

# Normalizing Facial Recognition Technology and The End of Obscurity\*

Woodrow Hartzog

(Professor of Law, Boston University)

Evan Selinger

(Professor of Philosophy, Rochester Institute of Technology)

Judy Hyojoo Rhee

(Independent Scholar)

---

**ABSTRACT** This article argues that facial recognition technology is the most dangerous surveillance tool ever invented. Given the unique threats this morally suspect tool poses to privacy, civil liberties, human flourishing, and democracy, the only appropriate response is a ban. To justify our position, we explain why facial recognition is distinctive among biometrics, clarify how even seemingly benign and positive uses of the technology can trigger dangerous normalization dynamics, and pinpoint why current United States laws (with reverberations in the EU's AI Act) are designed to accelerate a slippery slope that makes mass surveillance nearly inevitable. Our most fundamental contribution lies in demonstrating how the concept of "obscurity" connects all three arguments: facial recognition algorithms technologically eviscerate obscurity, normalization psychologically undermines it, and the law doctrinally abandons it - a perfect storm that only prohibition can stop.

---

**KEYWORDS:** Facial Recognition Technology - Obscurity - Privacy - Normalization

---

**TABLE OF CONTENTS:** 1. Introduction. – 2. Facial Recognition Technology: A Uniquely Powerful Surveillance Tool. – 3. Normalizing Facial Recognition Technology. – 4. How the Law Facilitates Normalizing Facial Recognition. – 5. What Should Be Done?. – 6. Conclusion.

---

## 1. Introduction

This article advances a radical argument: facial recognition technology should be banned. Not limited, not constrained by guardrails, but outright prohibited. No society is better off for having facial recognition technology in it.

We reach this dire conclusion by examining three interconnected issues. First, facial recognition is fundamentally different from every other surveillance tool. It exploits our faces - features that are difficult to hide or change and often define who we are. Combined with billions of photos already online, facial recognition technology enables anyone to identify and track strangers instantly, inexpensively, and on a massive scale.

Second, even seemingly good uses of facial recognition technology create a psychological trap. When we unlock phones with our faces or breeze through airport security, we grow comfortable with being scanned. Each use makes the next seem less invasive. We call this process "normalization," and contend it only moves in one direction - toward accepting more surveillance.

Third, U.S. privacy laws exacerbate this problem rather than alleviating it. They focus on a threshold of harm that ignores small but persistent invasions that add up over time. Most dangerously, these "privacy nicks" actually weaken legal protections as people get used to surveillance, creating a downward spiral where yesterday's outrage becomes today's reasonable take on normal daily life. Even the EU's AI Act, despite its ban on real-time biometric surveillance in public spaces, contains exceptions that risk normalizing the very practices they are designed to prohibit. These three forces - technology, psychology, and law - work together to destroy what we call "obscurity," a type of privacy that we take for granted, which is essential for civil liberties, human flourishing, and democracy.

We proceed by examining each force in

---

\* Article submitted to double-blind peer review. Portions of this essay have been adapted from W.Hartzog, E. Selinger and J. Gunawan, *Privacy Nicks: How the Law Normalizes Surveillance*, in *Washington University Law Review*, vol. 101, 2024; E. Selinger and J.H. Rhee, *Normalizing Surveillance*, in *North European Journal of Philosophy*, vol. 22, 2021, 49; E. Selinger and W. Hartzog, *The Inconsistency of Facial Surveillance*, in *Loyola Law Review*, vol. 66, 2019, 101; and W. Hartzog, *Two AI Truths and a Lie*, in *Yale Journal of Law and Technology*, vol. 26, 2024, 595.

detail. Section 2 explains what makes facial recognition uniquely dangerous. Section 3 reveals how normalization works. Section 4 shows how U.S. law fails. Section 5 considers legal remedies but shows only one response is truly justified: prohibition.

## 2. Facial Recognition Technology: A Uniquely Powerful Surveillance Tool

There is only one way to have an honest and realistic discussion about facial recognition technology. We must first admit that it is a uniquely powerful surveillance tool that poses grave privacy and civil liberties risks.<sup>1</sup> At its core, facial recognition technology is morally suspect because it is a perfect tool for oppression. Even this tool's seemingly benign and beneficial uses could normalize more invasive ones, tilting democracies, including the United States, toward authoritarianism.<sup>2</sup> What's more, Europe, which set a global example with its groundbreaking EU AI Act and general commitment to protecting human rights, could buckle under public pressure for algorithmically provided security and convenience.<sup>3</sup>

Most U.S. policymakers reject banning

facial recognition outright.<sup>4</sup> Some endorse targeted prohibitions, like banning real-time remote biometric identification in publicly accessible spaces (e.g., one of the restrictions in the EU AI Act), but even the most robust prohibitions to date are porous with broad exemptions.<sup>5</sup> Similarly, forward-thinking scholars propose novel measures to limit AI-infused surveillance, including facial recognition technology, that could enhance crucial Constitutional protections, such as the Fourth Amendment. But there are always exceptions, especially where public safety is concerned.<sup>6</sup> And most consider sweeping proposals for an outright ban, including prohibiting the use of the tool at airports, concerts, stores, and even our phones, impractical and overzealous.

When most policymakers are presented with the rallying cry of "ban it!" they nearly cannot believe sensible people would take such an extreme and uncompromising position for a technology with so many seemingly desirable uses. Lawmakers (particularly in the U.S.) and industry representatives who reject outright prohibitions seem to commonly make two misguided assumptions: (1) all digital innovations should be encouraged; (2) the key to responsible innovation is to limit the harmful uses of tools.<sup>7</sup> This is the allure of "dual use technologies," those capable of harmful and beneficial uses.<sup>8</sup> As long as a tool

<sup>1</sup> E. Selinger and W. Hartzog, *The Inconsistency of Facial Surveillance*, in *Loyola Law Review*, vol. 66, 2019, 101.

<sup>2</sup> Adrienne de Ruiter introduced the concept of "morally suspect" to describe deepfake technology. De Ruiter claims that since there are some justified uses of deepfakes, the technology cannot be classified as intrinsically morally wrong. However, she notes that since deepfake technology "lends itself particularly well" to actions that violate fundamental moral norms, "it should be classified in a manner that puts on high alert—which is to say, as "morally suspect." A. de Ruiter, *The Distinct Wrong of Deepfakes*, in *Philosophy & Technology*, vol. 34, 2021, 1311-1332, <https://link.springer.com/article/10.1007/s13347-021-00459-2>; W. Hartzog, E. Selinger and J. Gunawan, *Privacy Nicks: How the Law Normalizes Surveillance*, in *Washington University Law Review*, vol. 101, 2024, 717; E. Selinger and B. Leong, *The Ethics of Facial Recognition Technology*, in C. Véliz (ed.), *The Oxford Handbook of Digital Ethics*, Oxford, UK, Oxford University Press, 2023, <https://academic.oup.com/edited-volume/37078/chapter-abstract/337809992?redirectedFrom=fulltext>.

<sup>3</sup> Parliament and Council Regulation 2024/1689 laying down Harmonised Rules on Artificial Intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 and EU Parliament-EU Council, Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (14 May 2024).

<sup>4</sup> M. Fidler and G. Hurwitz, *An Overview of Facial Recognition Technology in the United States*, in R. Matulionyte and M. Zalnieriute (eds.), *The Cambridge Handbook of Facial Recognition in the Modern State*, Cambridge, UK, Cambridge University Press, 2024.

<sup>5</sup> Shubam, *EU AI Act Will Fail Commitment to Ban Biometric Mass Surveillance*, in *Reclaim Your Face 2024*, <https://reclaimyourface.eu/eu-ai-act-will-fail-commitment-to-ban-biometric-mass-surveillance>; Access Now, *The EU AI Act: A Failure for Human Rights, a Victory for Industry and Law Enforcement*, in *Access Now*, 2024, [www.accessnow.org/press-release/ai-act-failure-for-human-rights-victory-for-industry-and-law-enforcement](http://www.accessnow.org/press-release/ai-act-failure-for-human-rights-victory-for-industry-and-law-enforcement).

<sup>6</sup> A.G. Ferguson, *Facial Recognition and the Fourth Amendment*, in *Minnesota Law Review*, vol. 105, 2021, 1105 and 1132.

<sup>7</sup> See, e.g., U.S. Senate Committee on Commerce, Science, and Transportation, *Winning the AI Race: Strengthening U.S. Capabilities in Computing and Innovation*, 8 May 2025, [www.commerce.senate.gov/2025/5/winning-the-ai-race-strengthening-u-s-capabilities-in-computing-and-innovation\\_2](http://www.commerce.senate.gov/2025/5/winning-the-ai-race-strengthening-u-s-capabilities-in-computing-and-innovation_2) ("The way to beat China in the AI race is to outrace them in innovation, not saddle AI developers with European-style regulations").

<sup>8</sup> See, C. Kang, *OpenAI's Sam Altman Urges A.I. Regulation in Senate Hearing*, N.Y. Times, 16 May 2023, [www.nytimes.com/2023/05/16/technology/openai](http://www.nytimes.com/2023/05/16/technology/openai)

can do *some* good, why not keep it around?

Policymakers often try to regulate dual-use tools in a technology-neutral way. They believe passing tech-neutral rules like “do not lie” and “do not harm” that apply to all tools is the best way to discourage bad outcomes while encouraging good ones. To regulate facial recognition technology in a tech-neutral manner, lawmakers might assign risk tiers and impose stricter limitations on higher-risk activities. Under this approach, police officers would be able to use facial recognition technology to locate missing children, but stalkers would be barred from using facial recognition technology to harass others. Lawmakers could even pass some rules to ensure that tools like facial recognition technology work equally well for dominant groups and marginalized populations. Ultimately, the tech-neutral approach assumes that all innovation can be channeled for the public good and that, with proper oversight, the benefits of facial recognition technology, like every other digital tool, can outweigh the risks.

In many instances, it is a good idea to use tech-neutral regulation to get the most good from dual-use tools.<sup>9</sup> But facial recognition is no ordinary tool. It is the most dangerous surveillance tool ever created. No other surveillance tool rivals its affordances for destruction and oppression. Lawmakers seeking to preserve the benefits of facial recognition underestimate its core purpose and capabilities.

Given the power facial recognition bestows on the watcher, it stands a good chance of constantly drifting towards abuse, with its harms outweighing its benefits. Facial recognition technology deserves to be uniquely stigmatized because it is the most

lethal combination of apparent convince bundled with hidden dangers imaginable. Our faces can reveal who we are, where we’ve been, and what we’re doing more than any other single currently observable trait. Using computer vision and machine learning algorithms to automate the detective work of revealing who an unknown person is based on their most personal physiological features encourages heightened mass surveillance at an unprecedented scale and scope.<sup>10</sup>

As if this was not enough, facial recognition involves more than just identifying who people are. Because facial recognition is easy to implement inside existing surveillance systems, the threat facial recognition systems pose goes far beyond rapidly processing vast amounts of visual data from cameras and comparing detected faces against large databases of known individuals. Cameras with facial recognition capabilities can be easily and cheaply enhanced with related plug-and-play features. One additional tool is emotion recognition software that supposedly infers what people are feeling based on their facial expressions.<sup>11</sup> This type of information is known as facial characterization data, and it is used for junk science. Its misuse has been rightly compared to the discredited, eugenicist-approved, 19th-century practice of cranioscopy (later known as phrenology).<sup>12</sup> According to phrenology, you could learn about a person’s character and mental abilities by studying the shape of different parts of their skull. Consider what could happen now with digital phrenology. If

[i-altman-artificial-intelligence-regulation.html](#) (“Tech companies have argued that Congress should be careful with any broad rules that lump different kinds of A.I. together. In Tuesday’s hearing, Ms. Montgomery of IBM called for an A.I. law that is similar to Europe’s proposed regulations, which outlines various levels of risk. She called for rules that focus on specific uses, not regulating the technology itself. “At its core, A.I. is just a tool, and tools can serve different purposes,” she said, adding that Congress should take a “precision regulation approach to A.I.”).

<sup>9</sup> See, e.g., B.J. Koops, *Should ICT Regulation Be Technology-Neutral?*, in B.-J. Koops, M. Lips, C. Prins and M. Schellekens (eds.), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, vol. 9, The Hague, T.M.C. Asser Press, 2006, 77-108.

<sup>10</sup> J. Stanley, *The Dawn of Robot Surveillance*, in *American Civil Liberties Union*, 2019, [www.aclu.org/publications/dawn-robot-surveillance](http://www.aclu.org/publications/dawn-robot-surveillance). Institutions have also begun to take notice. See Artificial intelligence must be grounded in human rights, says High Commissioner, United Nations (12 July 2023), [www.ohchr.org/en/statements-and-speeches/2023/07/artificial-intelligence-must-be-grounded-human-rights-says-high](http://www.ohchr.org/en/statements-and-speeches/2023/07/artificial-intelligence-must-be-grounded-human-rights-says-high).

<sup>11</sup> N. Andalibi, *Emotion-tracking AI on the job: Workers fear being watched – and misunderstood*, in *The Conversation*, 6 March 2024, <https://theconversation.com/emotion-tracking-ai-on-the-job-workers-fear-being-watched-and-misunderstood-222592>, (“Emotion artificial intelligence uses biological signals such as vocal tone, facial expressions and data from wearable devices as well as text and how people use their computers, promising to detect and predict how someone is feeling. It is used in contexts both mundane, like entertainment, and high stakes, like the workplace, hiring and health care”).

<sup>12</sup> L. Stark and J. Hutson, *Physiognomic Artificial Intelligence*, in *Fordham Intellectual Property, Media & Entertainment Law Journal*, vol. 32, 2022, 922.

police used body cameras with facial and emotional recognition, non-threatening suspects could easily be labeled aggressive. Given pervasive racial, gender, and ability biases, it would not be surprising if those who get misclassified are members of marginalized communities and are at risk of being subject to overly forceful responses.

To better explain why we think facial recognition technology is uniquely dangerous, let us compare it to other combinations of artificial intelligence (AI) and surveillance, like automated license plate readers or social media monitoring systems. These technologies also have profound implications for privacy and power. However, not everyone is on social media or drives a car - and even those who are and do spend time away from them. But we bring our unique faces with us everywhere we go. Our faces are constant, personally identifiable features that we cannot easily change, often cannot conceal without arousing suspicion, and link our online and offline lives. They are also core to our identity. When you think of a friend in your mind, you don't think of their elbow or shoulder. You certainly don't think of their fingerprints or palm prints. You think of their face. Unlike other biometric identifiers, our faces are also already scattered all over the Internet, making turnkey surveillance easy and cheap. No other surveillance system - not license plate readers, CCTV cameras, social media, or any other tool - comes close to that blend of vulnerabilities in terms of depth, breadth, and cost efficiency.

Consider I-XRAY, a recent activist project from Harvard students AnhPhu Nguyen and Caine Ardayfio.<sup>13</sup> They demonstrated how readily available technology and services - Ray-Ban Meta smart glasses (to photograph a face), a public facial recognition search engine (Pimeyes), easily obtainable information from data brokers, and a large language model (that can rapidly pick out and extract personal information from unstructured data) - can produce horrifying results. As the students walked around in public secretly

photographing strangers, they nearly instantaneously identified their victims. While doing so, an app provided them with a wealth of information about the strangers and, in some cases, their family members. This example of hyper-efficient, unauthorized, and hidden doxxing shows just how thin the line is between living in a society with adequate obscurity protections and creating one where your life is an open book.<sup>14</sup>

"Obscurity," as we use the term here, is a concept similar to "privacy." However, obscurity has distinctive features that make it a better term for understanding why facial recognition technology is so menacing.<sup>15</sup> Obscurity refers to the practical challenges, also known as transaction costs, associated with finding or understanding information. Unlike secret or truly anonymous information, obscure information may *literally* be available to a member of the public with sufficient motivation, resources, and know-how. But obscure information is, as a practical matter, difficult enough to find or use that it's likely to remain private. While not a perfect safeguard, obscurity thrives on the friction created by time, effort, and other deterrents. These expenses provide a buffer against causal and arbitrary intrusions into our lives.

Obscurity allows us to have something like group privacy and privacy in public.

Imagine eating at a restaurant and two strangers, who are not public figures, are having an intimate, quiet conversation about their personal lives at another table. They will be protected by a natural zone of obscurity that prevents most people from trying to hear much of what they have to say. Of course, determined intruders will pose a threat. A nosy person might be a problem, and a gossip who has the rare skill of being able to read lips

<sup>14</sup> This is to say nothing of the risk of fraud and identity theft, which becomes irreversible when biometric data is stolen or exposed in a data breach.

<sup>15</sup> See, e.g., W. Hartzog and E. Selinger, *Surveillance as Loss of Obscurity*, in *Washington and Lee Law Review*, vol. 72, 2015, 1343-46 [hereinafter Hartzog and Selinger, *Surveillance*]; W. Hartzog and E. Selinger, *Increasing the Transaction Costs of Harassment*, in *Boston University Law Review Annex*, vol. 95, 2015, 47; E. Selinger and W. Hartzog, *Obscurity and Privacy*, in J. Pitt and A. Shew (eds.), *Spaces for the Future: Routledge Companion to Philosophy of Technology*, London, Routledge, 2018, [www.routledge.com/Spaces-for-the-Future-A-Companion-to-Philosophy-of-Technology/Pitt-Shew/p/book/9780415842969](http://www.routledge.com/Spaces-for-the-Future-A-Companion-to-Philosophy-of-Technology/Pitt-Shew/p/book/9780415842969); see also W. Hartzog and F. Stutzman, *The Case for Online Obscurity*, in *California Law Review*, vol. 101, 2013, 1, especially 5.

<sup>13</sup> J. Cox, *Someone Put Facial Recognition Tech onto Meta's Smart Glasses to Instantly Dox Strangers*, in *404 Media*, 2024, [www.404media.co/someone-put-facial-recognition-tech-onto-metas-smart-glasses-to-instantly-dox-strangers](http://www.404media.co/someone-put-facial-recognition-tech-onto-metas-smart-glasses-to-instantly-dox-strangers); K. Hill, *Two Students Created Face Recognition Glasses. It Wasn't Hard*, in *New York Times*, 2024, [www.nytimes.com/2024/10/24/technology/facial-recognition-glasses-privacy-harvard.html](http://www.nytimes.com/2024/10/24/technology/facial-recognition-glasses-privacy-harvard.html).

is especially dangerous. However, most people will go about their lives without bothering to find out who is at the table and why they are having a particular discussion. They lack the incentive to divert their attention, and the effort required to snoop is better spent elsewhere.

Contrast this scenario with the same two strangers wanting to have the same conversation while strolling through a smart city park where surveillance cameras are plastered everywhere. Furthermore, imagine the cameras linked to the same technologies that were used in the I-XRAY demonstration, along with emotion recognition and lip-reading software, which are easy add-ons. Given the EU AI Act, the scenario is more likely to occur in the U.S. than in Europe. However, as our discussion of normalization will suggest, things may change.

The mere presence of this infrastructure could easily have chilling effects that prevent people from speaking their minds.<sup>16</sup> After all, there will be a dramatic reduction in the transaction costs of surveillance and data processing, making it easier and more likely for public spaces to be constantly watched and analyzed. The reasonable expectation of obscurity - and the freedom it provides - would be eroded by the constant potential for observation and analysis. Chilling effects would occur whether or not anyone actively monitors the data in real-time. The mere possibility is destabilizing.

These examples highlight two important things. First, it is easy to take obscurity for granted. For much of history, obscurity protections have not required legal measures; technological limitations have sufficed. Consider this analogy. Today, most people are not worried about the government reading their minds. Indeed, it would seem paranoid to believe the FBI or CIA has access to secret, perfected telepathy machines. And yet, not too long out, it would have seemed far-fetched to imagine government agents would have access to technology that could identify us by our faces wherever we go. And neurotechnology is getting better by the day.

Consequently, prominent neurotechnology

scholars believe we should enact laws as quickly as possible to better protect our right to mental freedom, also known as cognitive liberty.<sup>17</sup> They recognize that people have mistaken the contingent biological safeguards protecting our private thoughts for absolute ones. The better we appreciate obscurity, the better prepared we will be to face future surveillance challenges. Conversely, if we had cared more about obscurity in the past, facial recognition technology might not be widely used today.

Second, facial recognition differs considerably from much more easily regulated biometrics, like fingerprinting. Fingerprinting typically requires some form of physical interaction, like touching a scanner or leaving a visible print on objects, even if only a latent one. In contrast, facial recognition can be performed at a distance on vast numbers of people without anyone giving even nominal consent or being aware of the collection. Of course, contactless fingerprint scanning exists. However, it is not the typical approach to acquiring fingerprints, and the process is limited to short distances away. Even as fingerprinting research advances, the fact remains that facial recognition poses a much more immediate threat, which is why it requires the greatest restraints.

### **3. Normalizing Facial Recognition Technology**

One key to understanding how seemingly safe and positive uses of facial recognition are dangerous lies in how society comes to normalize practices. Generally, to say that something is “normal” is to describe it as either commonplace or adhering to an ideal or expected standard. Thus, the process of normalization involves repeating instances of something so frequently that people come to view it as commonplace or become acclimated to the occurrence such that it is no longer noteworthy.

Scholars across disciplines study the concept of normalization (including psychologists, sociologists, cognitive scientists, philosophers, and surveillance scholars) and privacy activists constantly highlight its dangers.<sup>18</sup> Normalizing facial

<sup>16</sup> See, J.W. Penney, *Understanding Chilling Effects*, in *Minnesota Law Review*, vol. 106, 1451, 2022; M. Buchi, N. Festic and M. Latzer, *The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda*, in *Big Data society*, vol. 9, Issue 1, 2022, 14, spec. 4.

<sup>17</sup> N. Farahany, *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology*, 2023.

<sup>18</sup> See Z. Bauman and D. Lyon, *Liquid Surveillance: A Conversation*, Cambridge, UK, Polity Press, 2012; J.B.

recognition systems is dangerous for several reasons. First, when people become acclimated to the privacy encroachments enabled by facial recognition, they become subject to a constant infliction of autonomy harms that fail to meet the harm thresholds demanded by privacy rules or prompt a social outcry. Second, normalization dynamics lead society to constantly re-negotiate its collective sense of reasonable expectations of privacy regarding when they can be identified and how much of their lives are an open book.<sup>19</sup> Our threshold for rejecting invasive new facial surveillance practices is perpetually being redrawn, excusing evermore invasive practices.<sup>20</sup> Without intervention, the normalization of facial recognition systems will result in a slow, inevitable, and irreversible erosion of obscurity and loss of power through exposure.

It's easy to imagine society completely normalizing facial recognition tools. Just look at what we've already gotten used to. We've long stopped noticing many surveillance tools like CCTV as exceptional or out of place.<sup>21</sup>

---

Rule, *Private Lives and Public Surveillance: Social Control in the Computer Age*, Belmont, CA, Wadsworth Publishing, 1974, 22; S.E. Igo, *The Known Citizen: A History of Privacy in Modern America*, Cambridge, MA, Harvard University Press, 2018; O.H. Gandy, Jr., *The Panoptic Sort: A Political Economy of Personal Information*, 2nd ed., Cambridge, MA, MIT Press, 2019, 31; D. Lyon, *Surveillance Studies: An Overview*, Cambridge, UK, Polity Press, 2007, 27; G.T. Marx, *Windows into the Soul: Surveillance and Society in an Age of High Technology*, Chicago, University of Chicago Press, 2016; W.G. Staples, *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*, 2nd ed., Boulder, CO, Paradigm Publishers, 2013, 5; see also: S. Byrne, *The Banality of Surveillance*, in *Surveillance & Society*, vol. 20, 2022, 372; D.M. Wood and K. Ball, *Brandscapes of Control? Surveillance, Marketing and the Co-Construction of Subjectivity and Space in Neoliberal Capitalism*, in *Marketing Theory*, vol. 13, 2013, 47; G. Deleuze, *Postscript on the Societies of Control*, in *October*, vol. 59, 1992, 3.

<sup>19</sup> This is particularly consequential in the United States which conditions many of its privacy rules upon a finding of a "reasonable expectation of privacy." See, W. Hartzog, E. Selinger and J. Gunawan, *Privacy Nicks: How the Law Normalizes Surveillance*, in *Washington University Law Review*, vol. 101, 2024; E. Selinger and J.H. Rhee, *Normalizing Surveillance*, in *North European Journal of Philosophy*, vol. 22, 2021, 49.

<sup>20</sup> W. Hartzog, E. Selinger and J. Gunawan, *Privacy Nicks: How the Law Normalizes Surveillance*, in *Washington University Law Review*, vol. 101, 2024; E. Selinger and J.H. Rhee, *Normalizing Surveillance*, in *North European Journal of Philosophy*, vol. 22, 2021, 49.

<sup>21</sup> R. Santana and R. Gentilo, *TSA Is Testing Facial Recognition at More Airports, Raising Privacy*

Facial recognition is being sold to us as something convenient and desirable, and we're hastening our new normal of exposure with every new sensor we deploy in public, bring into our home, strap on our face, and put in our pocket.<sup>22</sup> Chris Gilliard calls this "luxury surveillance," and it will be our undoing.<sup>23</sup>

When facial recognition goes unchecked, profound societal ramifications can follow. People often develop positive beliefs about these tools that lead them to lose sight of how and why privacy protections provide essential checks against power. Normalizing facial recognition contributes to a "slippery slope dynamic," where society slides further and further into a state of diminishing privacy expectations. Empirical "slippery slope" arguments, the idea that a course of action will eventually snowball into unacceptable outcomes, are often presented as fallacious. Indeed, sometimes they are. The standard objection to empirical slippery slope prognostics is that they fail to identify credible causal mechanisms powerful enough to lead society towards ruinous outcomes without people and institutions changing course in time to avoid catastrophe. The skeptical objection thus suggests if society is ever heading in the wrong direction because of slippery slope factors like path-dependency, emergent governance responses will kick in and prevent tragedy. However, not all slippery slope arguments are fallacious, which is why we argue that slippery slope dynamics have gotten a bad rap. They are merely claims about expected outcomes, which can be prevented if the power of the slippery slope mechanisms can be muted. Thus, to make a valid empirical slippery slope argument, one must specify the causal mechanisms and

---

*Concerns*, in *AP News*, 2023, <https://apnews.com/article/facial-recognition-airport-screening-tsa-d8b6397c02afe16602c8d34409d1451f>; B. Goold *et al.*, *The Curious Case of Surveillance Cameras*, in *British Journal of Criminology*, vol. 53, 2013, 977.

<sup>22</sup> See, e.g., S. Andrade, *Clear Wants to Scan Your Face at Airports. Privacy Experts Are Worried*, in *Washington Post*, 2023, [www.washingtonpost.com/travel/2023/12/20/clear-facial-recognition-technology-airport-security/](http://www.washingtonpost.com/travel/2023/12/20/clear-facial-recognition-technology-airport-security/); J. Winner, *3 Tangible Ways That AI Will Continue to Make Your Life Better*, in *Fast Company*, 2023, [www.fastcompany.com/90892907/3-tangible-ways-that-ai-will-continue-to-make-your-life-better](http://www.fastcompany.com/90892907/3-tangible-ways-that-ai-will-continue-to-make-your-life-better).

<sup>23</sup> C. Gilliard, *Amazon and the Rise of 'Luxury Surveillance'*, in *The Atlantic*, 2022, [www.theatlantic.com/technology/archive/2022/10/amazon-tracking-devices-surveillance-state/671772](http://www.theatlantic.com/technology/archive/2022/10/amazon-tracking-devices-surveillance-state/671772).

explain why their influence is not likely to be dampened adequately in time to prevent disaster.

Scholars have identified two processes by which initially “creepy” deployments of technology become normalized.<sup>24</sup> We think facial recognition systems will follow suit. A process called “unexceptional habituation” occurs when “people in liberal Western democracies take ubiquitously encountered surveillance systems for granted - seeing them as so commonplace and mundane they are not worth thinking about critically.”<sup>25</sup> The more a tool is deployed, the less remarkable it becomes as it fades into the background. For example, most people probably use Apple’s FaceID to unlock their phones without much critical reflection. They also scan their faces to board airplanes and get into concerts. While most people’s first encounter with these facial recognition technologies might have felt novel, each encounter is less remarkable than the last because of people’s growing familiarity with the tool. Ultimately, people will stop critically engaging with these systems because they are part of their habits. Even if uses like FaceID or airport identity verification are themselves relatively innocuous, they habituate people to technologies that are ready-made for more obviously harmful surveillance programs.

Once people come to see facial recognition as exceptional, they will often come to view a practice as acceptable, if not desirable, reflecting a psychological dynamic called “favorably disposed normalization.”<sup>26</sup> The idea is that people often take moral cues from the behavior of others, so observing routine behavior involving facial recognition systems could signal that the technology is good.<sup>27</sup> There is also evidence that people come to rationalize their own use of a technology as desirable to avoid the difficult conclusion they are acting wrongfully.<sup>28</sup> Few like to think of themselves as the bad person, so it’s often just easier to recast our use of dangerous tools as benign so we can continue to see ourselves as

good.<sup>29</sup> Or maybe what happens when we come to view a practice as acceptable is that we look back on our past behavior, such as using Face ID to open our phones, to retroactively attribute those actions to an attitude or motive, such as thinking facial recognition is efficient and helpful.<sup>30</sup>

Another driver normalizing facial recognition is people’s tendency to selectively focus on its benefits and overlook or unduly discount its harms. Consider the example of airport screening, which offers an allegedly fast and convenient way to confirm someone’s identity. In the moment when a person stands in line for screening, the benefit of arriving at the airport gate on time is clear and easy to prioritize. But the deeper harms of facial surveillance - such as having their faceprint potentially stored indefinitely in a government database - are abstract, if not completely invisible.<sup>31</sup> Because of this, even when people are aware that they have the option to avoid facial recognition technology, most do not opt out.<sup>32</sup>

<sup>29</sup> People generally are motivated to see themselves positively, as moral, intelligent, and in control of their lives. To maintain this narrative and minimize inconsistency when making decisions that seem unethical, stupid, or unfree, they often subconsciously turn to rationalization. Put otherwise, being aware of a gap between how we would like to act and how we actually behave can be stressful because it creates cognitive dissonance. Rationalization is ameliorative because it can minimize or dispel cognitive dissonance. Rationalization provides people with a means to convince themselves they should see their situation differently - that seemingly troubling behavior is justifiable, tolerable, and in some cases, even laudable. J.P. Friesen *et al.*, *System Justification: Experimental Evidence, Its Contextual Nature, and Implications for Social Change*, in *British Journal of Social Psychology*, vol. 58, 2019, 315; L. Festinger, *A Theory of Social Comparison Processes*, in *Human Relations*, vol. 7, 1957, 117.

<sup>30</sup> D.J. Bem, *Self-Perception Theory*, in *Advances in Experimental Social Psychology*, vol. 6, 1972, 1.

<sup>31</sup> See, e.g., C. Liu, *The Federal Government Just Can’t Get Enough of Your Face*, in *Electronic Frontier Foundation*, 15 September 2021, [www.eff.org/deeplinks/2021/09/federal-government-just-cant-get-enough-your-face](http://www.eff.org/deeplinks/2021/09/federal-government-just-cant-get-enough-your-face); J.Reid, *TSA Starts Testing Facial Recognition Technology at 16 Major Airports*, Avionics International (29 December 2022), [www.aviationtoday.com/2022/12/29/tsa-starts-testing-facial-recognition-technology-16-major-airports](http://www.aviationtoday.com/2022/12/29/tsa-starts-testing-facial-recognition-technology-16-major-airports).

<sup>32</sup> See, A. Funk, *I Opted Out of Facial Recognition at the Airport—It Wasn’t Easy*, in *Wired*, 2 July 2019, [www.wired.com/story/opt-out-of-facial-recognition-at-the-airport/](http://www.wired.com/story/opt-out-of-facial-recognition-at-the-airport/) (“Federal agencies and airlines claim that facial recognition is an opt-out system, but my recent experience suggests they are incentivizing travelers to have their faces scanned - and disincentivizing them to sidestep the tech - by not clearly communicating

<sup>24</sup> E. Selinger and J.H. Rhee, *Normalizing Surveillance*, in *North European Journal of Philosophy*, vol. 22, 2021, 49.

<sup>25</sup> *Id.*

<sup>26</sup> *Id.*

<sup>27</sup> *Id.*

<sup>28</sup> See, e.g., J.P. Friesen *et al.*, *System Justification: Experimental Evidence, Its Contextual Nature, and Implications for Social Change*, in *British Journal of Social Psychology*, vol. 58, 2019, 315.

As a result, giving people a “choice” regarding facial recognition is another way to normalize it. On the surface, allowing people to decide for themselves whether to use facial recognition seems empowering and autonomy-enhancing. In reality, however, those who are reluctant to undergo face scans don’t have a real choice to opt out of facial recognition technology. Opting out would mean they would have to go through a separate screening procedure that is likely slower and inconvenient.<sup>33</sup> People would view this as a penalty, especially because the vast majority of travelers prefer to go through security as fast as possible.<sup>34</sup> The normalizing effects of strategies designed to give people control over personal information are just another reason to be skeptical of “consent and control” schemes to protect people’s privacy.<sup>35</sup>

To be sure, the legitimacy and presence of these normalizing effects are still open for debate.<sup>36</sup> But they are so intuitively plausible that academics and activists frequently offer normalization warnings like the following ones: if surveillance intensifies at schools, students will be more inclined to accept more intrusive instances of it later in life; and, if during emergencies, new forms of surveillance get introduced, citizens will be more willing to look favorably upon

---

alternative options. Last year, a Delta customer service representative reported that only 2 percent of customers opt out of facial recognition. It’s easy to see why.”)

<sup>33</sup> A. Funk, *I Opted Out of Facial Recognition at the Airport—It Wasn’t Easy*, in *Wired*, 2 July 2019, [www.wired.com/story/opt-out-of-facial-recognition-at-the-airport](http://www.wired.com/story/opt-out-of-facial-recognition-at-the-airport).

<sup>34</sup> This is an instance of ‘domination’ - a form of exercising power through control. In this particular situation, control is exercised by giving people the illusion of freedom, which encourages the continued use of facial recognition technology. As demonstrated here, normalization is in many ways enabled by the processes of domination.

<sup>35</sup> E. Selinger and W. Hartzog, *The Inconsistency of Facial Surveillance*, in *Loyola Law Review*, vol. 66, 2019, 101; D. Solove and W. Hartzog, *Kafka in the Age of AI and the Futility of Privacy as Control*, in *Boston University Law Review*, vol. 104, 2024, especially 1025-1029.

<sup>36</sup> Additional research is needed to better understand the psychology behind normalization in a privacy context. What is also clear, however, is that the law cannot wait for more research before regulating facial recognition technology. In our view, the various ways surveillance can be normalized are enough to show that the absence of regulation will create the conditions for a slippery slope. When left unchecked, the processes of normalization may undermine democracy and our fundamental rights, including autonomy.

comparable, if not more expansive varieties, after the crises end.<sup>37</sup> In other words, the history of surveillance shows that it only runs one way: more.<sup>38</sup> Facial surveillance will be no different. We will get used to it and, as a result, view it as desirable.<sup>39</sup>

Normalizing facial recognition will cost society dearly. We will end up entrenching these systems slowly and incrementally, ensuring that society does not focus enough critical attention to mount meaningful democratically driven resistance. As such, our expectations of privacy will be perpetually eroded until we reach a fully transparent society. People living in that future will be deprived of crucial avenues for human flourishing. Consequently, failing to take facial recognition seriously is fundamentally a problem of intergenerational justice that ensures future generations will have little to no obscurity.

#### 4. How the Law Facilitates Normalizing Facial Recognition

Lawmakers should act quickly and decisively to address the threat that normalizing facial recognition poses to our obscurity. Though industry, lawmakers, advocates, and scholars disagree about the substance and the goals of facial recognition regulation, the common wisdom is that robust new privacy rules should preserve or at least re-establish our solitude and freedom in light of invasive facial recognition practices.<sup>40</sup>

---

<sup>37</sup> E. Selinger and J.H. Rhee, *Normalizing Surveillance*, 49.

<sup>38</sup> See D. Lyon, *Surveillance: A Short Introduction*, 2024.

<sup>39</sup> Research suggests that the more common something is, the more likely people are to see it as desirable. Simply “increasing the frequency of something occurring,” such as surveillance more becoming more prevalent, can lead people to perceive it as “more normal,” not just increasingly widespread. Given the practical value of heightened moral motivation for rectifying injustice, in some circumstances, “beliefs about normality might be more important than moral beliefs.” E. Selinger and J.H. Rhee, *Normalizing Surveillance* at 62. Supporting evidence for this thesis exists in the experimental literature on environmental messaging. N.J. Goldstein *et al.*, *A Room with a Viewpoint: Using Social Norms to Motivate Environmental Conservation in Hotels*, in *Journal of Consumer Research*, vol. 35, 2008, 472; R.B. Cialdini *et al.*, *Managing Social Norms for Persuasive Impact*, in *Social Influence*, vol. 1, 2006, 3.

<sup>40</sup> See H. Rahnama and A. Pentland, *The New Rules of Data Privacy*, in *Harvard Business Review*, 2022, <https://hbr.org/2022/02/the-new-rules-of-data-privacy>. See generally O.S. Kerr, *The Fourth Amendment and*

Scholars sometimes frame proposals for new facial recognition rules and other checks on surveillance in terms of re-establishing or preserving our state of privacy.<sup>41</sup> The idea is to keep change steady without too many wild swings toward exposure or opacity. Unfortunately, under our current surveillance frameworks, equilibrium adjustment for facial recognition is impossible. Even our most robust privacy laws will normalize facial recognition in ways that will leave society worse off due to the erosion of obscurity.<sup>42</sup> Lawmakers concerned about the risks of facial recognition have so far largely failed to see the big picture.<sup>43</sup>

Obscurity, perhaps more than any other conceptualization of privacy, is jeopardized by the normalization of facial recognition technology. It feels mundane because it exists all around us. We are, by default, obscure to the world unless something happens to make us more apparent, like facial recognition tools finding and highlighting an obscure photo of us on the Internet or identifying us while out and about in public. So, it's unsurprising that obscurity is already one of the law's least protected notions of privacy. Society largely takes it for granted. But something worse is actually happening under the radar. Our laws don't just ignore obscurity diminutions that happen incrementally and over time. They *facilitate* the normalization of tools and practices that erode obscurity. Such facilitation occurs through four legal dynamics that were established in technologically simpler times long before facial recognition technology existed. These

dynamics amplify the normalization processes we have discussed, making social and psychological processes like favorably disposed normalization and unexceptional habituation more likely to take hold.

First, U.S. privacy law rigidly demands demonstrable and significant privacy harms to justify legal intervention. Privacy law suffers from a limited vocabulary to differentiate harms based on their magnitude. Under the law, people usually either suffer a privacy violation or they don't. But that's not how people experience privacy incursions, particularly obscurity erosions.<sup>44</sup> Some harms, like those that result in extreme emotional distress, debilitating physical injury, and deprivation of significant life opportunities, clearly are worse than mild annoyances and feelings of "creepiness." But over time, even dispersed and incremental harms take their toll. By ignoring small, *de minimus* encroachments (what we call "privacy nicks"), U.S. lawmakers encourage the normalization of harmful extractive and exploitative practices using surveillance tools like facial recognition.

Privacy nicks are the proverbial "thousand cuts" that lead to death, which explains why even robust privacy protections have failed to halt the expansion of facial surveillance.<sup>45</sup> Privacy nicks are caused by the deployment of new information technologies like facial recognition that generally seem tolerable but can lead to perilous long-term individual and social consequences. They often fail to raise social alarms or trigger legal privacy protections. And they are enabled by the proliferation of facial recognition affordances as part of our cameras and biometric sensors on doorbells, glasses, and watches, as well as the drift of surveillance and data analytics into new areas of our lives like travel, exercise, and social gatherings.

Next, the law over-endows the concept of waiver, particularly in U.S. frameworks. The law typically justifies otherwise objectionable behavior like facial surveillance when people consent to data practices or voluntarily expose themselves to others. This is a dangerous approach for facial recognition because our faces are the most exposed part of our bodies and the most salient physical tie to our

---

*New Technologies: Constitutional Myths and the Case for Caution*, in *Michigan Law Review*, vol. 102, 2004, 801, especially 855-57.

<sup>41</sup> O.S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, in *Harvard Law Review*, vol. 125, 2011, 476, especially 480.

<sup>42</sup> W. Hartzog, E. Selinger and J. Gunawan, *Privacy Nicks: How the Law Normalizes Surveillance*, in *Washington University Law Review*, vol. 101, 2024; E. Selinger and J.H. Rhee, *Normalizing Surveillance*, in *North European Journal of Philosophy*, vol. 22, 2021, 49.

<sup>43</sup> Though there are notable exceptions. See, CNIL, *Facial Recognition: For a Debate Living Up to the Challenges*, [www.cnil.fr/sites/cnil/files/atoms/files/facial-recognition.pdf](http://www.cnil.fr/sites/cnil/files/atoms/files/facial-recognition.pdf) ("Experimentations should not have the ethical purpose or effect of accustoming people to intrusive surveillance techniques, with the more or less explicit aim of preparing the ground for further deployment. At this stage, there should be no question of making devices, which weaken people's autonomy or violate their fundamental rights, "acceptable").

<sup>44</sup> W. Hartzog and E. Selinger, *Surveillance*.

<sup>45</sup> See W. Hartzog, E. Selinger and J. Gunawan, *Privacy Nicks*, 717.

identities. One of the central assumptions behind the notion that people lack a reasonable expectation of privacy when in public is that they have consciously waived privacy protections by choosing to make their presence and activities visible to others. Judges considering privacy tort claims have said for years that there is no privacy in public information or people's whereabouts in public. Their opinions are littered with statements saying people have no legitimate expectation of privacy in the materials intended for publicly accessible websites. When people walk outside with their face exposed or select a photo of their face as their profile photo on a social media account, they likely are counting on a reasonable amount of obscurity in their whereabouts and a relatively transient or limited audience online.<sup>46</sup> Yet, in the U.S., lawmakers and judges routinely justify the scraping of profile photos to power facial surveillance systems, and when the law applies such a waiver rationale to justify surveillance and data processing, it presumes such actions are no longer worthy of additional scrutiny or restrictions within the current context.<sup>47</sup> This conclusion allows facial surveillance to run rampant and become normalized.

Third, privacy law has a misplaced focus on proximity, looking only at localized harms that imminently flow from the actions of others. When lawmakers and judges ask what the harm is from facial recognition, they often look to discrete acts of face scanning and identification to determine if a person suffered physical, financial, emotional, reputational, discrimination, or autonomy harm. This isolated focus on atomistic harms excludes scrutiny of the cumulative effects of discrete actions, thereby abdicating responsibility for addressing the costs of privacy-diminishing externalities. It's hard to hold many different actors responsible for the net result of a slow

accretion of diffuse exposures. Who's to say that one scan of your face by an IoT doorbell is the one that resulted in a chilling effect or loss of autonomy? Privacy's obsession with proximity also includes another pathology: most privacy laws are self-oriented, almost to the point of narcissism. Any aspect of privacy law focused on "individual control over data" or "informational self-determination" is designed to force people to contemplate questions like "what is in it for me?" and "what is the worst that can happen to me or my data?" This egoistic bias ignores how one person's choices affect others. The result is the systemic oppression of marginalized people. In our current system, people of color, members of the LGBT+ community, and other marginalized people fall outside the scope of the majority's self-interested privacy considerations.

Finally, the U.S. rules that ostensibly keep facial recognition systems (and other surveillance practices) in check "too often look to people's expectations to set the limits of surveillance; yet over time, people become increasingly acclimated to being watched. People's desensitization to exposure affects how they view reasonable surveillance measures and fair tradeoffs."<sup>48</sup> Because legal thresholds in the U.S. are keyed to people's expectations, the normalization of privacy nicks results in a constant re-negotiation of privacy standards to our disadvantage. Without a firm backstop, nothing can prevent the gradual tolerance of a maximally transparent culture. It is already happening - slowly but surely.<sup>49</sup> As a result, we are lowering our 'reasonable expectations of privacy.' In sum, privacy law permits whatever people can be conditioned to tolerate. We are on track to tolerate everything.

### 5. What Should Be Done?

What should be done? First, we must recognize that 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. Even legislation that holds out the promise of stringent protective procedures won't prevent chill from impeding crucial

<sup>46</sup> E. Selinger and W. Hartzog, *Obscurity and Privacy*, in J. Pitt and A. Shew (eds.), *Spaces for the Future: Routledge Companion to Philosophy of Technology*, London, Routledge, 2018, [www.routledge.com/Spaces-for-the-Future-A-Companion-to-Philosophy-of-Technology/Pitt-Shew/p/book/9780415842969](http://www.routledge.com/Spaces-for-the-Future-A-Companion-to-Philosophy-of-Technology/Pitt-Shew/p/book/9780415842969); see also W. Hartzog and F. Stutzman, *The Case for Online Obscurity*, in *California Law Review*, vol. 101, 2013, 1, especially 5.

<sup>47</sup> D. Solove and W. Hartzog, *The Great Scrape: The Clash Between Scraping and Privacy*, in *California Law Review*, forthcoming, at [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4884485](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4884485).

<sup>48</sup> W. Hartzog, E. Selinger and J. Gunawan, *Privacy Nicks*, 717.

<sup>49</sup> *Id.*

opportunities for human flourishing by dampening expressive and religious conduct. Even requiring a warrant before facial recognition can be used as part of a government search will 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.

But is there a way to avoid normalizing facial recognition technology and protect obscurity? We think only outright prohibitions on the most dangerous surveillance tool ever will suffice. Nevertheless, recognizing that the most robust prohibitions might require time and political capital, we propose a few half-measures that can be applied to facial recognition but also be adapted more broadly to correct the law's normalization of surveillance. First, instead of focusing on individuals, our facial recognition rules should focus more on the collective good.<sup>50</sup> Privacy law is largely built around protecting individual autonomy and individual rights that individuals can exercise one right at a time. As we explained above, this "proximity" frame fails to consider the impact of surveillance on groups or society. Privacy law misses the forest by focusing only on the trees. This myopia causes lawmakers to miss some of the most harmful aspects of surveillance, including how coercion and discrimination only become apparent at scale. Focusing on the individual effect of surveillance also ignores how one person's actions can affect other people.<sup>51</sup>

As a first step away from individuals toward groups, lawmakers could better recognize threats to collective and social well-being as a privacy harm to satisfy damage and standing requirements.<sup>52</sup> They could also abandon the "reasonable expectation of privacy" test to focus on collective well-being

or unjust uses of power, similar to calls for data collectors to be bound by duties of loyalty to trusting parties.<sup>53</sup> Dislodging individual expectations and individual harm as the center of privacy law would guide lawmakers to systematically examine the danger of privacy nicks.

Next, lawmakers should target the design of facial recognition systems themselves. Most privacy rules target surveillance and data processing behavior but are agnostic about the tools used to observe and collect our personal information. For example, electronic surveillance law prohibits the interception of aural signals or information but ignores how spycams hidden in everyday objects practically encourage surreptitious monitoring. Privacy torts limit the ways in which people can disclose private facts or intrude upon our seclusion, but they ignore how facial recognition tools make these actions so easy. It's a mistake for lawmakers to ignore the design of facial recognition technologies. Design is everywhere, design is power, and design is political.<sup>54</sup> When lawmakers ignore the design of information technologies, as they traditionally have in the U.S., they allow companies to escape accountability for malicious and negligent design decisions that encourage privacy harms and an overall degradation of obscurity.

Lawmakers and judges could prohibit combining facial recognition with existing surveillance systems designed for particular uses (like CCTV) or target "dark patterns," which are interface elements and designs that trick users into unwanted or unintentional exposures to facial recognition systems against their best interests.<sup>55</sup> The U.S. Federal

<sup>50</sup> See, e.g., L. Taylor et al. (eds.), *Group Privacy: New Challenges of Data Technologies*, 2017; D. Solove and W. Hartzog, *Kafka in the Age of AI and the Futility of Privacy as Control*, in *Boston University Law Review*, vol. 104, 2024, especially 1025-1029.

<sup>51</sup> S. Viljoen, *A Relational Theory of Data Governance*, in *Yale Law Journal*, vol. 131, 2021, 573.

<sup>52</sup> See, e.g., J.A.T. Fairfield and C. Engel, *Privacy As A Public Good*, in *Duke Law Journal*, vol. 65, 2015, 387; D.K. Citron and D.J. Solove, *Privacy Harms*, in *Boston University Law Review*, vol. 102, 2022, 793, especially 831.

<sup>53</sup> See, e.g., W. Hartzog and N. Richards, *The Surprising Virtues of Data Loyalty*, in *Emory Law Journal*, vol. 71, 2022, 985, especially 1012; W. Hartzog and N. Richards, *Legislating Data Loyalty*, in *Notre Dame Law Review Reflection*, vol. 97, 2022, 356; N. Richards and W. Hartzog, *A Duty of Loyalty for Privacy Law*, in *Washington University Law Review*, vol. 99, 2021, 961.

<sup>54</sup> W. Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, Cambridge, MA, Harvard University Press, 2018, 279.

<sup>55</sup> See, e.g., G. Gunawan et al., *Understanding Dark Patterns in Home IoT Devices*, in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 2023 (forthcoming); R. Calo, *Digital Market Manipulation*, in *George Washington Law Review*, vol. 82, 2014, 995; G. Conti and E. Sobiesk, *Malicious Interface Design: Exploiting the User*, in *Proceedings of the WWW Conference*, 2010; L. Di Geronimo et al., *UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception*, in

Trade Commission has filed complaints against companies for “unfair default settings,” design choices that unfairly risk the security of personal data, and design choices that unfairly interfere with a technological privacy safeguard.<sup>56</sup>

Another way lawmakers might target the design of facial recognition systems is to expand theories of secondary liability to account for dangerous design choices. The FTC has developed a “means and instrumentalities” theory of wrongdoing for unfairly designing tools to encourage consumer harm. Product liability law has long developed theories of wrongdoing around design and warning defects. Given the widespread fraud and harassment enabled by mass facial recognition, these theories should be leveraged in combination with lawmakers’ and judges’ recognition of collective and social harms. All of these approaches - specific design rules, consumer protection doctrines, and expanded notions of secondary and product liability, can be leveraged to check the starting point for virtually any facial recognition system.

Finally, lawmakers should get serious about outright prohibitions and bans on facial recognition. Privacy law’s favorite tool is procedure.<sup>57</sup> Surveillance laws justify

observation through warrants and subpoenas. Data privacy laws justify information processing through consent or upon proof of certain contracts or business interests. People are given privacy when they have “control” over personal information and rights of transparency, access, and deletion.<sup>58</sup> Both due process and the Fair Information Practices, the bedrock principles of surveillance and data protection law, are built upon the idea that if you follow the right procedures, surveillance and data processing are justified.<sup>59</sup> The problem with procedural frameworks is that they end up justifying the practices they seek to mitigate.<sup>60</sup> This is a recipe for normalizing facial recognition because if the procedure is followed, the technology is used in a way that, over time, becomes unexceptional and entrenched.

Instead, lawmakers should outright substantively prohibit the dangerous activities that no amount of procedure can justify. Lawmakers might join cities like Portland, San Francisco, Oakland, Somerville, and others that have banned facial and biometric surveillance by law enforcement or in places of public accommodation.<sup>61</sup> The European Union’s AI Act, which prohibits facial surveillance and emotion recognition as part of a broad ban on unacceptably risky AI systems is the most prominent and substantive example of this approach.<sup>62</sup> Though even this

*Proceedings of the CHI Conference on Human Factors in Computing Systems*, 2020; C.M. Gray et al., *End User Accounts of Dark Patterns as Felt Manipulation*, in *Proceedings of the ACM on Human-Computer Interaction*, vol. 5, n. 372, 2021, 1, especially 5; J. King and A. Stephan, *Regulating Privacy Dark Patterns in Practice—Drawing Inspiration from the California Privacy Rights Act*, in *Georgetown Law Technology Review*, vol. 5, 2021, 251; J. Luguri and L. Strahilevitz, *Shining a Light on Dark Patterns*, in *Journal of Legal Analysis*, vol. 13, 2021, 43.

<sup>56</sup> See, e.g., *Complaint, Zoom Video Communications, Inc.*, FTC Matter/File Number 192 3167, 9 November 2020; see also D. Solove and W. Hartzog, *The FTC Zoom Case: Does the FTC Need a New Approach?*, in *LinkedIn*, 2020, [www.linkedin.com/pulse/ftc-zoom-case-does-need-new-approach-daniel-solove](http://www.linkedin.com/pulse/ftc-zoom-case-does-need-new-approach-daniel-solove); R. Hutchinson, *FTC says IntelliVision’s claims about facial recognition software were deceptive* | Opinion, Commercial Appeal (8 April 2025), [www.commercialappeal.com/story/opinion/contributors/2025/04/08/better-business-bureau-ftc-facial-recognition/82983225007](http://www.commercialappeal.com/story/opinion/contributors/2025/04/08/better-business-bureau-ftc-facial-recognition/82983225007).

<sup>57</sup> See, e.g., J.E. Cohen, *How (Not) to Write a Privacy Law*, in *Knight First Amendment Institute*, 2, 2021, 8, <https://knightcolumbia.org/content/how-not-to-write-a-privacy-law/>; A.E. Waldman, *Privacy, Practice, and Performance*, in *California Law Review*, vol. 110, 2022, 1221. The FTC also filed a complaint against Rite Aid for “Unfair Facial Recognition Practices,” which involved using “facial recognition technology in their retail stores without taking reasonable steps to address

the risks that their deployment of such technology was likely to result in harm to consumers as a result of false-positive facial recognition match alerts.” *Complaint, FTC v. Rite Aid Corp.*, Case No. 2:23-cv-5023, 19 December 2023.

<sup>58</sup> D. Solove and W. Hartzog, *Kafka in the Age of AI and the Futility of Privacy as Control*, in *Boston University Law Review*, vol. 104, 2024, especially 1025-1029; A.E. Waldman, *The New Privacy Law*, in *UC Davis Law Review Online*, vol. 55, 2021, 39-40.

<sup>59</sup> J. Rule et al., *The Politics of Privacy*, Belmont, CA, Wadsworth Publishing, 1980, 93.

<sup>60</sup> See also J.E. Cohen, *How (Not) to Write a Privacy Law*, in *Knight First Amendment Institute*, 2, 2021, 8, <https://knightcolumbia.org/content/how-not-to-write-a-privacy-law>.

<sup>61</sup> See, e.g., R. Metz, *Portland Passes Broadest Facial Recognition Ban in the U.S.*, in *CNN*, 2020, [www.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html](http://www.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html); S. Flynn, *13 Cities Where Police Are Banned from Using Facial Recognition Tech*, in *Innovation & Tech Today*, 2023, <https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech> (last visited 2 March 2023).

<sup>62</sup> European Union AI Act, Chapter II, Article 5: “The following AI practices shall be prohibited:...e) ...the use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage; (f) ...the use

supposed high-water mark for substantive bans on facial recognition has been criticized as not enough or even a form of privacy theater that functionally authorizes facial recognition in the most important contexts in spite of ostensibly prohibiting it.<sup>63</sup> The AI Act still permits the use of facial recognition for limited purposes by governments. While these purposes are laudable, such as finding missing persons, they are a foot in the door. Lawmakers must make fewer compromises if they are to protect against normalizing facial recognition and protect obscurity. Bright-line prohibitions on facial recognition provide a substantive backstop to prevent surveillance creep. In other words, they protect people by restricting dangerous behavior now

matter how acclimated people become to being watched through privacy nicks.

We believe society can't wait years for lawmakers and judges to get the balance just right when regulating facial recognition to maximize its benefits while minimizing its harms. By then, facial recognition infrastructure will be ubiquitous, and exploiting its full potential will seem like a good use of resources. And the accompanying surveillance creep such a balance would bring is inevitable. The law singles out specific technologies all the time because they are so

---

of AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons; (g) ...the use of biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; this prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement; (h) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the following objectives: (i) ...the search for missing persons; (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons...; (iii) the localisation or identification of a person suspected of having committed a criminal offence....").

<sup>63</sup> Shubam, *EU AI Act Will Fail Commitment to Ban Biometric Mass Surveillance*, in *Reclaim Your Face 2024*, <https://reclaimyourface.eu/eu-ai-act-will-fail-commitment-to-ban-biometric-mass-surveillance>; Access Now, *The EU AI Act: A Failure for Human Rights, a Victory for Industry and Law Enforcement*, in *Access Now*, 2024, [www.accessnow.org/press-release/ai-act-failure-for-human-rights-victory-for-industry-and-law-enforcement/](http://www.accessnow.org/press-release/ai-act-failure-for-human-rights-victory-for-industry-and-law-enforcement/).

exceptional. Automobiles, spyware, medical devices, and a host of other technologies have their own specific rules. Airplanes and telecommunications technologies were given their own federal regulatory agencies. Facial recognition is similarly worthy of exceptional treatment.

While outright prohibitions are more politically fraught and practically inflexible, they are the most significant tools available to resist the normalization of surveillance. It might sound extreme to call for an outright ban on the most dangerous surveillance practices, even when they might have some utility, but we think it is necessary.<sup>64</sup> Even if advocates of informed consent and warrant requirements for government searches got everything on their wish list, society would still end up worse off with facial recognition. 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 sufficiently stop the harms of face surveillance. It must be banned outright.<sup>65</sup> Compromises that fall back on procedure and "individual control" will end up compromising the entire endeavor.

## 6. Conclusion

Facial recognition is truly a one-of-a-kind technology - and we should treat it as such. Our faces are central to our identities, online and off, and they are difficult to hide. People look to our faces for insight into our innermost feelings and dispositions. Our faces are also easier to capture than biometrics like fingerprints and DNA, which require physical contact or samples. And facial recognition technology is easy to use and accessible, ready to plug into police body cameras and other systems.

---

<sup>64</sup> See, e.g., E. Selinger and W. Hartzog, *The Inconsistency of Facial Surveillance*, 122 ("[I]f 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").

<sup>65</sup> *Id.*

The stakes are high. Over time, the slippery slope of normalizing facial recognition stands to change fundamental social beliefs about and dispositions toward privacy. The endpoint of the slope is the wide-scale degradation of obscenity protections necessary for pursuing the good life and maintaining the full potential of a liberal democracy. One of the most problematic aspects of society becoming acclimated to privacy nicks is that we become unable to fully appreciate how our autonomy, and thus dignity, are being routinely violated. We are being programmed not to worry about forms of face surveillance that once struck many of us as creepy, ambiguous threats. Over time, these privacy diminutions, once seen as worrisome, fail to trigger even basic concern. Lawmakers must not allow society to grow ever more alienated from appreciating the goods privacy offers without engaging in the oversight required to protect our invaluable obscenity.