2019

The Inconsentability of Facial Surveillance

Evan Selinger

Woodrow Hartzog
Boston University School of Law

THE INCONSENTABILITY OF FACIAL SURVEILLANCE

Evan Selinger and Woodrow Hartzog***

ABSTRACT

Governments and companies often use consent to justify the use of facial recognition technologies for surveillance. Many proposals for regulating facial recognition technology incorporate consent rules as a way to protect those faces that are being tagged and tracked. But consent is a broken regulatory mechanism for facial surveillance. The individual risks of facial surveillance are impossibly opaque, and our collective autonomy and obscurity interests aren't captured or served by individual decisions.

In this article, we argue that facial recognition technologies have a massive and likely fatal consent problem. We reconstruct some of Nancy Kim's fundamental claims in Consentability: Consent and Its Limits*, emphasizing how her consentability framework grants foundational priority to individual and social autonomy, integrates empirical insights into cognitive limitations that significantly impact the quality of human decision-making when granting consent, and identifies social, psychological, and legal impediments that allow the pace and negative consequences of innovation to outstrip the protections of legal regulation.*

We also expand upon Kim's analysis by arguing that valid consent cannot be given for face surveillance. Even if valid individual consent to face surveillance was possible, permission for such surveillance is in irresolvable conflict with our collective autonomy and obscurity interests. Additionally, there is good reason to be skeptical of consent as the justification for any use of facial recognition technology, including facial characterization, verification, and identification.

---

* Evan Selinger is a Professor of Philosophy at Rochester Institute of Technology.

** Woodrow Hartzog is Professor of Law and Computer Science at Northeastern University School of Law and Khoury College of Computer Sciences. The authors would like to thank Kyle Berner for his excellent research assistance.

I. INTRODUCTION

"Surveillance" is an ominous word. In the post-Snowden world, it evokes Orwellian watchers who observe our every move, as persistent as they are powerful. Given the strong reactions the term can evoke, why hasn't greater resistance manifested against surveillance threats? An important reason is that surveillance technology is deployed in ways that make us feel comfortable with, not creeped out by, the algorithms and people observing us.[1] Facebook, for example, is designed to be an environment that feels so intimate that users focus on sharing information with friends without thinking about "surveillance capitalism" and all of the data the company collects, analyzes, and monetizes on the back end.[2] At airports and concerts, the experience of using facial recognition technology, a tool that is used for racial profiling and tracking in China and to scan the streets of Russia for "people of interest," can feel like a godsend, saving us and everyone else who socially conforms from waiting in long frustrating lines.[3] The more familiar and beneficial a surveillance technology like facial recognition seems, the easier it is for technology companies, government agencies, and entrepreneurs to create conditions for widespread passive acceptance.

Normalization, which involves treating facial recognition technology as a mundane part of the machinery that is necessary for powering a complex digital society, and function creep, which entails incrementally expanding how the technology is used, mask harms to individual and collective autonomy. They make it easy for surveillers to operate within a permissive regulatory regime: one that has porous boundaries between the government and the private sector, and treats consent as the basis for authorizing permission for watching, tagging, tracking, and sorting.[4] Even when our consent is obtained through questionable means, perhaps nudged by dark patterns and hidden options, many of us

---

1. *See* Evan Selinger, *Why Do We Love To Call New Technologies "Creepy"?*, SLATE (Aug. 22, 2012), https://slate.com/technology/2012/08/facial-recognition-software-targeted-advertising-we-love-to-call-new-technologies-creepy.html.

2. Evan Selinger, *Facebook Fabricates Trust Through Fake Intimacy*, MEDIUM (Jun. 4, 2018), https://medium.com/s/trustissues/facebook-fabricates-trust-through-fake-intimacy-b381e60d32f9.

3. Ian Sample, *What is facial recognition-and how sinister is it?*, THE GUARDIAN (July 29, 2019), https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it.

4. For more on normalization and function creep, *see* BRETT FRISCHMANN AND EVAN SELINGER, RE-ENGINEERING HUMANITY (2018).

will say yes when companies ask for it while engaging in surveillance or surveillance-related activities.[5] With limited alternatives to choose from and barriers to collective action that impede creating new, less surveillance intensive options, assenting to surveillance seems like the most rational "choice" for avoiding the penalties that come from being an opt-out outlier while accruing whatever take-it-or-leave-it benefits are offered by the consent-seeker, however meager they may be.[6]

The law has long struggled with problems associated with consent. In *Consentability: Consent and Its Limits*, Nancy Kim provides a promising path forward by integrating legal and ethical scholarship on consent with scientific inquiry into humanity's predictable irrationality. Drawing from these interdisciplinary resources, she constructs a new consentabilty framework and applies it to difficult cases: assisted suicide, body modification (from cosmetic surgery to RFID chip implants), bodily integrity exchanges (sexual services, surrogacy, and organ sales), and experimental activities (such as traveling to Mars and becoming cryopreserved).

In this article, we draw upon Kim's work along with our previous research on surveillance and privacy theory to make one simple point: facial recognition technologies probably have a fatal consent problem. After reviewing some of Kim's main ideas, we will apply aspects of her framework to explore how facial recognition technologies generally, and face surveillance specifically, affects us in ways that are difficult for most people to appreciate.

When we use the term face surveillance, we mean the use of facial recognition technologies and faceprint or name-faceprint databases to monitor behavior, identify people, or gain insight or information for the purposes of influencing, managing, directing, or deterring people. Examples include real-time observation, tracking, and identifying people in airports, retail stores, and public parks, as well as using faceprints and algorithms to identify and analyze people in stored photos and videos for law enforcement, commercial, and marketing purposes. The Future of Privacy Forum conceptualized instances of "identification: one to many" as situations where software tries to determine who an

5. For more on the conflicts between design and valid consent, *see* WOODROW HARTZOG PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 5 (2018).

6. *See* Frischmann and Selinger, *supra* note 4.

unknown person is, and "unique persistent identifiers," which are cases where algorithms try to determine what someone is doing "in a limited context, not linked to other personal identifiable information?"[7] We also use the terms "facial detection," which are instances of software trying to determine if a face can be found in a picture, and "facial characterization," which are situations where algorithms code assumptions about faces, such as emotions people might be experiencing.

We argue that valid consent is not possible for face surveillance in many of its current and proposed applications because of its inevitable corrosion of our collective autonomy, to say nothing of the dubious validity of individual consent in these contexts.[8] Additionally, we argue that some forms of characterization are inconsentable due to collective autonomy problems and are at least vulnerable to defective consent. Even "1:1 facial identification" features are highly subject to defective consent and should be highly scrutinized. Only facial detection tools ("is this a face?") seem entitled to the benefit of the doubt because they are not used to persistently track, identify, or manipulate people.

One reason consent to facial recognition is highly suspect is that people do not and largely cannot possess an appropriate level of knowledge about the substantial threats that facial recognition technology poses to their own autonomy.[9] Additionally, the framing of this debate around the amorphous concept of individual "privacy" has hidden unjustifiable risks to two of the most important values implicated by facial recognition: obscurity and collective autonomy. Even if some people withhold consent for face surveillance, others will inevitably give it. Rules that facilitate this kind of permission will normalize behavior, entrench organizational practices, and fuel investment in technologies that

---

7. Brenda Leong, *FPF Releases Understanding Facial Detection, Characterization, and Recognition Technologies and Privacy Principles for Facial Recognition Technology in Commercial Applications*, FUTURE OF PRIVACY FORUM (Sept. 20, 2018), https://fpf.org/wp-content/uploads/2019/03/Final-Privacy-Principles-Edits-1.pdf.

8. In addition to drawing from our own research and prior collaborations, our approach to analyzing consent will integrate insights from Neil Richards and Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461 (2019).

9. The entire field of behavioral economics is built around the idea that people have limited knowledge and capacity as decisionmakers. *See, e.g.,* DANIEL KAHNEMAN, THINKING FAST AND SLOW 4 (Farrar, Straus and Giroux ed., 2011); DAN ARIELY, PREDICTABLY IRRATIONAL (HarperCollins ed., 2008); CASS SUNSTEIN AND RICHARD THALER, NUDGE (2008).

will result in a net increase of surveillance. Expanding a surveillance infrastructure will increase the number of searches that occur which, in itself, will have a chilling effect over time as law enforcement and industry slowly but surely erode our collective and individual obscurity.

Building an infrastructure to facilitate surveillance will also provide more vectors for abuse and careless errors. No one is perfect, and the more requests for permission to surveil that are made the more harm from mistakes and malice will exist. Additionally, the larger and more entrenched facial recognition infrastructure becomes, the more opportunities exist for law enforcement to bypass procedural rules on searches to obtain information directly from industry. For example, if the government were prohibited from directly using facial recognition technologies, it could purchase people's location data obtained from facial recognition technology (and thus linked to their identities) from private industry. Procedural rules wouldn't address the true harm of these technologies without further prohibitions to prevent end-runs around the aims of a restriction.

We conclude this article with the argument that to defend against these dangers, lawmakers should pursue strong policy measures beyond procedural protections such as warrant requirements and informed consent frameworks. At a minimum, lawmakers should immediately enact moratoriums to prevent entrenchment of and dependence on facial recognition systems before they can be properly considered by lawmakers and society. In all areas where consentability conditions cannot be met, and procedural rules and compliance frameworks for government and industry will facilitate an outsized harm and abuse relative to their gains, facial recognition technology should be outright banned.

II. CONSENTABILITY AND INVALID CONSENT

Consent is a foundational concept in the American law. As one of us wrote with Neil Richards,

> We live in a society that lionizes individual choice in the many social roles we play every day, whether as consumers, citizens, family members, voters, lovers, or employees. Consent reinforces fundamental cultural notions of autonomy and choice. It transforms the moral landscape between people and makes the otherwise impossible possible.[1] It is essential to the exercise (and waiver) of fundamental constitutional rights, and it is at the essence of political freedom, whether we are

> talking broadly about a "social contract" or making political choices for individual candidates and referenda in the voting booth.[10]

Morally and legally, consent involves the "'intentional transfer of rights and obligations between parties,' which transforms the moral landscape between them and makes the otherwise impossible possible."[11]

Kim noted that "[c]onsent in the law is typically viewed as a conclusion, an all-or-nothing concept where the actions of the parties are considered objectively and statically."[12] The problem with this, Kim argued, is that "[t]his conception provides no guidance regarding which acts should be consentable."[13] According to Kim, "while the requirement of consent recognizes the value of autonomous decision-making, the *validity* of consent hinges upon the context in which it is given and the dynamic unleashed by both parties."[14] This means that valid consent is not only suspect in some contexts, but not even possible. She labels this concept regarding the circumstances under which consent can be valid "consentability."

In Kim's framework, consentability revolves around two requirements. First, an individual must be able to validly consent to a proposed activity. This means that they can intentionally manifest consent, possess the requisite knowledge in light of the motive for consenting, and exercise their volition to do so. Second, the social benefits of the activity must outweigh the social harms. In both cases, Kim maintains there is a range of fundamental yet hierarchically differentiable interests that the liberal state should safeguard: equality, justice and due process, public safety, democracy, free market capitalism, the right to bodily integrity, freedom of movement, civil and political rights, and property rights. At their core, Kim contends all these interests are expressions of autonomy, which she argues is a primary societal value. Since people can be born into a range of life-impacting circumstances that are beyond their control, the fairest way to foster and protect everyone's autonomy is to configure a social order that promotes liberty for all citizens. While individuals have

---

10. Neil Richards and Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1462 (2019).
11. *Id.* at 1462, 1468.
12. NANCY KIM, CONSENTABILITY: CONSENT AND ITS LIMITS 3 (2019).
13. *Id.*
14. *Id.*

autonomy interests at the personal level, Kim also identifies collective autonomy interests, which she defines as "the interest that all members of a society have in a particular right." From this structural perspective, if a clash occurs over comparable autonomy interests, Kim insists that "the collective autonomy interest prevails over the individual autonomy interest."[15]

At the individual level, Kim identified three essential features underlying legal determinations of consent. They are "an intentional manifestation of consent, knowledge, and volition/voluntariness."[16] Ideally, a person should not agree to an offer unless she understands what it entails, freely chooses to enter into the agreement, and demonstrates her agreement through clear words or deeds. In the real world, however, each condition is challenging. Voluntariness is vexing because real people, unlike hypothetically postulated rational actors, are bound by so many constraints that "no human being is truly or ideally autonomous all the time."[17] Clear affirmation is debated because the standard is context dependent. For example, Kim endorses some transactions requiring the consenting party to sign once at the end of a contract. However, she objects to the one-and-done practice being used in other circumstances, such as manifesting "consent to a bodily integrity contract where the consenter agrees to transfer his kidney."[18] While these are daunting complications, Kim deems the knowledge condition to be the hardest one to satisfy. This is because people can make poor decisions not only when they lack pertinent information, but also when they have access to all of the relevant details.

The problem of missing information is self-evident. But why doesn't having enough of it suffice for making informed decisions? It is because the quality of information matters. In order for information to be useful, it must be "understandable and salient."[19] Unfortunately, U.S. contract law exacerbates the problem. It incentivizes creating contracts that use jargon and provide overwhelming amounts of detail.[20] As a result, online user agreements regularly minimize the consent seeker's liability by hiding risks in plain sight.

---

15. NANCY KIM, CONSENTABILITY: CONSENT AND ITS LIMITS 84, 88 (2019).
16. *Id.* at 9.
17. *Id.* at 55.
18. *Id.* at 122.
19. NANCY KIM, CONSENTABILITY: CONSENT AND ITS LIMITS 125 (2019).
20. *See, e.g.,* Frishmann & Selinger, *supra* note 4; Neil Richards and Woodrow Hartzog, The Pathologies of Digital Consent, 96 WASH. U. L. REV. 1461, 1484 (2019).

To illustrate this problem, Kim declares that "a company that creates a product that records a person's conversations and collects their images should not be able to justify those actions by claiming that its customers consented by clicking 'agree' to the company's terms and conditions."[21]

To determine how to communicate a risky opportunity without rendering consent illegitimate, Kim turns to cognitive science and behavioral economic research on bounded rationality and the dual-process model of human cognition. In accordance with leading dual-process theorists, Kim maintains that human decision-making capacity is flawed in many ways, often in ways that we are unaware of. For example, we may not know whether our decisions are guided by the deliberative or intuitive cognitive system, if our decisions are impaired by heuristic techniques laden with cognitive biases, if we are self-sabotaging by misperceiving irrational decisions as rational ones, and if we are being swayed by misleading or manipulative information. From this perspective, people may make choices they later regret due to flawed heuristics like representative, anchoring, and availability; cognitive biases like overconfidence, optimism, and confirmation; heated emotional and physical states; or an inclination towards social conformity.[22]

While being attuned to cognitive limitations is necessary for formulating communication criteria that satisfies the knowledge condition, it is also insufficient. When consent is sought, the quality of information provided must be calibrated to adjust for two things: how much risk the transaction poses to individual and collective autonomy, and how trustworthy the consent-seeking parties are. Kim thus tailors her consentability framework on a sliding scale of consent standards. The greater the risk to autonomy, the more she believes a person is entitled to understand. For extremely risky situations, such as ones that could lead to "permanent disfigurement," Kim argues the "conditions of consent must be established with absolute certainty, the equivalent of the judicial standard 'beyond a reasonable doubt.'"[23]

By linking risk-level to the quality of consent-seeking disclosures, Kim derives a basis for demarcating valid from invalid consent at the individual level. She argues that consent is invalid if "the threat to autonomy interest outweighs the robustness of the

21. KIM, *supra* note 12, at 119.
22. *Id.* at 13.
23. Nancy Kim, Consentability: Consent and Its Limits 83 (2019).

consent conditions."[24] This means that if a transaction poses a great threat to autonomy and the consent conditions are not commensurate with the risk, valid consent cannot be given.

Although it might seem that consent must be either valid or invalid since an offer either can meet or fall short of the consentability standard, things are actually more complicated. An offer accepted under deficient consentability conditions results in one of two outcomes. Either the transaction transpires without genuine consent being given or else the offer is accepted through "defective consent." Kim characterizes this outcome as the "purgatory between valid consent and non-consent."[25] Kim's paradigm case of defective consent is a patient in an emergency situation agreeing to a medical procedure out of fear that failing to do so will pose high-level risks to her autonomy. In this instance, the patient is not acting in a truly voluntary manner. Even when professional standards nevertheless allow her to proceed with the procedure, Kim maintains that contractual bargaining should not transpire that includes terms that limit "the liability of the surgeon for malpractice nor require the patient to agree to mandatory arbitration in the event of a dispute."[26]

III. FACIAL RECOGNITION TECHNOLOGY DYSTOPIA

Consentability contains a passage about technology-induced change that is so bleak, it is worth quoting at length.

> Technology will continue to push the boundaries of what society thinks is acceptable. In some cases, the changes will be gradual, occurring first on the fringes of society and undetected by the public. . . . Sometimes the changes will go undetected because they are not visible or obvious to most people. As Lori Andrews observed in the context of genetics policy, "When technologies are introduced incrementally and policies are adopted in small units to deal with a few isolated issues, there is less opportunity to stimulate a social debate about whether we are moving in a direction in which we want to go." Companies, skilled in the art of marketing and sales, may try to manipulate the public and intimidate lawmakers into accepting products and services which degrade, rather than enhance, social relations. Legislatures will be indifferent or reluctant to act until there is some sort of social outcry or

24. *Id.* at 81.
25. *Id.* at 132.
26. *Id.*

> the impact on society is too great to ignore. The law will arrive too late, after social norms have already been established and when it is much more difficult to reverse society's course.[27]

Before showing how Kim's consentability framework can be applied to the facial recognition technology debates, we will sketch the outline of dystopian future. The scenario is a thought experiment about a possible world where the dire risks posed by facial recognition technology poses are realized. The transition from the present world to this hypothetical future could occur due to structural problems like the ones Kim outlines in the above passage.

Much of the discussion about the immediate and short to medium term problems with facial recognition technology focuses on the harm that could occur if the technology continues to produce inaccurate results.[28] Law-abiding people could be put on government watchlists, deprived of due process in court, prevented from accessing places they should be allowed to enter, and questioned or detained by law enforcement. Government and industry could deny people access to their assets, deprive them of job opportunities, and mischaracterize their identities and behaviors. While everyone is vulnerable to these harms, false positives and negatives disproportionately affect minorities, especially people of color.[29] These discussions also emphasize that the law poses few restrictions on facial recognition technology. Furthermore, there is little transparency about how facial recognition technology is used as we can see from the fact that state legislatures are not required to openly debate and approve (i.e., consent) using driver's license photos for government facial recognition databases.[30] Finally, internal policies for the

---

27. NANCY KIM, CONSENTABILITY, CONSENT AND ITS LIMITS S 118-119 (2019).

28. *See, e.g.,* Sahil Chinoy, *The Racist History Behind Facial Recognition*, N.Y. TIMES (July 10, 2019), https://www.nytimes.com/2019/07/10/opinion/facial-recognition-race.html; 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; Natasha Singer, *Amazon's Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says*, N.Y. TIMES (July 26, 2018), https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html.

29. *See* Joy Boulamwini, *When the Robot Doesn't See Dark Skin*, N.Y. TIMES (June 21, 2018), https://www.nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html.

30. Drew Harwell, *FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches*, WASH. POST (July 7, 2019),

government using facial recognition technology are not standardized.

Over time, advances in facial recognition technology might eliminate all kinds of errors. Unfortunately, more accurate versions of the technology pose even greater dangers because the problems with facial surveillance are fundamental and unique. Evan Greer contends, "Biometric surveillance powered by artificial intelligence is categorically different than any surveillance we have seen before. It enables real-time location tracking and behavior policing of an entire population at a previously impossible scale."[31] The technology can be used to create chill that routinely prevents citizens from engaging in First Amendment protected activities, such as free association and free expression. They could also gradually erode due process ideals by facilitating a shift to a world where citizens are not presumed innocent but are codified as risk profiles with varying potentials to commit a crime. In such a world, the government and companies alike will find it easy to excessively police minor infractions, similar to how law enforcement already uses minor infractions as pretexts to cover up more invasive motives.[32] Surveillance tools bestow power on the watcher. Abuse of the power that was once localized and costly could become systematized, super-charged, and turnkey. Companies could expand their reach of relentless and manipulative marketing by peddling their wares over smart signs that display personalized advertisements in public spaces. And as more emotional states, private thoughts, and behavioral predictions are coded from facial data, people will lose more and more control over their identities. They could be characterized as belonging to groups that they don't identify with or don't want everyone knowing they belong to. And while schools might monitor students more intensely and make the educational environment more like a prison, bad actors will have opportunities to create even more general security problems through hacking and scraping.

---

https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.

31. Evan Greer, *Don't Regulate Facial Recognition. Ban it.*, BUZZFEED NEWS (July 18, 2019), https://www.buzzfeednews.com/article/evangreer/dont-regulate-facial-recognition-ban-it.

32. *See* Angela Caputo, *Berwyn Police Rack up Citations with Questionable DUI Checkpoints*, CHI. TRIB. (Sept. 20, 2015), https://www.chicagotribune.com/investigations/ct-berwyn-dui-checkpoints-met-20150920-story.html.

How might this social transformation occur? With the law lagging behind innovation and an existing legacy of name-face databases ripe for plug-and-play expansion, the perceived advantages of easily and cheaply analyzing biometric faceprints that link our on- and off-line lives could drive widespread adoption. As this happens, people could get used to thinking of facial recognition technology as the go-to solution for solving all kinds of problems throughout society. Tired of remembering and entering in a passcode to unlock your phone? Try facial recognition. Long lines boarding a plane? Maybe facial recognition could help. Not sure who's knocking at your door? Facial recognition could tell you. Missing your child while they're at summer camp and want to watch them play? Facial recognition to the rescue! And so on.

Patching social problems with technological solutions is easier than mustering the will to solve harder issues around inequality, education, and opportunity. The drumbeat of security stokes fear. And enhancing convenience is a powerful motivating force in American life. Consequently, it won't be reasonable to expect most people to grasp that they should summon the political will to push back against incremental buildup of negative effects that initially concentrate the worst outcomes on people of color and activists. Immediate gratification, abstract perceptions of risk, and certain harm is a recipe for doom.

IV. THE FRAMING PROBLEM: OBSCURITY, NOT PRIVACY OR ANONYMITY

To apply Kim's insights to the debate over facial recognition technology, it is useful to begin by leveraging a concept from the literature on cognition that she relies upon: *framing effects*. Word choice can have a framing effect because how options and issues are presented can impact how people perceive risks and what solutions they propose. For example, since research into the cognitive bias of loss aversion suggests that people tend to perceive losses as more significant than gains, it matters whether doctors describe a surgical procedure as having a 90% success rate or a 10% failure rate.[33]

33. Erving Goffman, Frame Analysis 7 (Harper Colophon ed., 1974); Robert D. Benford & David A. Snow, *Framing Processes and Social Movements: An Overview and Assessment*, 26 ANN. REV. SOC. 611, 614 (2000); Dennis Chong & James N. Druckman, *Framing Theory*, 10 ANN. REV. POL. SCI. 103, 104 (2007); Laura E. Drake & William A. Donohue, *Communicative Framing Theory in Conflict Resolution*, 23 COMM. RES. 297, 300 (1996); Daniel Kahneman & Amos Tversky, *Choices, Values, and Frames*, 39 AM. PSYCHOLOGIST 341, 341 (1984); Deborah Tannen, *What's in a Frame? Surface*

The debates over facial recognition technology, like other debates over surveillance, are marred by the fact that they are framed around the concepts of "privacy" and "anonymity" instead of "obscurity."[34] The harm from surveillance is often described as loss of privacy.[35] But the concept of privacy is famously amorphous. It can mean almost anything from secrecy to intimacy to control to "the right to be let alone."[36] With respect to surveillance, people often make the argument that as long as you're in "public," people can already see you; since it is not reasonable to ask people to avert their eyes in public, you allegedly have no privacy in accessible spaces.[37] Others make the argument that they don't fear surveillance as a privacy threat because they have "nothing to hide."[38] These arguments either reduce privacy to secrecy and assume that only things that are completely stowed away are worthy of protection, or else myopically frame privacy as a concern for individuals, not society writ large.

At least initially, framing surveillance harms in autonomy terms is also problematic. This is because the concept of autonomy can be stretched in an almost limitless fashion. Jeb Rubenfeld writes:

> What, then, is the right to privacy? What does it protect? A number of commentators seem to think that they have it when they add the word 'autonomy' to the privacy vocabulary. But to call an individual 'autonomous' is simply another way of saying that he is morally free, and to say that the right to privacy protects freedom adds little to our understanding of the doctrine. To be sure, the privacy doctrine involves the 'right to make choices and decisions,' which, it is said, forms the 'kernel' of autonomy. The question, however, is which

---

Evidence for Underlying Expectations, in Framing in Discourse 137 (Deborah Tannen ed., 1979); Amos Tversky & Daniel Kahneman, *The Framing of Decisions and the Psychology of Choice*, 211 SCIENCE 453, 453 (1981).

34. *See, e.g.,* Joseph Kupfer, *Privacy, Autonomy, and Self-Concept*, 24 AM. PHIL. Q. 81,81 (1987); Louis Henkin, *Privacy and Autonomy*, 74 COLUM. L. REV. 1410, 1419 (1974).

35. *See* Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L. J. 1131, 1131 (2011).

36. *See* DANIEL SOLOVE, UNDERSTANDING PRIVACY 13 (First Harvard Univ. Press eds., 2008).

37. For an exploration and rebuttal of this argument, *see* Woodrow Hartzog, *The Public Information Fallacy*, 99 B.U. L. REV. 459, 461 (2019).

38. *See* Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007).

choices and decisions are protected?[39]

While surveillance certainly implicates Kim's twin foci of individual and social autonomy, the concept of autonomy is likely too broad to meaningfully and consistently resonate with people who are making decisions that would put it at risk. In the context of facial recognition technology, autonomy, like privacy, needs a better, more specific, framing. We propose framing surveillance issues generally, and facial recognition specifically, as a loss of "obscurity," a diminution that clearly detracts from many of the goods that autonomy is valued for enabling.

To briefly summarize key points from our extensive prior research, the concept of obscurity concerns transaction costs—the ease or difficulty of finding information and correctly interpreting it.[40] The harder it is to locate information or reliably understand what it means in context, the safer, practically speaking, the information is. Safety is a matter of probability, not certainty, since a range of factors can change transaction costs. Examples of such factors include advances in technological capabilities, the democratization of technological functions, and advances in data science. For much of history, obscurity has been protected by what Harry Surden calls "structural constraints."[41] These are not legal protections, they are technological limitations such as a lack of easy to use, inexpensive, and accurate means of identifying us, tracking our movements, behaviors, and communications, and inferring our thoughts and emotions. Structural constraints may also be biological. For instance, the fact that the human cognitive and perceptual systems can only make sense of and store limited amounts of information without technological aid. While the transaction costs imposed by warrant requirements, encryption software, and other strategies provide some obscurity protections, they are of limited value in a society that rules out privacy protections in public and when information is disclosed to third parties (e.g., the Third Party Doctrine).[42] They are also limited

39. Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 750-52 (1989).

40. Evan Selinger & Woodrow Hartzog, *Obscurity and Privacy*, *in* ROUTLEDGE COMPANION TO PHILOSOPHY OF TECHNOLOGY (Joseph Pitt and Ashley Shew, eds. Forthcoming 2014); Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH & LEE L. REV. 1343 (2015); Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1 (2013); Woodrow Hartzog & Frederic Stutzman, *Obscurity By Design*, 88 WASH. L. REV. 385 (2013).

41. Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605 (2007).

42. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) (providing a defense of the third-party doctrine).

because our society fundamentally does not view privacy in terms of nuanced categories. like select publics or private publics, where information is meant to be disclosed to some audiences but not everyone, rather than blunt ones like anonymity, which presuppose that nobody knows who you are.

In order for people to be capable of giving valid consent to a range of surveillance practices, including facial recognition, they need to have a better understanding of how they rely on obscurity to protect their privacy. By taking obscurity for granted, they miss how it fosters individual autonomy. Obscurity enables people to establish meaningful and intimate relationships because it allows us to selectively disclose information and share different aspects of our identity in different contexts.[43] Obscurity enables us to develop intellectually and emotionally by giving us breathing room to embrace risks and make mistakes without the stigma of being forever associated with failures and fads.[44] Obscurity enables citizens to participate in democracy by allowing them to confidently engage in political activities without worrying about recriminations from the government.

However, such appreciation means little on its own. What good is recognizing the value of obscurity if it is unobtainable? Consequently, this understanding needs to be bolstered by substantial changes to the privacy regulatory regime that provide meaningful obscurity protections. At present, neither a great obscurity awakening, nor a regulatory obscurity revolution are likely; both entail too much of a departure from entrenched theories and practices.

V. FACIAL RECOGNITION TECHNOLOGY: INDIVIDUAL CONSENT AND COLLECTIVE AUTONOMY

Should facial recognition surveillance be consentable? By appealing to Kim's framework to answer this question, we must ask whether it is possible to validly consent to the proposed activity, and whether social harms caused by the activity outweigh its social benefits. It seems unlikely that someone could give valid consent to most forms of facial surveillance because the context in which such consent would be sought frustrates the pre-conditions for meaningful decision-making. In order for consent to data and surveillance practices to be knowing and voluntary, at least three

43. *See* ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1956).

44. For an exploration on the importance of privacy for "play" and human flourishing, *see* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904 (2013).

pre-conditions should exist: (1) such a request should be infrequent, (2) the harms to be weighed must be vivid, and (3) there should be incentives to take each request for consent seriously.[45] If the requests for consent are too frequent people will become overwhelmed and desensitized. This renders them susceptible to user interfaces and dense, confusing, turgid privacy policies that are designed to exploit their exhaustion to extract consent. If the harms are framed in terms of abstract notions of privacy and autonomy or the possibility of abuse is too distant to be readily foreseeable, then people's cost/benefit calculus may be corrupted by an inability to take adequate stock of the risks. Finally, if the risk of harm is distributed over the course of many different decisions—as is common with loss of obscurity through surveillance—people will lack the proper incentive to take each request for consent seriously. After all, no single decision represents a significant threat. Instead, society is exposed to death by a thousand cuts, with no particular cut rising to the threat level where substantive and efficacious dissent occurs.

In the case of facial recognition technology things are further complicated by the fact that the public is routinely given seemingly good reasons to believe that the social benefits caused by consenting to surveillance would outstrip any social harms. As we previously described this illusory worldview:

> From this perspective, you'll never have to meet a stranger, fuss with passwords, or worry about forgetting your wallet. You'll be able to organize your entire video and picture collection in seconds—even instantly find photos of your kids running around at summer camp. More important, missing people will be located, schools will become safe, and the bad guys won't get away with hiding in the shadows or under desks. Total convenience. Absolute justice. Churches completely full on Sundays. At long last, our tech utopia will be realized.[46]

But many of these touted benefits are meager, incremental improvements that could likely be approximated through less dangerous means. For example, facial recognition is being deployed to streamline the hassle associated with paper boarding

---

45. *See* Neil Richards and Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1466 (2019).

46. 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.

passes, cash and debit cards, and passcodes and fingerprint access.[47] But these technologies already worked reasonably (or exceptionally) well. The legitimately compelling benefits, such as finding missing people and keeping people safe, would require large, promiscuous databases working with interconnected and ubiquitous sensors making a mind-bogglingly large number of fraught algorithmic decisions. Such an infrastructure would extract a massive toll on our freedoms, civil liberties, and autonomy. Setting up this infrastructure also intrinsically incentivizes its use due to the sunk cost fallacy, a cognitive bias emphasized by the cognitive science literature that Kim discusses.[48] The sunk cost fallacy is the tendency for humans continue down a particular course once they have made significant investment in it. Spending all the resources required for getting the infrastructure built and stoking expectations that the infrastructure is required for social progress would therefore make it hard to change course and accept the reality that previous resources could have been better spent.

The harms of facial surveillance are legion. The mere existence of facial recognition systems, which are often invisible, harms civil liberties because people will act differently if they suspect they're being surveilled.[49] Even legislation that promises stringent protective procedures won't prevent chill from impeding crucial opportunities for human flourishing by dampening expressive and religious conduct. Warrant requirements for facial recognition will merely set the conditions for surveillance to occur, which will normalize tracking and identification, reorganize and entrench organizational structure and practices, and drive government and industry investment in facial recognition tools and infrastructure.

Facial recognition technology also enables a host of other abuses and corrosive activities, many of which we outlined in the

---

47. *See* Brian Feldman, *Replacing Touch ID With Face ID is a Worse Idea Than You Think*, N.Y. INTELLIGENCER (Sept. 12, 2017), http://nymag.com/intelligencer/2017/09/replacing-touch-id-with-face-id-is-worse-than-you-think.html; Betsy Isaacson, *Facial Recognition Systems Turn Your Face Into Your Credit Card, PIN, Password*, HUFFPOST (July 19, 2013), https://www.huffpost.com/entry/facial-recognition-credit-card_n_3624752; Gregory Wallace, *Instead of the Boarding Pass Bring Your Smile to the Airport*, CNN (Sept. 10, 2018), https://www.cnn.com/travel/article/cbp-facial-recognition/index.html.

48. *See* Jamie Ducharme, *The Sunk Cost Fallacy is Ruining Your Decisions. Here's How*, TIME (July 26, 2018), https://time.com/5347133/sunk-cost-fallacy-decisions/.

49. Neil Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013).

previous section.

- Disproportionate impact on people of color and other minority and vulnerable populations.
- Due process harms, which might include shifting the ideal from "presumed innocent" to "people who have not been found guilty of a crime, yet."
- Facilitating harassment and violence.
- Denial of fundamental rights and opportunities, such as protection against "arbitrary government tracking of one's movements, habits, relationships, interests, and thoughts."
- The suffocating restraint of the relentless, perfect enforcement of law.
- The normalized elimination of practical obscurity.
- Digital epidermalization and applied junk science (e.g., digital phrenology).
- The amplification of surveillance capitalism.
- Security vulnerabilities.

Finally, even assuming that an individual could consent, facial recognition systems inevitably will lead to unacceptable harm to our collective autonomy. In a democracy, it is reasonable to expect that many people will put greater weight on the costs and benefits of a particular decision that are relevant to them and people like them. Such is the pull of tribalism and privilege, which bias decision-making much like the compromising factors that Kim emphasizes. In practice, this means if citizens are not members of minority communities, they might not be sufficiently concerned with how their gain from facial recognition comes at other people's expense. Addressing this hidden cost, Chris Gillard aptly states:

> Until we can come to better terms with the disparate impacts of privacy harms, the privileged will continue to pay for luxury surveillance, in the form of Apple Watches, IoT toilets, quantified baby products, Ring Doorbells, and Teslas, while marginalized populations will pay another price: Surveillance, with the help of computer data, deployed against them—in the form of ankle bracelets, license plate readers, drones, facial recognition, and cell-site simulators. As one group pays to be

> watched, other groups continue to pay the price for being watched.[50]

Over time, when majority groups consent to offers that are cost-benefit justified for themselves, large-scale social transformation can result that compromises the autonomy interests of marginalized groups. The end result is likely a society that won't be able to provide an adequate base level of autonomy protections for all citizens. For if marginalized groups come to experience the pervasive chill of having not just their public movements but also their identities (e.g., gay-identifying algorithms) and mental states (e.g., emotion detection) monitored—then the rest of society isn't justified in making choices that lead to this outcome. The end result would be the unraveling of obscurity, and with it, the erosion of democratic legitimacy through tyranny of the majority—an outcome that Kim characterizes as unjust by assigning primacy to collective autonomy in her framework.

VI. CONCLUSION: MORATORIA AND BANS

When Kim considers bans in *Consentability*, she approaches the issue through the framing of paternalism to inquire into the liberties the government is justified in curtailing. For example, she argues that it should not be consentable to smoke tobacco or marijuana in public due to the adverse harm it can cause to third parties, but junk food should only be more restrictively regulated, not banned.[51] Bans, however, are not limited to expressions of state power. In both principle and practice, they also can be restrictions upon it.

To that end, an unexpected shift in governance has begun. U.S. cities have started banning government agents from using facial recognition technology.[52] Statewide moratoriums on government agents are being considered too.[53] Bans, whether temporary or permanent, are extremely rare in U.S. governance because lawmakers and policy advocates often make three core

---

50. Chris Gilliard, *Privacy's Not an Abstraction*, FAST COMPANY (Mar. 25, 2019), https://www.fastcompany.com/90323529/privacy-is-not-an-abstraction.

51. NANCY KIM, CONSENTABILITY: CONSENT AND ITS LIMITS 168-171 (2019).

52. Caroline Haskins, *Oakland Becomes Third U.S. City to Ban Facial Recognition*, VICE MOTHERBOARD (July 17, 2019), https://www.vice.com/en_us/article/zmpaex/oakland-becomes-third-us-city-to-ban-facial-recognition-xz.

53. Steve LeBlanc, *Mass. Lawmakers Aim to Block Facial Recognition Technology*, BOSTON 25 NEWS (June 22, 2019), https://www.boston25news.com/news/mass-lawmakers-aim-to-block-facial-recognition-technology/960520513.

presumptions about regulation. The first is that extreme fears about new technologies should be viewed as over-reactions that parallel previous panics about technologies that society effectively adapted to, such as the automobile, radio, and television.[54] The second is that all dual-use technologies should be integrated into society through policies that aim to appropriately balance costs and benefits.[55] The third is that the best approach to regulating surveillance is through tech-neutral legislation that applies to all surveillance technologies and does not single out specific ones for unique treatment.[56]

For the reasons that we have provided, we believe that these presumptions do not apply here and conclude that, at a minimum, moratoriums are justified because the conditions for consentability for facial recognition technology have not been met. Furthermore, face surveillance of all kinds presents a panoply of harms, most notably corrosion of collective autonomy through the chill of increased surveillance and machines indulge the fatally flawed notion of perfect enforcement of the law. Neither consent nor procedural frameworks like warrant requirements are sufficient to address these harms. As such, we argue face surveillance should be banned. Regulating the government without also imposing restrictions on technology companies is insufficient, but a promising start because, at present, government agents pose the greatest threats.

As Clare Garvie rightly observes, mistakes with facial recognition technology can have deadly consequences.[57] This means they can trample an individual's right to be free from bodily harm, the highest of the individual autonomy rights in Kim's

---

54. *See* Adam Thierer, *The Great Facial Recognition Technopanic of 2019*, MERCATUS CTR. (May 17, 2019), https://www.mercatus.org/bridge/commentary/great-facial-recognition-technopanic-2019.

55. *See, e.g.,* James O'Neil, *How Facial Recognition Makes You Safer*, N.Y. TIMES (June 9, 2019), https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html; *America is Turning Against Facial-Recognition Software*, ECONOMIST (May 23, 2019), https://www.economist.com/united-states/2019/05/23/america-is-turning-against-facial-recognition-software.

56. *See, e.g.,* Judith Donath, *You Are Entering an Ephemeral Bio-Allowed Data Capture Zone*, MEDIUM (July 23, 2018), https://medium.com/@judithd/you-are-entering-an-ephemeral-bio-allowed-data-capture-zone-5ecafd2dbdaf.

57. Clare Garvie, *Facial Recognition Threatens Our Fundamental Rights*, WASH. POST (July 19, 2018), https://www.washingtonpost.com/opinions/facial-recognition-threatens-our-fundamental-rights/2018/07/19/a102703a-8b64-11e8-8b20-60521f27434e_story.html.

framework.[58]

> What happens if a system like this gets it wrong? A mistake by a video-based surveillance system may mean an innocent person is followed, investigated, and maybe even arrested and charged for a crime he or she didn't commit. A mistake by a face-scanning surveillance system on a body camera could be lethal. An officer alerted to a potential threat to public safety or to himself, must, in an instant, decide whether to draw his weapon. A false alert places an innocent person in those crosshairs.[59]

Lawmakers could regulate facial recognition a few different ways, and all but one will lead to an irrevocable erosion of obscurity and collective autonomy. When considering how to regulate private commercial use of facial recognition, lawmakers will be tempted to go back to that old standby regulatory mechanism that they always reach for when they lack political capital, resources, or imagination: consent. Consent is attractive because it pays lip service to the idea that people have diverse preferences, it's steeped in the law, and at a glance appears to be a compromise between competing values and interests. But as Kim demonstrated and we argue, it is fool's gold for facial recognition technologies, especially face surveillance. Even highly regulated and constrained use of facial recognition technology that has been agreed to will lead to an erosion of obscurity and a harm to our collective autonomy without actually serving our individual autonomy interests.

The problem is that there aren't many proven alternatives to consent regimes for commercial use of facial recognition that go beyond mere procedural frameworks. If the E.U.'s General Data Protection Regulation is any guide, the most prominent alternative to legitimize collection and processing of face biometric data is to require companies to have a "legitimate interest" in doing so.[60] But

---

58. NANCY KIM, CONSENTABILITY: CONSENT AND ITS LIMITS (2019).

59. Garvie, *supra* note 56.

60. General Data Protection Regulation 2016/679 of May 25, 2018, Lawfulness of Processing, art. 6(1)(f), http://www.privacy-regulation.eu/en/article-6-lawfulness-of-processing-GDPR.htm; *Recommendations for Implementing Transparency, Consent, and Legitimate Interest Under the GDPR*, CTR. FOR INFO. POL'Y LEADERSHIP (May 17, 2017), https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2017/06/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf ("Legitimate interest may be the most accountable ground for processing in many contexts, as it requires an assessment and balancing of the risks and benefits of processing for organisations, individuals[,] and society . . . . The legitimate interests to be considered may include

what constitutes a "legitimate interest" is notoriously slippery and subject to drift. Lawmakers have yet to get serious in using this concept to significantly rein in the power wielded by data controllers.

So, if facial recognition becomes entrenched in the private sector by procedural frameworks, that means that in addition to a warrant framework's accretion problem, the government will also have a backdoor to retroactive surveillance via the personal data industrial complex. Through public/private cooperation, surveillance infrastructure will continue to be built, chill will still occur, harms will still happen, norms will still change, collective autonomy still will suffer, and people's individual and collective obscurity will bit by bit continue to diminish.

The end result is that even if advocates of consent and warrant requirements got everything on their wish list, society would still end up worse off. We would suffer unacceptable harm to our obscurity and collective autonomy through a barrage of I agree buttons and search warrants powered by government and industry's unquenchable thirst for more access to our lives. There is only one way to stop the harms of face surveillance. Ban it.

---

the interests of the controller, other controller(s), groups of individuals[,] and society as a whole."); *CIPL Examples of Legitimate Interest Grounds for Processing of Personal Data*, CTR. FOR INFO. POL'Y LEADERSHIP (Mar. 16, 2017), https://iapp.org/media/pdf/resource_center/final_cipl_examples_of_legitimate_interest_grounds_for_processing_of_personal_data_16_march_2017.pdf.