499 (S.D.N.Y. 2017)., finding among other things that procedural violations of BIPA did not demonstrate a "material risk of harm." In the wake of the Supreme Court's decision in *Ramirez v. TransUnion* (2021), it seems quite possible that federal courts will increasingly rule against plaintiffs in analogous cases involving BIPA, sending litigation back to state courts. See section 4, below, for *TransUnion*.

[25] *Rosenbach*, 129 N.E.3d 1206. (¶34-5)

injury beyond its infringement. As a matter of statutory interpretation, the Illinois Court notes that the law's provision of statutory liability "whether or not actual damages, beyond violation of the law's provisions, can be shown" is "as integral to implementation of the legislature's objectives as the" notice-and-consent requirements, since the threat of private lawsuits is the law's only enforcement mechanism and since a regime of statutory liability provides "the strongest possible incentive to conform to the law and prevent problems before they occur and cannot be undone."[26] This holding is however specific to Illinois, and the standing requirements in federal court are different.

In the federal litigation, Facebook accordingly made a slightly different standing argument, claiming that the privacy violation involved in photo-tagging is not a substantive one because it is not "concrete" under *Spokeo v. Robins* (2016). In that case, Robins argued that Spokeo's profile inaccurately (and thus actionably under the Fair Credit Reporting Act) "state[d] that he is married, has children, is in his 50's, has a job, is relatively affluent, and holds a graduate degree." Justice Alito's opinion emphasized that standing requires demonstrating an injury that is both "concrete and particularized" and sends the case back to the 9th Circuit on the grounds that it only considered particularity but not concreteness. That is, Robins had demonstrated that the inaccurate information was specific to him, but the Court had not considered whether he demonstrated more than procedural violation of the law. As an example, Alito suggested an inaccurately reported zip code, because "it is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm."[27]

---

[26] *Rosenbach*, 129 N.E.3d 1207. (¶37)

[27] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016), 1550.. One might object that it is not hard to imagine how an inaccurately reported zip code might cause concrete harm, because it could negatively affect one's credit score and thus job and other prospects. On the importance of FICA score, see Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Cambridge, MA: Harvard University Press, 2015).

On remand, the 9th Circuit emphasized that "given the ubiquity and importance of consumer reports in modern life—in employment decisions, in loan applications, in home purchases, and much more—the real-world implications of material inaccuracies in those reports seem patent on their face."[28] That is, reporting inaccurate credit information is itself a substantive harm. The Court then argued that the publication of the kinds of inaccurate information Robins alleges rises above the inaccurate zip-code standard, since "even seemingly flattering inaccuracies can hurt an individual's employment prospects as they may cause a prospective employer to question the applicant's truthfulness or to determine that he is overqualified for the position sought."[29] The Court accordingly concluded that Robins has met the requirements for standing.

In assessing standing in the FB litigation, the 9th Circuit picks up on the concreteness language from *Spokeo*. It begins by noting a long history of instances where privacy is viewed as substantive right with roots in common law. The Court also cites Supreme Court jurisprudence noting that technological advances can implicate these substantive interests. The Court notes that:

> Once a face template of an individual is created, Facebook can use it to identify that individual in any of the other hundreds of millions of photos uploaded to Facebook each day, as well as determine when the individual was present at a specific location. Facebook can also identify the individual's Facebook friends or acquaintances who are present in the photo …. It seems likely that a face-mapped individual could be identified from a surveillance photo taken on the streets or in an office building. Or a biometric face template could be used to unlock the face recognition lock on that individual's cell phone.[30]

---

[28] *Robins v. Spokeo, Inc.*, 867 F.3d 1108 (9th Cir.), 1114.
[29] *Spokeo (9th Cir.)*, 867 F.3d 1117.
[30] *Patel v. FB*, 932 F.3d 1274.

The Court concludes that similar privacy invasions would be actionable under common law. Since "Facebook's alleged collection, use, and storage of plaintiffs' face templates here is the very substantive harm targeted by BIPA," the Court concludes that the *Spokeo* standard has been met.[31]

As these cases illustrate, standing operates as a reductive principle in that it narrows and organizes the indefinitely large universe of possible interests and harms into those that cause injury to someone who could demand their protection. Clearly some sort of organizing principle is necessary in that a functioning judiciary depends on the finitude of possible claims. However, the specific determinations of what interests are actionable is a political one. That is, there is a political economy of data at work behind Facebook's argument, and a competing political economy behind BIPA. Facebook depends on biometric data being part of what Julie Cohen calls the biopolitical public domain as there for the taking; BIPA construes that information as alienable and thus under the aegis of traditional norms associated with property.[32] In this context, Facebook's litigation strategy is legible as an assertion that certain kinds of information are so far removed from personhood that there is no subject position from which their protection matters. In rejecting it, the 9th Circuit relied on the close connections between biometric surveillance and personal identity.

2. Does the software analyze faces?

---

[31] *Patel v. FB*, 932 F.3d 1275.

[32] For "biopolitical public domain," see Cohen, *Between Truth and Power*.; for "there for the taking," see also Nick Couldry and Ulises A. Mejias, "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject," *Television & New Media* 20, no. 4 (2018), https://doi.org/10.1177/1527476418796632.

One way to declare the data subject dead is to deny it standing. Another is to argue that it is irrelevant. Here the question is: does Facebook's software violate the law, *i.e.*, does it collect and process biometric identifiers? Facebook argues that it does not. The district court outlined the issue as follows:

> Plaintiffs say the technology necessarily collects scans of face geometry because it uses human facial regions to process, characterize, and ultimately recognize face images. Facebook disagrees and says the technology has no express dependency on human facial features at all. Rather, according to Facebook, the technology "learns for itself what distinguishes different faces and then improves itself based on its successes and failures, using unknown criteria that have yielded successful outputs in the past."[33]

Facebook's litigation strategy here expressly tries to interpret the question of juridical subjectivity as resolved solely by the details of its software. More specifically, the argument depends on distinguishing what one might call the functional and phenomenal attributes of facial recognition, and then claiming that the software recognizes faces in the functional sense, but that the law requires that it do so in the phenomenal one.

I draw this distinction from a recent paper on artificial intelligence (AI) in the law by Mala Chatterjee and Jeanne Fromer, which points to an emerging need to know "whether machines can have mental states, or – at least – something sufficiently like mental states for the purposes of the law."[34] Their focus is primarily on copyright, and the act of infringement specifically, but they underscore that mental state requirements are ubiquitous in law, covering everything from torts to crime. Following David Chalmers, they invoke a distinction between functionalist and phenomenal accounts of mental states. As they summarize, "Chalmers demonstrates that individual human mental states can be analyzed either in terms of what he calls

---

[33] *In re Facebook Biometric Info. Privacy Litig.*, 2018 U.S. Dist. LEXIS 810448, p. 8.
[34] Chatterjee and Fromer, "Minds, Machines," 1888.

their psychological properties—their functional role in producing behavior, or what they do—or their phenomenal properties—their conscious quality, or how they feel."[35] This produces an ambiguity in the law around mental states:

> For each of the law's mental state requirements, it remains an open question whether the law ultimately seeks to track the conscious or functional properties of the states in question. Because the law has primarily been designed for human actors, for whom the conscious and the functional typically coincide, this is a question we have principally been able to avoid until now.[36]

In other words, advances in technology have exposed a latent ambiguity in the law around mental states. This matters because "if the law is concerned only with functional properties, then these properties could very well be possessed by the states of a nonhuman machine."[37] Phenomenal states could not.

Prior usage of terms like "facial recognition" similarly had no need to distinguish between a functionalist and phenomenalist account, since the activity was only done by people. Facebook's argument, in essence, is that (a) "facial recognition" (or biometric identification) necessarily designates a phenomenal state which would have to be replicated in a machine in order to count as an instance of the category, and that (b) their software is only functional, and so is not facial recognition. The argument has to concede that the software is functional (otherwise it wouldn't work). But is it merely functional? It clearly does not do exactly the same thing that an embodied human being does when they identify a face. For the argument to work, then, the law would need to track the phenomenal sense of recognition, on the theory that an entity that recognizes a face must be constituted a certain way, as evidenced by its phenomenal state. This

---

[35] Chatterjee and Fromer, "Minds, Machines," 1906.
[36] Chatterjee and Fromer, "Minds, Machines," 1907.
[37] Chatterjee and Fromer, "Minds, Machines," 1907.

would have the convenient result of making all facial recognition software unregulable under BIPA.

However, the initial ambiguity between phenomenal and functional understandings of recognition means that Facebook's preferred construction of "recognize" is not necessary: one might instead ask not what the software is, but what it does. Chatterjee and Fromer offer one proposal for how to resolve the legal question:

> It might be that the law is interested in conscious properties of mental states when it seeks to treat the actor in question as a rightsholder (such as in copyright authorship) or an autonomous and responsible agent (such as in criminal punishment). But in contexts in which the law is seeking simply to protect the rights or interests of others from the actor (such as copyright infringement), functionality might be all that matters.[38]

It is quite clear that BIPA was designed to protect the interests of citizens from entities that collect and use their biometric data. If that is the case, there is not only no reason to accept Facebook's reliance on phenomenal properties of recognition, but a good reason to reject it. The law is then about addressing power relations, even as it operates through traditional privacy concepts.

Facebook's defense is thus again legible as an effort to deny that the data subjects its software constructs are like the archaic legal subjects of older theory. These data subjects produce information, and their software analyzes it, all without implicating the traditional concerns of subjectivity. Since it is juridical subjects who can make BIPA claims, no such claims are relevant here. In so doing, the company relies on a literalist reading of "recognition" that compares what humans do with what its software presumably does, and then relies on the

---

[38] Chatterjee and Fromer, "Minds, Machines," 1915-16.

differences between those processes to conclude that its software does not recognize faces; rather than finding subjects, the software finds only information to interpret.

III. Terms of Service: Long Live the Data Subject!

If Facebook's litigation strategy against BIPA relies on the fictionality of the data subject and her legal illegibility, the company's treatment of its users depends precisely on the reality of this legal fiction. I will emphasize two aspects of this strategy here: the reliance on an individualist theory of contract and the promotion of personalization.

1. Standing, Round 2: It's a contract.

As is well-known, sites like Facebook condition access on the acceptance of terms of service (ToS), which are laid out in a lengthy document that the user has to "click here" to accept. These terms of service govern the user's interaction with the site, the resolution of disputes the user might have with the site, and the subsequent handling of the data as an alienable property. As Cohen argues, "the activities of collecting and processing personal data require an enabling legal construct;" the terms-of-service regime is that construct.[39] Its narrative support is that of liberal contract theory, which imagines a negotiation between an autonomous subject and a vendor, at the conclusion of which the subject makes an informed decision about whether to accept the vendor's offer.

Although the term "contract" recalls this image, it departs fundamentally from traditional contract in at least two ways that are relevant here. First, the legal relation being constructed

---

[39] Cohen, *Between Truth and Power*, 48.

does not conform to any historical model of contract. As Robin Kar and Margaret Jane Radin argue, if one takes the model of oral negotiation as paradigmatic, then the resulting regime is best described as one of "pseudo-contract" because the terms and conditions include a profusion of boilerplate, advice, descriptive statements, and other verbiage.[40] For example, it is bizarre to imagine someone reading to a consumer multiple pages of boilerplate as they decide to buy a $0.99 song, especially given that large amounts of that boilerplate either adds conditions that no consumer would consent to if they understood them, or which cannot possibly be intended to create a contractual condition in the first place ("if you want to disable this default, you can change it in 'Settings'").

Moreover, the notion of consent involved is, from this point of view, deeply pathological.[41] Most generally, consent hinges on a functioning notion of autonomy, which website practices often undermine.[42] Demands to consent to privacy practices are incessant, causing consumers to pay less attention to them individually. Consent is often unwitting in that consumers don't understand either the terms or the technology behind them. They also don't understand the consequences and risks of the site's privacy practices. If not fully coerced, consent can be induced by both the fact that it is difficult now not to use the Internet (no viable opt-out) and that both ISPs and networks are de facto monopolies (no market competition).[43] Various website design techniques also make opting out physically difficult. Pop-ups cover the

---

[40] Robin Bradley Kar and Margaret Jane Radin, "Pseudo-Contract and Shared Meaning Analysis," *Harvard Law Review* 132, no. 4 (2019).

[41] Richards and Hartzog, "The Pathologies of Digital Consent."

[42] Daniel Susser, Beate Roessler, and Helen Nissenbaum, "Technology, autonomy, and manipulation," *Internet Policy Review* 8, no. 2 (2019), https://doi.org/10.14763/2019.2.1410.

[43] For monopoly and subjectification in the context of data, see Gordon Hull, "Infrastructure, Modulation, Portal: Thinking with Foucault about how Internet Architecture Shapes Subjects," *Techné: Research in Philosophy and Technology* forthcoming (2021).

screen, browser tabs open with no 'back' button, and language turns to various techniques of social manipulation: "Yes! I want this product! No thanks, I choose to die a lonely death."[44]

Terms of Service also increasingly contain mandatory arbitration clauses stipulating that any and all disputes arising out of the use of the site be settled in private arbitration or using automated dispute resolution systems, often with an arbitrator chosen by the company. This is also a significant departure from traditional juridical subjectivity, which generally presupposed that subjects could vindicate their rights in court. Recent Supreme Court jurisprudence has been increasingly deferential to arbitration agreements, especially when they prevent individuals from pursuing actions as a class, rather than as individuals, with the effect that ordinary principles of contract do not apply, especially when those principles tend to level the playing field. For example, in a recent employment case, the Court emphasizes both that (a) arbitration agreements are to be respected on an equal basis with other contracts, per the Federal Arbitration Act (FAA), and (b) that ordinary, state-level public policy provisions governing contractual interpretation (such as *contra proferentem*) are preempted by the FAA's attempt to promote informal, quick and individual (but not class) arbitration.[45]

The Court justifies (b) on the grounds that departures from the FAA baseline regime can only be allowed when there is unambiguous consent. As a practical matter, this justification codifies a federal policy prioritizing the privatization of dispute resolution procedures against the ordinary expectations of consumers and does so in a way that both masks the asymmetrical

---

[44] For a catalogue of such "confirmshaming" and other manipulative "dark patterns," see (in addition to Richards and Hartzog) Arunesh Mathur et al., "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites," *Proceedings of the ACM on Human-Computer Interaction* 3, no. Article 81 (2019), https://doi.org/10.1145/3359183; Arvind Narayanan et al., "Dark Patterns: Past, Present, and Future: The evolution of tricky user interfaces," *Queue* 18, 2 (2020), https://doi.org/10.1145/3400899.3400901., as well as the account of "hypernudges" in Karen Yeung, "'Hypernudge': Big Data as a mode of regulation by design," *Information, Communication & Society* 20, no. 1 (2017), https://doi.org/10.1080/1369118X.2016.1186713..

[45] *Lamps Plus, Inc. v. Varela*, 139 S. Ct. 1407 (2019).

power relations behind consumer contracts and removes minimal state law safeguards against their abuse. Indeed, in dissent, Justice Ginsburg pursues the tendency of consent to be coercive, and Justices Kagan and Sotomayor both warn against too quick preemption of state laws. In terms of the contractual imaginary, one should note the presence of a double-standard: it is very easy for consumers to consent to arbitration provisions, and very difficult for companies to consent to their waiver. In this way, the imaginary of "contract" obscures significant shifts of power toward the platform companies that insist on the term.

In short, the notice-and-consent regimes contemplate not so much as a contract classically conceived, but a specific and novel relationship, the subject positions within which are defined by fiat. When convenient for the companies that describe these relationships, they declare them enforceable as contracts and point to formal rather than substantive indicators of consent. As Waldman documents, corporate repetition of privacy desiderata tends to mold legal regimes.[46] Hence, when courts do rule against these relationships, they tend to follow the focus on formalistic determinations of whether consent has occurred, such as whether notice of terms is sufficiently prominent or the existence of evidence that users accessed sites in a way that would trigger consent; rulings tend not to be in terms of how consumers were induced to consent or the substance of what they have consented to.[47] That the game is rigged is not lost on consumers; as a result, they become discouraged and resigned to it, and that resignation is then used as evidence that they have freely traded away their privacy because they assign it little

---

[46] Waldman, "Privacy, Practice, and Performance."

[47] Nancy S. Kim, "Digital Contracts," *The Business Lawyer* 75 (2020); Woodrow Hartzog, "The New Price to Play: Are Passive Online Media Users Bound By Terms of Use?," *Communication Law and Policy* 15, no. 4 (2010), https://doi.org/10.1080/10811680.2010.512514.

value.[48] Cohen concludes that "the conception of consent emerging from that default condition is unprecedented in the law of contracts or any other body of law," serving mainly as "a form of Kabuki theater that distracts both users and regulators from what is really going on."[49]

In the context of the litigation around BIPA, it is thus predictable that Facebook would try to prevent judicial class certification for its users, and it is enormously significant that this strategy ultimately failed. In its ruling upholding the standing of users to sue under BIPA, the 9th Circuit also rejected Facebook's claim that the district court had abused its discretion in granting class certification. Specifically, the Court rejected the company's contention that "the possibility of a large, class-wide statutory damages award here defeats superiority" of class certification to individual lawsuits. As the Court notes, "nothing in the text or legislative history of BIPA indicates that a large statutory damages award would be contrary to the intent of the General Assembly."[50] Shortly after the Supreme Court refused the case, Facebook settled for over $500 million.[51] It is difficult not to read the settlement as a direct response to losing the standing and class certification arguments. Were Facebook's strategy to succeed, it would have largely escaped liability, either because no one would have standing to sue, or because the litigation risk could be dispersed to indefinitely many individual plaintiffs with small claims that would be too expensive for them to pursue.

2. Promotion of "personalization"

---

[48] Nora A. Draper and Joseph Turow, "The corporate cultivation of digital resignation," *New Media & Society* 21, no. 8 (2019/08/01 2019), https://doi.org/10.1177/1461444819833331.

[49] Cohen, *Between Truth and Power*, 58-59.

[50] Kugler, "From Identification," 1276-7.

[51] Kathleen Foody, "Unique Illinois privacy law leads to $550M Facebook deal," *ABCNews.com*, Feb. 9 2020, https://abcnews.go.com/Business/wireStory/unique-illinois-privacy-law-leads-550m-facebook-deal-68861584.

When data collection is not presented as a necessary condition for access to goods and services, it is often presented as enabling the benefits of "personalization." Such personalization has long been presented as a desirable goal of datafication, often attached to ideas of user autonomy and control. As far back as the 1970s, Nicholas Negroponte was promoting the idea of a "Daily Me" personalized news feed; an early iteration of the concept, FishWrap, was developed at the MIT Media Lab in the mid-1990s.[52] Pushing back against complaints that the project was isolating, MIT's Pascal Chesnais argued that "it's really about control, decision making …we have no editors making decisions involving what people should read. The readers do that."[53] For his part, Negroponte invites his readers to "imagine a future in which your interface agent can read every newswire and newspaper and catch every TV and radio broadcast on the planet, and then construct a personalized summary."[54] Today, such personalization is ubiquitous, beyond the inevitably curated news from Facebook; if you turn off "personalized" ads in Google, it warns you that you will no longer see advertising of particular "interest" to "you."

Here, I want to underscore the rhetorical construction of a data subject. Personalization is construed on the model of an agent that caters to an individual's interests and needs. This individual is understood exogenously to its information environment, which is to say that the construction does not acknowledge an underlying process of subjectification, where the subject itself can be modified by the feedback of its agent.[55] This move should be familiar from defenses of notice-and-consent privacy, which similarly construct an underlying subject making

---

[52] Fred Hapgood, "The Media Lab at 10," *Wired*, Nov. 1, 1995, https://www.wired.com/1995/11/media/.
[53] qt. in Christopher Harper, "The daily me," *American Journalism Review* 19, no. 4 (1997): 42.
[54] Nicholas Negroponte, *Being Digital* (London: Hodder and Stoughton, 1996), 153-4.
[55] For a sustained critique of this view of subjectivity in the online/data context, see Cohen, *Configuring*..

decisions about its environment, and similarly elide difficulties in how that decision process functions and how the environment both constrains and helps to produce the decisions which are viable for the subject. As noted above in the context of consent, underneath the surface construction of an individual and her agent, the system works to constantly reconstruct the individual as a target of intervention. That is, the data subject is not an entity whose desires are to be known, but a moment in a process of intervention, constructed in order to appropriate and direct her desires.

Recent work by Nick O'Donovan on the network effects of personalization helps to illustrate the issue.[56] Many of the products that use personalization are valuable to their users because of network effects: the more people who are connected to a social network, the more valuable it is to each of its members. O'Donovan points out that personalization also exhibits network effects, because the more users a platform has, the more data it collects, and the better its recommendation and personalization algorithms will perform. For example, the more people whose movie tastes Netflix's algorithm sees, the better it will be able to predict the tastes of a given user. There are two problems in the present context. First, the things that I think make me unique may not be the ones that matter to a personalization algorithm. In that sense, there is an almost necessary gap between the platform's appeal to my phenomenological experience of being a unique individual and the algorithm's use of different data to classify my tastes. The problem is not that the algorithm works by classification and so I am not as unique as I am told; the problem would still manifest in a hypothetical case where I was the only member of my class, since the reasons I view myself as unique have no necessary relation to the reasons the

---

[56] Nick O'Donovan, "Personal Data and Collective Value: Data-Driven Personalisation as Network Effect," in *Data-Driven Personalisation in Markets, Politics and Law*, ed. Jacob Eisler and Uta Kohl (Cambridge: Cambridge University Press, 2021).

algorithm does. For example, music personalization algorithms differentiate between users based on their avidity, measured in quantified time spent on the site – and not on anything deriving from their subjective experiences.[57]

Second, the data used for personalization might or might not be used to foster the uniqueness of my experience. As O'Donovan points out, the algorithm might be targeted to matching me with the products that the data indicates I would most like or would find most engaging. However, it might also be directed to matching me with the products and content that maximize revenue for the platform. At that point, the recommendation is personalized, but "I" am not in "control" because the recommendation system is not actually operating as my agent; rather, it is operating as the agent of the platform company. Worse, and as O'Donovan emphasizes, the network effects of data personalization will tend to concentrate market power in the companies that have the most data, erecting substantial barriers for new competitors, even if those competitors offer a service that consumers would prefer. Even consumers who know that the recommendation system does not work for them have little choice but to play along.

This gap between the rhetorical construction of personalization as an especially helpful butler and its more subtle efforts to mold the subject's choice architecture shows the political function of the data subject. If the data subject of a Terms of Service is designed to create a legal subject, the data subject of the personalization narrative is designed to create a phenomenological subject whose experience as a self-centered entity is unable to see the extent to which it is itself the product of a process of curation. That is, the appeal to the uniqueness of the user's experience serves to mask the extent to which that uniqueness serves ends other than those of the

---

[57] Nick Seaver, "Seeing like an infrastructure: avidity and difference in algorithmic recommendation," *Cultural Studies* 35, no. 4-5 (2021), https://doi.org/10.1080/09502386.2021.1895248.

user. By encouraging users to focus on the phenomenological uniqueness of their encounter with the platform, the platform company discourages them from seeing either how that experience is manipulated or how their experience is used to structure that of others. At the same time, a company like Facebook will claim that only the phenomenal experience of facial recognition is actually facial recognition: personalization depends on phenomenal states being inessential, but tort liability depends on their being essential.

IV. Conclusion: Toward a Progressive Politics of Privacy

Foucault says at one point that "a progressive politics" does not make a "universal operator" of the subject; rather, it "defines the different projects and functions that subjects are able to occupy in a domain which has its rules of formation."[58] In so doing, he points us to the risk of focusing too much either on privacy as an abstract term or on the data subject itself; in both cases, it is important to look at the underlying institutional and political power relations, and how those are mediated. As many have noted, the underlying context is the rise of informational capitalism; and as Cohen has argued at length, the increasing power of informational capital is leading to subtle changes in legal doctrine.[59]

For that reason, the issues raised here are increasingly important. First, the Facebook case represents the tip of a rapidly growing iceberg of litigation around BIPA and facial recognition. In April 2020, a pair of Illinois students (seeking class certification) filed suit in Illinois against Google, accusing it of collecting face templates and voiceprints of children using

---

[58] Michel Foucault, "Réponse à une question [D&E #58]," in *Dits et Écrits* (Paris: Editions Gallimard, 2001), 721.

[59] Cohen, *Between Truth and Power*.

its educational software.[60] That suit is in addition to a case filed over Google Photos two months earlier.[61] Clearview, which has scraped billions of photographs from social media sites and used them to create facial recognition technologies which it then sells to law enforcement, has also been sued under BIPA. Following a *New York Times* article suggesting that the technology could "end your ability to walk down the street anonymously," a number of cases were filed in federal court; as of this writing, consolidated litigation is ongoing in New York.[62] The Chicago Blackhawks have been sued for collecting facial scans at home games, and sports franchises are being advised to develop rigorous compliance programs.[63] The Facebook settlement, in short, is opening a floodgate of litigation.

Second, although the analysis here has been narrow, there is good evidence that this sort of rhetorical two-step occurs elsewhere. For example, in *Dinerstein v. Google* (2020), a district court granted Dinerstein Article III standing to pursue claims over a hospital's transfer of his health data to Google, averring that he had suffered concrete harm. The court then dismissed the case on the grounds that he had no legal interest in the data such that it could grant him relief.[64] At the same time, the Court held that the data was plausibly consideration for the "license [for the hospital] to use trained models and predictions developed by Google."[65] In other words, the data has exchange value for the hospital and Google, but not for Dinerstein. More generally, as

---

[60] Richard Nieva, "Two children sue Google for allegedly collecting students' biometric data," *CNet News*, April 3 2020, https://www.cnet.com/news/two-children-sue-google-for-allegedly-collecting-students-biometric-data/.

[61] Anthony Kimery, "Google hit with new biometric data privacy class action under BIPA," *BiometricUpdate.com*, Feb. 10 2020, https://www.biometricupdate.com/202002/google-hit-with-new-biometric-data-privacy-class-action-under-bipa.

[62] For the initial report, see Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *New York Times*, Jan. 18 2020.. The cases are consolidated as *Calderon v. Clearview AI, Inc.,*, 2020 U.S. Dist. LEXIS 94926 (S.D.N.Y. 2020)..

[63] Blank Rome LLP, "Facial Recognition at Sports Venues: Enhancing the Gameday Experience While Minimizing Liability," *Newstex Blogs JD Supra*, Nov. 11, 2020.

[64] *Dinerstein v. Google*, 2020 U.S. Dist. LEXIS 161996 (ND Illinois), 39, referring to 18-19.

[65] *Dinerstein*, 2020 U.S. Dist. LEXIS 32.

Frank Pasquale notes, platform companies routinely claim to be both neutral conduits for information and speakers, depending on the circumstance. As he puts it, "when intellectual property or defamation claims arise, they emphasize their role as mere conduits, reflecting the preferences and serving the interests of users. But when classic business tort or privacy claims arise, intermediaries argue that they are speakers, their selection and arrangement of information a type of activity best protected as freedom of expression."[66]

Part of what is happening is a subtle reconfiguration of legal structures as they are mediated by common law, and the cases here underscore the extent to which legal rules in practice depend on common law concepts that might be a difficult fit. In particular, data privacy cases appear to increasingly depend on the extent to which judges are able to imagine the case before them in terms of common law protections.[67] Consider the Supreme Court's decision in *Ramirez v. TransUnion* (2021). In it, a 5-4 majority ruled that the credit agency's mere possession of information erroneously suggesting that someone was a terrorist was insufficient to establish liability under the FCRA; to establish Article III standing, plaintiffs needed to show that the credit agency had disseminated this information to someone else.[68] In writing for the majority, Justice Kavanaugh explicitly compared the dissemination of this erroneous information to defamation, and ruled it "unquestionably" sufficient to establish legal injury. In simultaneously denying standing to plaintiffs whose files contained erroneous information that the credit agency had not yet disseminated, his analogy was to possession of a defamatory letter

---

[66] Frank Pasquale, "Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power," *Theoretical Inquiries in Law* 17 (2016): 494.

[67] The judicial basis for this is articulated in *Spokeo*: intangible harms are to be assessed according to "whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts" *Spokeo*, 136 S. Ct. 1549.

[68] Justice Thomas' dissent objected on separation of powers grounds; notably, he also clearly thought the agency's possession of erroneous information established the likelihood that it would disseminate it, making the harm immanent.

that one keeps in a desk drawer. Independently of the extent to which *TransUnion* overrules explicit Congressional statute, it is important to note the work that analogy to common law torts is doing in deciding the case.[69] As noted above, Facebook's loss on standing also involved comparison to traditionally actionable privacy torts. In those situations, the resolution seems to depend on the ability to imagine a traditionally injured legal subject. Indeed, it is not clear that the harms of BIPA would be "concrete" under *TransUnion*, since that case blocked application of a statutory harm regime analogous to BIPA's.

On the other hand, the deference to common law imaginaries is notably shrinking in the case of arbitration and other contract rules, where, as *Varela* demonstrates, the Court is willing to override longstanding common law contractual interpretation provisions to further its reading of the FAA. Similarly, the contractual standards being defended in Terms of Service cases have little to do with common law imaginaries of contract. One possible reason for this is that the kind of subjectivity at issue is not analogous to traditional forms of juridical subjectivity. This is harder to see in the Terms of Service cases, where there is a formal moment of consent, but even there, judicial pushback against abusive terms of service is most likely where the consent strays the furthest from common law models. It is more clear in the facial recognition cases, where Facebook's litigation strategy has been to deny that a juridical subject is implicated in the first place. Together, these suggest both the possibility and need for significant work in reimagining the law to encompass new kinds of data subjectivity.

One result is negative: insisting on individual privacy rights as they have been traditionally imagined is unlikely to protect data subjects. Privacy harms will often fail to be

---

[69] It is not clear to me that the outcome of *Spokeo* on remand is compatible with *TransUnion*. First, plaintiffs will have to show that their erroneous credit was actually disseminated. Second, the inaccurate information in *Spokeo* was not defamatory: it was wrong, but did not call anyone a terrorist.

analogous to current imaginaries of the common law, as in the case of concreteness or dissemination of credit information. At the same time, the imagined consenting contractual subject can be deployed to limit consumer protections, as in the case of arbitration cases. A necessary first step is to recognize the contingency of the data subject: there is no essential subject that subtends the different processes of data collection and that can be pointed to as their exogenous author. That sense of subjectivity is an illusion; the very practice of data collection presupposes projects of singularization that are incompatible with any notion of an enduring, exogenous subject. The illusion is actively maintained by the rhetoric surrounding both the contractual obligations of data subjects and the personalization of content for them. Its function is political, and it allows data to be alienated and therefore subject to appropriation by others, while simultaneously shielding those who extract data from tort liability. Like religious belief in the early Marx, the uniquely personal data subject mainly serves to make the disempowered feel better.

Once one understands the role of subjectivity politically and structurally, then the possibility of different kinds of reform become apparent. As suggested above, one strategy is to work to restructure the imaginary of common law. Common law is not static, evolving from multiple sources over time. As Dan Solove and Danielle Citron note in their critique of *TransUnion*, the case of privacy tort law, which developed in the wake of an academic article, illustrates the point.[70] A broader strategy is to recognize the power relations involved in the construction of data subjects, and to respond to vulnerabilities at that level. If the structural position of the data subject is one of weakness, then that subject is never going to be in a good

---

[70] Daniel J. Solove and Danielle Keats Citron, "Standing and Privacy Harms: A Critique of TransUnion v. Ramirez," *Boston University Law Review Online* 101 (2021): 67, https://www.bu.edu/bulawreview/2021/07/21/standing-and-privacy-harms-a-critique-of-transunion-v-ramirez/.

position to vindicate its own rights, and procedural requirements for disclosure and consent are unlikely to make much of a difference. The problems need to be addressed at the structural level. For example, if inaccurate credit reporting causes harm, then the use of credit reporting could be restricted and other "do not use" rules could be put on private information.[71] If the monopoly power of platform companies makes it impossible for consumers to seek better terms of service, then legislation can either attempt directly to weaken those monopolies through antitrust law or attempt to blunt its effects with data portability or other requirements. If algorithmic constructions of individuals discriminate against them, then there can be requirements for algorithmic accountability or auditability.[72]

The point here is not to assess any particular policy option; rather it is to notice that there are two kinds of strategies for protecting data subjects. One treats the data subject as an agent that can vindicate its rights in court. This strategy is failing, in part because the subject position is one structured by significant power asymmetries. It is not just that notice-and-consent and similar theories do not protect privacy (although it is definitely that); it is that insisting on them, as though the data subject were not problematic, directly facilitates the processes of data

---

[71] These rules will need to be carefully tailored and often contextually specific; for some of the debate, compare Anita L. Allen, *Unpopular Privacy: What must We Hide?* (Oxford: Oxford University Press, 2011). and Lior Jacob Strahilevitz, *Information and Exclusion* (New Haven and London: Yale University Press, 2011). Rules that offer structural protections from data misuse also encourage its sharing; as Michele Gilman and Rebecca Green note in their critique of excessive surveillance of society's most vulnerable, Europeans worry less about sharing health data because they have a right of access to healthcare. Michele Gilman and Rebecca Green, "The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization," *N.Y.U. Review of Law and Social Change* 42 (2018).

[72] These requirements can apply even if algorithms cannot be "transparent:" see Joshua A. Kroll, "The fallacy of inscrutability," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2133 (2018/11/28 2018), https://doi.org/10.1098/rsta.2018.0084, https://doi.org/10.1098/rsta.2018.0084.. For the importance of understanding algorithmic fairness as a substantive and not procedural question (i.e., in a manner broadly compatible with the argument here), see Ben Green, "Impossibility of What? Formal and Substantive Equality in Algorithmic Fairness," *arXiv Preprint 2107.04642* (2021), https://arxiv.org/abs/2107.04642; Ben Green and Salomé Viljoen, "Algorithmic realism: expanding the boundaries of algorithmic thought" (Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, Barcelona, Spain, Association for Computing Machinery, 2020).

extraction against which it supposedly protects. It increases the vulnerability of data subjects by binding them to very broad-based adhesion contracts according to which their data belongs to someone else and according to which they have little hope of redress if something goes wrong. At the same time, it shields data companies from vulnerability by depriving any point on which to attach liability. For that reason, it might make more sense to pursue a second approach: protect the data subject by attacking the power asymmetries that make the subject position a vulnerable one in the first place.

Works Cited

Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. "Privacy and Human Behavior in the Age of Information." *Science* 347, no. 6221 (2015): 509-14. https://doi.org/10.1126/science.aaa1465.

Allen, Anita L. *Unpopular Privacy: What Must We Hide?* Oxford: Oxford University Press, 2011.

Alterman, Anton. "'A Piece of Yourself:' Ethical Issues in Biometric Identification." *Ethics and Information Technology* 5, no. 3 (2003): 139-50. https://doi.org/10.1023/B:ETIN.0000006918.22060.1f.

Aranda V. Caribbean Cruise Line, Inc., 202 F. Supp. 3d 850 (ND Illinois 2016).

Arvidsson, Adam. "On the 'Pre-History of the Panoptic Sort:' Mobility in Market Research." *Surveillance and Society* 1, no. 4 (2004): 456-74. http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3331.

Blank Rome LLP, "Facial Recognition at Sports Venues: Enhancing the Gameday Experience While Minimizing Liability," *Newstex Blogs JD Supra*, Nov. 11, 2020.

Boyle, James. *Shamans, Software and Spleens: Law and the Construction of the Information Society.* Cambridge, MA: Harvard University Press, 1997.

Browne, Simone. *Dark Matters: On the Surveillance of Blackness.* Durham, NC: Duke University Press, 2015.

Buolamwini, Joy, and Timnit Gebru. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." Proceedings of the 1st Conference on Fairness, Accountability and Transparency, New York, 2018.

Calderon V. Clearview Ai, Inc.,, 2020 U.S. Dist. LEXIS 94926 (S.D.N.Y. 2020).

Chatterjee, Mala, and Jeanne C. Fromer. "Minds, Machines, and the Law: The Case of Volition in Copyright Law." *Columbia Law Review* 119 (2019): 1887-916.

Cheney-Lippold, John. *We Are Data: Algorithms and the Making of Our Digital Selves.* New York: NYU Press, 2017.

Clapper V. Amnesty Int'l USA, 568 U.S. 398 (2013).

Cohen, Julie E. *Between Truth and Power: The Legal Constructions of Informational Capitalism.* Oxford: Oxford University Press, 2019.
———. *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice.* New Haven: Yale University Press, 2012.
———. "What Privacy Is For." *Harvard Law Review* 126 (2013): 1904-33.
Community for Creative Non-Violence V. Reid, 490 U.S. 730 (1989).
Couldry, Nick, and Ulises A. Mejias. "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject." *Television & New Media* 20, no. 4 (2018): 336-49. https://doi.org/10.1177/1527476418796632.
Dinerstein V. Google, 2020 U.S. Dist. LEXIS 161996 (ND Illinois 2020).
Draper, Nora A., and Joseph Turow. "The Corporate Cultivation of Digital Resignation." *New Media & Society* 21, no. 8 (2019/08/01 2019): 1824-39. https://doi.org/10.1177/1461444819833331.
Fairfield, Joshua A. T., and Christoph Engel. "Privacy as a Public Good." *Duke Law Journal* 65 (2015): 385-457.
Foody, Kathleen. "Unique Illinois Privacy Law Leads to $550m Facebook Deal." *ABCNews.com*, Feb. 9 2020. https://abcnews.go.com/Business/wireStory/unique-illinois-privacy-law-leads-550m-facebook-deal-68861584.
Foucault, Michel. "Réponse À Une Question [D&E #58]." In *Dits Et Écrits*, 701-23. Paris: Editions Gallimard, 2001.
Gilman, Michele, and Rebecca Green. "The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization." *N.Y.U. Review of Law and Social Change* 42 (2018): 253-307.
Glaser, April. "Biometrics Are Coming, Along with Serious Security Concerns." *Wired*, March 9, 2016. https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/.
Green, Ben. "Impossibility of What? Formal and Substantive Equality in Algorithmic Fairness." *arXiv Preprint 2107.04642* (2021). https://arxiv.org/abs/2107.04642.
Green, Ben, and Salomé Viljoen. "Algorithmic Realism: Expanding the Boundaries of Algorithmic Thought." Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, Barcelona, Spain, Association for Computing Machinery, 2020.
Hapgood, Fred. "The Media Lab at 10." *Wired*, Nov. 1, 1995. https://www.wired.com/1995/11/media/.
Harper, Christopher. "The Daily Me." *American Journalism Review* 19, no. 4 (1997): 40-44.
Hartzog, Woodrow. "The New Price to Play: Are Passive Online Media Users Bound by Terms of Use?". *Communication Law and Policy* 15, no. 4 (2010): 405-33. https://doi.org/10.1080/10811680.2010.512514.
Hartzog, Woodrow, and Frederic Stutzman. "The Case for Online Obscurity." *California Law Review* 101, no. 1 (2013): 1-49.
Hill, Kashmir. "The Secretive Company That Might End Privacy as We Know It." *New York Times*, Jan. 18 2020.
Hull, Gordon. *The Biopolitics of Intellectual Property: Regulating Innovation and Personhood in the Information Age.* Cambridge: Cambridge University Press, 2020.
———. "Infrastructure, Modulation, Portal: Thinking with Foucault About How Internet Architecture Shapes Subjects." *Techné: Research in Philosophy and Technology* forthcoming (2021).

———. "Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data." *Ethics and Information Technology* 17, no. 2 (2015): 89-101. https://doi.org/10.1007/s10676-015-9363-z.

Kar, Robin Bradley, and Margaret Jane Radin. "Pseudo-Contract and Shared Meaning Analysis." *Harvard Law Review* 132, no. 4 (2019): 1135-219.

Kearns V. Cuomo, 2020 U.S. App. LEXIS 37384 (2nd Cir. 2020).

Kim, Nancy S. "Digital Contracts." *The Business Lawyer* 75 (2020): 1683-93.

Kimery, Anthony. "Google Hit with New Biometric Data Privacy Class Action under Bipa." *BiometricUpdate.com*, Feb. 10 2020. https://www.biometricupdate.com/202002/google-hit-with-new-biometric-data-privacy-class-action-under-bipa.

Kroll, Joshua A. "The Fallacy of Inscrutability." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2133 (2018/11/28 2018): 1-14. https://doi.org/10.1098/rsta.2018.0084. https://doi.org/10.1098/rsta.2018.0084.

Kugler, Matthew B. "From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms." *U.C. Irvine Law Review* 10 (2019): 107-52.

Lamps Plus, Inc. V. Varela, 139 S. Ct. 1407 (2019).

Lessig, Lawrence. *Code and Other Laws of Cyberspace.* New York: Basic Books, 1999.

Mathur, Arunesh, Gunes Acar, Michael J. Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. "Dark Patterns at Scale: Findings from a Crawl of 11k Shopping Websites." *Proceedings of the ACM on Human-Computer Interaction* 3, no. Article 81 (2019). https://doi.org/10.1145/3359183.

Narayanan, Arvind, Arunesh Mathur, Marshini Chetty, and Mihir Kshirsagar. "Dark Patterns: Past, Present, and Future: The Evolution of Tricky User Interfaces." *Queue* 18, 2 (2020): 1-10. https://doi.org/10.1145/3400899.3400901.

Negroponte, Nicholas. *Being Digital.* London: Hodder and Stoughton, 1996.

Nieva, Richard. "Two Children Sue Google for Allegedly Collecting Students' Biometric Data." *CNet News*, April 3 2020. https://www.cnet.com/news/two-children-sue-google-for-allegedly-collecting-students-biometric-data/.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Palo Alto: Stanford University Press, 2010.

O'Donovan, Nick. "Personal Data and Collective Value: Data-Driven Personalisation as Network Effect." In *Data-Driven Personalisation in Markets, Politics and Law*, edited by Jacob Eisler and Uta Kohl, 74-92. Cambridge: Cambridge University Press, 2021.

Pasquale, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information.* Cambridge, MA: Harvard University Press, 2015.

———. "Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power." *Theoretical Inquiries in Law* 17 (2016): 487-513.

Patel V. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019).

Richards, Neil, and Woodrow Hartzog. "The Pathologies of Digital Consent." *Washington University Law Review* 96 (2019): 1461-503.

Rivera, Michael A. "Face Off: An Examination of State Biometric Privacy Statutes and Data Harm Remedies." *Fordham Intellectual Property, Media & Entertainment Law Journal* 29, no. 2 (2019): 571-610.

Robins V. Spokeo, Inc., 867 F.3d 1108 (9th Cir. 2017).

Rosenbach V. Six Flags Entertainment Corp., 129 N.E.3d 1197 (Sup. Ct. Illinois 2019).

Rothman, Jennifer E. *The Right of Publicity: Privacy Reimagined for a Public World.* Cambridge. MA: Harvard University Press, 2018.

Seaver, Nick. "Seeing Like an Infrastructure: Avidity and Difference in Algorithmic Recommendation." *Cultural Studies* 35, no. 4-5 (2021): 771-91. https://doi.org/10.1080/09502386.2021.1895248.

Selinger, Evan, and Woodrow Hartzog. "The Inconsentability of Facial Surveilance." *Loyola Law Review* 66 (2019): 101-22.

Selinger, Evan, and Brenda Leong. "The Ethics of Facial Recognition Technology." In *The Oxford Handbook of Digital Ethics*, edited by Carissa Véliz. Oxford: Oxford University Press, forthcoming.

Solove, Daniel J. "Privacy Self-Management and the Consent Dilemma." *Harvard Law Review* 126 (2013): 1880-903.

Solove, Daniel J., and Danielle Keats Citron. "Risk and Anxiety: A Theory of Data-Breach Harms." *Texas Law Review* 96 (2018): 737-86.

———. "Standing and Privacy Harms: A Critique of Transunion V. Ramirez." *Boston University Law Review Online* 101 (2021): 62-71. https://www.bu.edu/bulawreview/2021/07/21/standing-and-privacy-harms-a-critique-of-transunion-v-ramirez/.

Spokeo, Inc. V. Robins, 136 S. Ct. 1540 (2016).

Strahilevitz, Lior Jacob. *Information and Exclusion.* New Haven and London: Yale University Press, 2011.

Strandburg, Katherine J. "Free Fall: The Online Market's Consumer Preference Disconnect." *University of Chicago Legal Forum* 2013 (2013): 95-172.

Stuntz, William J. "The Substantive Origins of Criminal Procedure." *Yale Law Journal* 105 (1995): 393-447.

Susser, Daniel, Beate Roessler, and Helen Nissenbaum. "Technology, Autonomy, and Manipulation." *Internet Policy Review* 8, no. 2 (2019): 1-22. https://doi.org/10.14763/2019.2.1410.

Vigil V. Take-Two Interactive Software, Inc., 235 F. Supp. 3d 499 (S.D.N.Y. 2017).

Waldman, Ari Ezra. *Privacy as Trust: Information Privacy for an Information Age.* Cambridge: Cambridge University Press, 2018.

———. "Privacy, Practice, and Performance." *California Law Review* 110 (forthcoming) (2021).

Yeung, Karen. "'Hypernudge': Big Data as a Mode of Regulation by Design." *Information, Communication & Society* 20, no. 1 (2017): 118-36. https://doi.org/10.1080/1369118X.2016.1186713.