2024

Privacy Nicks: How the Law Normalizes Surveillance

Woodrow Hartzog
Boston University School of Law

Evan Selinger
Rochester Institute of Technology - Department of Philosophy

Johanna Gunawan

PRIVACY NICKS: HOW THE LAW NORMALIZES SURVEILLANCE

Woodrow Hartzog,[*] *Evan Selinger*[**] *and Johanna Gunawan*[***]

Privacy law is failing to protect individuals from being watched and exposed, despite stronger surveillance and data protection rules. The problem is that our rules look to social norms to set thresholds for privacy violations, but people can get used to being observed. In this article, we argue that by ignoring de minimis privacy encroachments, the law is complicit in normalizing surveillance. Privacy law helps acclimate people to being watched by ignoring smaller, more frequent, and more mundane privacy diminutions. We call these reductions "privacy nicks," like the proverbial "thousand cuts" that lead to death.

Privacy nicks come from the proliferation of cameras and biometric sensors on doorbells, glasses, and watches, and the drift of surveillance and data analytics into new areas of our lives like travel, exercise, and social gatherings. Under our theory of privacy nicks as the Achilles heel of surveillance law, invasive practices become routine through repeated exposures that acclimate us to being vulnerable and watched in increasingly intimate ways. With acclimation comes resignation, and this shift in attitude biases how citizens and lawmakers view reasonable measures and fair tradeoffs.

Because the law looks to norms and people's expectations to set thresholds for what counts as a privacy violation, the normalization of these nicks results in a constant re-negotiation of privacy standards to society's disadvantage. When this happens, the legal and social threshold for rejecting invasive new practices keeps getting redrawn, excusing ever more aggressive intrusions. In effect, the test of what privacy law allows is whatever people will tolerate. There is no rule to stop us from tolerating everything. This article provides a new theory and terminology to understand where privacy law falls short and suggests a way to escape the current surveillance spiral.

---

[*] Professor of Law, Boston University.

[**] Professor of Philosophy, Rochester Institute of Technology.

[***] Ph.D. Student, Khoury College of Computer Sciences, Northeastern University.

The authors would like to thank Mike Hintze, Neil Richards, Paul Schwartz, Jessica Silbey, and the participants of the 2022 Privacy Law Scholars Conference and the participants of the Yale Information Society Project's Law & Technology speaker series. The authors would also like to thank Kabbas Azhar, Enyonam Edoh, Giuliana Green, and Janelle Robins for their excellent research assistance and Microsoft for its support for this research. This research was also supported in part by NSF SATC Frontier Award 195639/1955227.+

Table of Contents

INTRODUCTION

On paper, privacy law has never been stronger. The European Union ignited a data protection revolution with the General Data Protection Regulation. The U.S. Federal Trade Commission developed a framework for protecting consumer privacy that is more ambitious and holistic than ever before. California kicked off a nationwide competition for the title of the state with the strongest privacy rules. The U.S. Supreme Court is adapting to people's vulnerabilities in a digitally connected world.

In practice, however, these legal advancements are doing little to stop or even slow the growth of surveillance technologies. The trajectory of surveillance has never deviated from increased exposure. Today, more sensors are used to watch more people for more purposes and longer

durations than ever before. This Article argues that this trend is going to continue, even as privacy laws become more robust than ever. That's because privacy law looks 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. It would be bad enough if lawmakers and judges merely ignored how people become conditioned to surveillance. Tragically, their laws and opinions *encourage* it.

In this Article, we argue that U.S. privacy and surveillance law has failed us because it ignores de minimis privacy encroachments. We introduce a new theory of privacy nicks as an allusion to the proverbial "thousand cuts" that lead to death, which explains why even robust privacy protections have failed to halt the expansion of surveillance. The theory of privacy nicks posits that lawmakers are systematically normalizing surveillance by ignoring smaller, more frequent, and more mundane privacy diminutions. Instead, lawmakers tend to target only larger and more serious privacy invasions—what we call "privacy chops" as an allusion to the swift and sharp swipe of a blade. Privacy nicks are enabled by the proliferation of 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.

The result of unchecked privacy nicks is a society that is gradually conditioned to being watched.[1] Cameras, once resisted as a tool for snoops, are now in everyone's pockets. CCTV, once thought to be the "death of privacy," can be seen on any random street corner, building, or classroom.

---

[1] *See* ZYGMUNT BAUMAN & DAVID LYON, LIQUID SURVEILLANCE: A CONVERSATION (2012); JAMES B. RULE, PRIVATE LIVES AND PUBLIC SURVEILLANCE: SOCIAL CONTROL IN THE COMPUTER AGE 22 (1974); SARAH E. IGO, THE KNOWN CITIZEN: A HISTORY OF PRIVACY IN MODERN AMERICA (2018); OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION 31 (2nd ed. 2019); DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW 27 (2007); GARY T. MARX, WINDOWS INTO THE SOUL; SURVEILLANCE AND SOCIETY IN AN AGE OF HIGH TECHNOLOGY (2016); WILLIAM G. STAPLES, EVERYDAY SURVEILLANCE: VIGILANCE AND VISIBILITY IN POSTMODERN LIFE 5 (2nd ed. 2013); *see also* Sarah Byrne, *The Banality of Surveillance,* 20 SURVEILLANCE & SOC'Y 372, 372 (2022); David Murakami Wood & Kristie Ball, *Brandscapes of Control? Surveillance, Marketing and the Co-Construction of Subjectivity and Space in Neoliberal Capitalism*, 13 MRKTG. THEORY 47 (2013); Gilles Deleuze, *Postscript on the Societies of Control*, 59 OCTOBER 3 (1992).

Once upon a time on the Internet, "nobody knew you were a dog."[2] Now targeted advertising and social media ensure that we are all identified and accounted for. And facial recognition technology, once the stuff of dystopian science fiction, is now used to unlock our phones, board our flights, pay for our groceries, and deem us worthy of employment.[3]

The common wisdom is that robust new privacy rules preserve or at least re-establish our solitude and freedom in light of invasive surveillance and data collection practices.[4] Professor Orin Kerr calls this an "equilibrium adjustment" in response to changing technologies and social practices.[5] According to Kerr, "[w]hen new tools and new practices threaten to expand or contract police power in a significant way, courts adjust the level of Fourth Amendment protection to try to restore the prior equilibrium."[6] Lawmakers, scholars, and journalists also frame reform of corporate surveillance practices in terms of re-establishing or preserving our state of privacy.[7] Unfortunately, under our current surveillance frameworks, equilibrium adjustment is impossible. Even our most robust privacy laws increase our exposure to being watched by governments and corporations.

We introduce the theory of privacy nicks and chops to explain the shortcomings of surveillance law and add precision to an issue that many people intuitively recognize but have lacked the language to precisely articulate. Privacy law suffers from a limited vocabulary to differentiate

---

[2] Michael Cavna, *'NOBODY KNOWS YOU'RE A DOG': As Iconic Internet Cartoon Turns 20, Creator Peter Steiner Knows the Joke Rings as Relevant as Ever*, WASH. POST (July 31, 2013), https://www.washingtonpost.com/blogs/comic-riffs/post/nobody-knows-youre-a-dog-as-iconic-internet-cartoon-turns-20-creator-peter-steiner-knows-the-joke-rings-as-relevant-as-ever/2013/07/31/73372600-f98d-11e2-8e84-c56731a202fb_blog.html.

[3] *See* Evan Selinger & Woodrow Hartzog, *What Happens When Employers Can Read Your Facial Expressions?*, N.Y. TIMES (Oct. 17, 2019), https://www.nytimes.com/2019/10/17/opinion/facial-recognition-ban.html.

[4] *See* Hossein Rahnama & Alex Pentland, *The New Rules of Data Privacy*, HARV. BUS. REV. (Feb. 25, 2022), https://hbr.org/2022/02/the-new-rules-of-data-privacy. *See generally* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 855–57 (2004).

[5] Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011).

[6] *Id.* at 480.

[7] *See, e.g.*, ROBERT H. SLOAN & RICHARD WARNER, THE PRIVACY FIX: HOW TO PRESERVE PRIVACY IN THE ONSLAUGHT OF SURVEILLANCE (2021).

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. 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."

In most cases, the only important question for lawmakers, regulators, and judges seems to be whether the harm threshold is met. While the harm from the release of intimate photos or sensitive health information might be convincing or self-evident enough to trigger legal action, finding a surveillance technology "creepy" will not cut it; neither will activity that increases the likelihood of future privacy problems. Without the ability to speak in a more nuanced way about how people's actions can make us and our data vulnerable, our framework of protection remains myopic, incomplete, and dangerous.

When lawmakers allow privacy nicks to become routine, repeated exposures can acclimate people to being vulnerable and watched in increasingly intimate ways. With acclimation comes resignation, and this shift in attitude biases how citizens and lawmakers view reasonable measures and fair tradeoffs. Smaller nicks continue to expand even when governments prohibit significant invasions into people's lives by targeting privacy "chops." Because the law looks to norms and people's expectations to set thresholds for what counts as a privacy violation, the normalization of these 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. We are lowering our 'reasonable expectations of privacy' as a result. In sum, privacy law permits whatever people can be conditioned to tolerate. We are on track to tolerate everything.

This Article proceeds in four parts. In Part One, we draw from privacy scholarship, surveillance studies, design theory, and psychology to introduce the theory of privacy nicks as the Achilles' heel of privacy law. We conceptualize privacy nicks as *deployments of technology that increase the extent to which human information is used or known but present a reasonably low or negligible risk of immediate harm*. Privacy nicks are

caused by the deployment of new information technologies that generally seem tolerable but can lead to perilous long-term individual and social consequences.

To better understand how to spot privacy nicks, we compare them to larger and more significant privacy "chops." We conceptualize chops as *actions or deployments of technology that increase the extent to which human information is known or used enough to present a significant, immediate, and unreasonable risk of privacy harm*. Chops happen quickly and are felt strongly and locally. In contrast, privacy nicks have a less noticeable or obvious impact. As a result, privacy nicks often fail to raise social alarms or trigger legal privacy protections. In this part we explore the role that transaction costs—the expenditure of resources like time, money, and labor that are necessary for undertaking an action—play in protecting our privacy and how they facilitate privacy nicks and chops. We also explore how nicks fuel privacy's slippery slope. While slippery slopes are often fallacious, we argue that the gradual diminution of privacy through nicks is a valid concern and lawmakers should take it seriously.

In Part Two, we identify three dynamics that cause the law to ignore nicks and, in doing so, normalize surveillance creep and privacy-invasive data processing. Specifically, we argue that privacy law makes three different missteps. First, the law's intense focus on *harm* causes it to overlook privacy nicks that are minimally disruptive to an individual or society at a given moment in time. Next, the law over-endows the concept of *waiver*. The law typically justifies otherwise objectionable behavior when people consent to data practices or voluntarily expose themselves to others. The law is particularly quick to recognize people's waivers in the context of privacy nicks. Third, privacy law has a misplaced focus on *proximity*, looking only at localized harms that imminently flow from the actions of others. 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. Privacy's obsession with proximity also includes another pathology: most privacy laws are self-oriented, almost to the point of narcissism. Almost every aspect of privacy law 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 wrongfully vulnerable people fall outside the scope of the majority's self-interested privacy considerations.

In Part Three, we identify fundamental problems that flow from the slow and steady accumulation of privacy nicks. First, lawmakers and judges create space for the constant infliction of autonomy harms that fail to meet the harm thresholds demanded by privacy rules. Second, normalization dynamics under current legal conditions allow society to constantly renegotiate its collective sense of reasonable expectations of privacy. The threshold for rejecting invasive new practices is perpetually being redrawn, excusing evermore invasive practices.

In Part Four, we propose how to keep the law from normalizing dangerous surveillance practices through privacy nicks. First, we explore what options are likely to be ineffective against privacy nicks, including looking to norms and subjective expectations, and "future-proofing" the law. We then propose that lawmakers embrace more relational and collective approaches, a focus on the design of information technologies, and substantive prohibitions on tools and practices. We conclude that unless the law confronts privacy nicks, a slow and irreversible loss of privacy through exposure is inevitable.

I. A PRIVACY NICKS THEORY OF NORMALIZING SURVEILLANCE

This part develops a theory of privacy nicks to explain how the law normalizes dangerous surveillance. Privacy nicks operate in the law's blind spots, which allows them to proliferate outside the purview of what lawmakers and judges consider a true privacy problem. If nicks are left unchecked, they will acclimate people to practices that were once unthinkable. This dynamic is the essence of normalization. For example, people once considered security cameras wildly invasive. Now they are unremarkable. Although society is currently pushing back against license plate readers, this technology remains on pace to follow a similar trajectory of widespread deployment.

Surveillance studies scholars have long observed how surveillance becomes normalized in society. Gary Marx identified four aspects of social processes in surveillance: "the *softening of surveillance*, meaning it

becomes less visible and directly coercive, often being engineered into an activity: *patters of expansion and contradiction*, such as the tendency of a given means to quietly expand to new users and goals beyond those initially envisioned; *changes in surveillance* as social relationships change; and *stages of behavior* in the application of a tactic."[8] James Rule explored the increasing use of computer databases by government agencies and corporations as central tools of governance and customer management, creating a slow and creeping threat of a "total surveillance society."[9] Oscar Gandy has noted how mass surveillance has been normalized in a system of identification, classification, and assessment, what Gandy calls the "panoptic sort": people's identity require constant authentication as they are classified into various social categories and assessed against one another to "establish norms and the bounds of reasonableness and acceptability."[10] William Staples calls the normalization of surveillance in everyday life "meticulous rituals of power," where we have entered "a state of permanent visibility where attempts to control and shape our behavior…are accomplished not so much by the threat of punishment and physical force but by the act of being watched—continuously, anonymously, and automatically."[11]

The expansion of information technologies has created what Marx calls a "new surveillance" that is "invisible…involuntary…[and] often integrated into routine activity."[12] Scholars have observed how surveillance becomes has a tendency to transform from "direct political surveillance" to a seemingly "benign…governance or administration" that justifies more and more information collection.[13] A "surveillance society" gets

---

[8] MARX, *supra* note 1, at 114.

[9] RULE, *supra* note 1, at 22.

[10] GANDY, *supra* note 1, at 31; *see also* Deleuze, *supra* note 1, at 3 (outlining that the twentieth century has led to a new regime of "societies of control" through systematic surveillance of 'dividuals').

[11] STAPLES, *supra* note 1, at 5 (arguing that contemporary life is increasingly technologically mediated by "meticulous rituals of power" that lead to more universal exposure to surveillance).

[12] Gary T. Marx, "*What's New About the New Surveillance?": Classifying for Change and Society*, 1 SURVEILLANCE & SOC'Y 9, 15 (2002) (arguing that society has entered a system of "new surveillance" that extends the senses and has blurred the lines between the self and surveillance).

[13] *Id.* at 18.

rationalized, often during moments of crises, in what Lyons calls "obsessive risk aversion and media-amplified public panic."[14]

Surveillance is incorporated and normalized in art[15], medicine[16], borders[17], work[18], our consumption[19], our daily social lives[20] and the home itself.[21] Thus, surveillance becomes as Sarah Byrne notes, "[M]undane. Quotidian. Banal…[and] more often than not, ordinary work done by ordinary people…"[22]

Under our theory, smaller nicks that expose people and extract information continue to expand even when governments prohibit significant invasions into people's lives—what we call privacy "chops." People intuitively understand peeping, spying, and the betrayal of

---

[14] LYON, *supra* note 1, at 27 (arguing that contemporary societies are "surveillance societies" where daily life is "suffused with surveillance" and "what once was experienced only in specific contexts…has spilled over in every dimension of daily life.").

[15] Andrea Mubi Brighenti, *Artveillance: At the Crossroads of Art and Surveillance*, 7 SURVEILLANCE & SOC'Y 137, 137 (2010) ("[S]urveillance does not simply produce substantive social control and social triage, it also contributes to the formation of an ideoscape and a collective imagery about what security, insecurity, and control are ultimately about…").

[16] David Armstrong, *The Rise of Surveillance Medicine,* 17 SOCIO. OF HEALTH & ILLNESS 393 (1995) (arguing that contemporary "surveillance medicine" depends on normalizing monitoring entire populations rather than just sick ones, shifting from the three-dimensional body to the four-dimensional space of the time-community).

[17] Louis Amoore, *Biometric Borders: Governing Mobilities in the War on Terror*, 25 POL. GEO. 336, 338 (2006) (arguing that biometric monitoring at the border is "categorically not about new border threats in a post 9/11 world, but rather a means of identifying and designating the safe from the dangerous at multiple borders of daily life").

[18] Graham Sewell & Barry Wilkinson, *Someone to Watch Over Me: Surveillance, Discipline, and the Just-in-Time Labour Process,* 26 SOCIO. 271 (1992) (arguing that Just-in-Time & Total Quality Control techniques make workers "internalize discipline" as they are surveilled constantly all the while being constantly aware that they are watched).

[19] Wood & Ball, *supra* note 1, at 47 (discussing how data subjects come to consider "the provision of data as a normal part of consumption practice, through loyalty schemes, social networking sites, location-based technology use and search engines to perform work in their own surveillance").

[20] Mark Andrejevc, *The Work of Being Watched: Interactive Media and the Exploitation of Self-Disclosure*, 19 CRITICAL STUD. MEDIA COMMC'N 230 (2002) (arguing that digital environments have become "digital enclosures" where consumers are used to their media participation being captured and commodified by private companies).

[21] Cindi Katz, *The State Goes Home: Local Hypervigilance of Children and the Global Retreat from Social Reproduction*, 28 SOC. JUST. 47 (2001) (arguing that nanny cams, and other electronic surveillance technologies inside the home are increasingly used as a measure to surveil children as parents feel guilty about their absentee parenting—all the while ignoring the lack of state support for safe and nurturing homes).

[22] Byrne, *supra* note 1, at 372.

intimacies as a chop because their impact is typically felt acutely and immediately upon revelation. Privacy nicks, however, are not quite as disruptive.

To frame our theory of privacy nicks, we focus on technological *deployments*. Rather than viewing technologies as static, potentially monolithic 'electronic or digital products and systems considered as a group,'[23] we mean 'deployment' as the act of arranging, using, or organizing something towards a specific purpose.[24] This definition is compatible with how software engineering uses the term, construing 'deployment' as the act of delivering a product either as a complete entity or partially completed increment, making it available for use.[25]

To define the term 'privacy,' we adopt Neil Richard's definition of the term, meaning "the degree to which human information is neither known nor used."[26] In this Article, we refer to technological deployments that change the degree to which human information is neither known or used as privacy encroachments. Harm is not implied within Richards' definition. Some privacy encroachments may result in harms, while others do not. For example, we constantly disclose private information to trusted sources, like our friends and family, often without getting harmed. People often share cursory details about their friends to new acquaintances with little adverse result. With this framing in the background, we turn to privacy nicks—a form of privacy encroachment that is rarely resisted.

We define privacy nicks as *deployments of technology that increase the extent to which human information is used or known but present a reasonably low or negligible risk of immediate harm*.[27] When people discuss privacy colloquially, they often intuitively recognize privacy nicks, usually describing them with terms like "creepy" or "troubling"—not

[23] From the third definition under the American Heritage Dictionary of the English Language, 5th Edition.

[24] From the Merriam-Webster definitions of 'deploy' and 'deployment,' as well as from the Encyclopedia Britannica definition of 'deployment.'

[25] ROGER S. PRESSMAN & BRUCE R. MAXIM, SOFTWARE ENGINEERING: A PRACTITIONER'S APPROACH (8th ed. 2014). This conceptualization of deployment designates a noun (the product, or something created) that is associated with an action (the use of the created item).

[26] NEIL RICHARDS, WHY PRIVACY MATTERS 22 (2021).

[27] We also conceptualize privacy harm as the full scope of potential harms. *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022); Ignacio Cofone & Adriana Robertson, *Privacy Harms*, 69 Hastings L. J. (2018).

copasetic, but not beyond the pale either.[28] For example, encountering seemingly prescient targeted advertising or eyeglasses with a camera embedded in them might cause people to bristle. Still, few would say such practices and tools should be outright prohibited and rejected by society.

Nicks often are triggered by new technologies that generally seem tolerable but can lead to perilous long-term individual and social consequences. For example, using facial recognition to identify shoppers in an Amazon grocery store might only modestly expose people to greater risk. But if we lived in a society that is thoroughly and constantly monitored by facial recognition in every building we enter, life would feel oppressive, and the technology would lead to abuse.

To make privacy nicks easier to identify and understand, we suggest comparing them larger and more significant privacy encroachments, which we call "chops." We conceptualize chops as *deployments of technology that increase the extent to which human information is known or used enough to present a significant, immediate, and unreasonable risk of privacy harm*. For example, when people use facial recognition apps like PimEyes to stalk and harass others, they are committing a privacy chop.[29] Chops happen quickly, make surveillance and information processing much easier to conduct, significantly empower watchers, and have a large societal footprint. In contrast, privacy nicks have some but not all the elements of privacy chops. As we'll cover in Part II, the distinction between privacy nicks and chops is important because while the law has a mixed record responding to privacy chops, it almost completely ignores privacy nicks.

---

[28] *See* Evan Selinger, *Why Do We Love To Call New Technologies "Creepy"?*, SLATE, (Aug. 22, 2012, 3:30 AM), https://slate.com/technology/2012/08/facial-recognition-software-targeted-advertising-we-love-to-call-new-technologies-creepy.html; Neil Richards, *"Creepiness" Is the Wrong Way to Think About Privacy*, Slate, (Dec. 2, 2021, 8:00 AM), https://slate.com/technology/2021/12/why-privacy-matters-excerpt-creepiness.html; RICHARDS, *supra* note 26; Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016) (discussing the creepiness trap).

[29] *See* Drew Harwell, This Facial Recognition Website Can Turn Anyone Into a Cop — or a Stalker, WASH. POST (May 14, 2021, 7:00 AM), https://www.washingtonpost.com/technology/2021/05/14/pimeyes-facial-recognition-search-secrecy/.

A. Obscurity and the Transaction Costs of Surveillance

To understand why some privacy invasions should be seen as chops and others as nicks, it is essential to understand the role that transaction costs—the expenditure of resources like time, money, and labor that are necessary for undertaking an action—play in protecting our privacy. Scholars have highlighted a particular kind of privacy called *obscurity* that focuses on the protection stemming from privacy-invasive activity being difficult and unlikely.[30] To appreciate the ability to protest in a crowd without being put on a law enforcement watch list, move on from the missteps of your youth without being weighed down by a permanent record, build and reinforce social ties by discretely gossiping about others, and run daily errands without others monitoring all of your behavior, you appreciate the benefits of obscurity. Simply put, the foundation of obscurity theory is the premise that when the costs of finding or understanding information are high, people are less likely to engage in that behavior.

Knowing that effort is a deterrent, people instinctually build their risk calculus around the transaction costs for engaging in privacy-invasive behavior.[31] For example, there are longstanding social norms about using hushed tones when speaking in public to prevent others from

[30] Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1345–46 (2015) [hereinafter Hartzog & Selinger, *Surveillance*] ("[W]e argue that the concept of "obscurity," which deals with the transaction costs involved in finding or understanding information, is the key to understanding and uniting modern debates about government surveillance."); Woodrow Hartzog & Evan Selinger, *Increasing the Transaction Costs of Harassment*, 95 B.U. L. REV. ANNEX 47 (2015); Evan Selinger & Woodrow Hartzog, *Obscurity and Privacy*, *in* SPACES FOR THE FUTURE: ROUTLEDGE COMPANION TO PHILOSOPHY OF TECHNOLOGY (Joseph Pitt & Ashley Shew eds., 2018), https://www.routledge.com/Spaces-for-the-Future-A-Companion-to-Philosophy-of-Technology/Pitt-Shew/p/book/9780415842969; *see also* Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1, 5 (2013) ("We argue the case for obscurity for two reasons. First, we argue that obscurity is a common and natural condition of interaction, and therefore human expectation of obscurity will transfer to the domains in which we spend time, both physical and virtual. Second, we argue that obscurity is a desirable state because we are protected by an observer's inability to comprehend our actions, and therefore social practice encourages us to seek obscurity."); Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385 (2013).

[31] Ching-Yi Lin, Jen-Yin Yeh & Yi-Ting Yu, *The Influence of Privacy Calculus, User Interface Quality and Perceived Value on Mobile Shopping*, 4 JOEBM 567–572 (2016); Evgenia Princi & Nicole C. Krämer, *Out of Control – Privacy Calculus and the Effect of Perceived Control and Moral Considerations on the Usage of IoT Healthcare Devices*, 11 Frontiers Psych. (2020); Han Li, Rathindra Sarathy & Heng Xu, *Understanding Situational Online Information Disclosure as a Privacy Calculus*, J. Comp. Info. Sys. 29 (2010).

eavesdropping. But no comparable strategies exist for protecting ourselves from automated voiceprint analysis that makes inferences about our identity and predicts our future behavior by dramatically reducing the transaction costs for others to come to putatively scientific conclusions about these matters based on how we speak. Likewise, the ease of using phones to take photographs and widely distribute images online contributed significantly to the proliferation of non-consensual pornography. This highly offensive behavior caught many victims off-guard and left them vulnerable and without legal recourse until privacy advocates championed reform.[32]

Our understanding of the role transaction costs play in safeguarding obscurity builds upon Harry Surden's work on structural privacy protections.[33] Surden observed that throughout much of history, many of our privacy interests had been shielded from undesirable behaviors, such as peeping and eavesdropping, by "constraints," not laws. When these constraints routinely and reliably limit access to personal information, societal expectations form about the strength of these safeguards. In some cases, the constraints are robust and function as behavior-guiding mechanisms comparable to the guidance instilled by the authority of legal rules. When this deep level of societal dependency occurs, and the constraints provide a viable substitute for legal prohibitions backed up by deterring sanctions, Surden argues it is reasonable to draw three conclusions.[34]

First, the constraints can disincentivize the need to create laws.[35] After all, why enact legislation to solve a problem for which adequate and widely available remedies already exist? Second, the constraints protect something so normatively powerful in the domain of negative individual rights (i.e., rights that limit what others do to us) that they preserve a good analogous to legal rights.[36] Surden used the term "structural rights" to capture this baseline defense. Third, suppose technological advances

---

[32] *See* DANIELLE KEATS CITRON, THE FIGHT FOR PRIVACY (2022); DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014); Mary Anne Franks, *'Revenge Porn' Reform: A View from the Front Lines*, 69 FLA. L. REV. 1251 (2017).

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

[34] *Id.* at 1607.

[35] *Id.*

[36] *Id.*

diminish transaction costs for accessing and correctly interpreting personal information to the extent that longstanding societal expectations of privacy are readily violated. In that case, the change does more harm than merely disrupt shared assumptions. It breaks something so socially significant that the outcome is comparable to the violation of a fundamental right.[37] Consequently, when regulators fail to enact legal reform to make up for critical privacy-protecting constraints losing their efficacy due to innovation in surveillance technology, they are, under Surden's theory, in effect failing to protect our rights.[38] Predictably, this will happen when regulators adopt the "conventional view in the privacy domain that privacy rights are coextensive with the set of explicit privacy laws and doctrines enumerated by legal rule-makers."[39]

Surden's account of constraints is broad enough to encompass explicitly designed tools, such as physical artifacts and digital code. Locks make it difficult but not impossible for unwanted intruders to open diaries. Well-encrypted communication can prevent most unintended recipients from reading it. Crucially for obscurity theory, Surden also identifies an implicit layer of protection that he calls "latent structural constraints."[40] He characterizes these constraints as barriers that members of society, including policymakers, are prone to take for granted. The protection latent structural constraints offer "are simply by-products of the technological or physical state of the world."[41] For example, due to current technological limitations, others cannot read our minds, and there is no need to regulate anything like telepathy legally. We can go about our business without worrying in the slightest that Elon Musk can peer into our thoughts without our permission using the latest version of Neuralink or any other device. Likewise, since the evolved structure of the human mind does not permit even the most intelligent of our species to engage in mind-reading, there is no need to be wary that someone like the fictional Prof. X from the X-Men comics might be secretly probing us. However, if someday, brain-computer interface technology becomes immensely powerful, or if biotechnological

---

[37] *Id.*

[38] *See* Hartzog & Selinger, *Surveillance*, *supra* note 30; Surden, *supra* note 33, at 1607.

[39] Surden, *supra* note 33, at 1607.

[40] *Id.*

[41] *Id.*

upgrades enable the post-human mind to do previously impossible things, new legal rules to protect our minds will be necessary.

This dynamic is occurring now with facial recognition technology. The ability for strangers to identify us by our faces has been historically protected by a default state of structural obscurity protections—specifically, technological limitations (i.e., previously, no automated technology could reliably infer who someone by analyzing facial features) and biological ones (i.e., there is a limit to how many name-face connections the average human can memorize). Based on Surden's theory, legal gaps that permit the use of facial recognition technology without our consent go beyond violating our privacy interests. They destroy our structural rights.

Importantly, Surden offers diagnostic insight into the functional reasons why policymakers are prone to overlooking the privacy-protecting role of latent structural constraints. First, policymakers are trained to critically examine explicit governance rules. By contrast, latent structural constraints are "more difficult to observe."[42] Perhaps these constraints require special methods, sociological and philosophical, for example, to identify and elucidate. Second, when latent structural constraints prove effective as background conditions, they make it easy for the privacy interests they protect to "garner little attention."[43] Third, unlike deliberately crafted laws underwritten by clear and rational justification, latent structural constraints only exist due to limitations in the world.[44] For example, the U.S. legal system typically asserts that people lack a reasonable expectation of privacy when in public. The reasoning is that people waive privacy rights or consent to being watched by venturing out; or that competing values like free expression and the democratic and social value of observing others take precedence over individual privacy rights. By contrast, the zone of obscurity that historically has protected our faces has little to do with our normative reasoning about justice.

Because the zones of obscurity that people rely upon all the time depend on the costs of finding or understanding information, the zones exist on a spectrum. The greater the cost of a particular activity, the less

---

[42] *Id.*
[43] *Id.*
[44] *Id.*

likely it will occur. The more unlikely it is that people's actions and data will be monitored and processed, the more freedom they have to act without fear of discovery. Transaction costs work like a knob or dial that can be modulated to affect risk. Increasing the cost of surveillance and processing increases protection; lowering these costs facilitates harm through increased risk of exposure.

But the smooth, undifferentiated spectrum of risk from changed transaction costs has made it very hard to have a real sense of when obscurity encroachments have gone too far. Indeed, there is no consensus around or method for knowing when people have lost too much obscurity, both individually and collectively as a society. In many instances, it is unclear where the threshold lies for determining what transaction costs are necessary for maintaining a zone of obscurity.

Even if it is hypothetically possible to answer the question of "how much loss of obscurity is too much," we must first better grasp how obscurity diminishes. Here we propose using the concepts of nicks and chops to distinguish between actions that cause significant and immediate harms from those that cause negligible but potentially long-term damage. When blades injure people, sometimes they are merely nicked. A small cut that hurts little heals quickly and leaves barely noticeable scars. Other times people are subjected to a more substantial, deeper cut—a chop. Chops are more painful and can leave lasting damage if they sever anything important. We believe privacy encroachments can be thought of along similar lines. Except in the world of privacy, it is time we started paying attention to the little things.

B. The Indicia of Privacy Nicks

In this part we identify the factors the determine the severity of a privacy encroachment and explore the indicia of privacy nicks. We return to Neil Richards' working definition of privacy, calling it "the degree to which human information is neither known nor used."[45] We draw upon this definition to conceptualize nicks and chops because it theorizes privacy as a matter of degree rather than a binary idea. We plot obscurity along a spectrum in the same way. We argue privacy nicks can be identified by

[45] RICHARDS, *supra* note 26, at 22.

asking four questions: 1) To what degree does a deployment reduce the transaction cost of surveillance?; 2) To what degree does a deployment challenge privacy norms?; 3) To what degree does a deployment appear to (and actually) endow power to the watchers?; and 4) How many people stand to be affected by a deployment? If the answer to any four of these questions is "not much," you might be looking at a privacy nick. This can be true even if you answered "significantly" to the other questions.

These four questions are just shorthand heuristics, not scientific variables to be formally and empirically measured. We present them as rough tools to help lawmakers and judges identify privacy nicks and see how they contrast with privacy chops, which are more traditionally targeted by surveillance law. The purpose of looking for signs of privacy nicks is to help identify *which* actions are not receiving enough scrutiny, *why* they are dangerous, and *where* the law might intervene.

First, the extent of a privacy encroachment is often contingent upon the cost of surveillance. The design of technologies can *reduce the transaction costs* of knowing or using human information.[46] A chop often is the result of *significantly* reduced transaction costs, whereas nicks often follow from more minor affordances. To revisit a previous example, automating the process of voiceprint analysis dramatically reduces transaction costs for inferring aspects of our identity and predicting our future behavior.

Second, privacy encroachments can *change existing norms*.[47] Chops typically not only challenge norms but often outright *defy* them, surpassing people's existing assumptions about surveillance and shifting paradigms too quickly for society to meaningfully consider and foment an appropriate democratic response. The speed at which chops occur also typically frustrates people's ability to develop individual avoidance strategies. For example, it seemed unimaginable for an unknown private

---

[46] Dave Davies, *Surveillance And Local Police: How Technology Is Evolving Faster Than Regulation*, NPR (Jan. 27, 2021, 12:51 PM), https://www.npr.org/2021/01/27/961103187/surveillance-and-local-police-how-technology-is-evolving-faster-than-regulation.

[47] Nicholas Proferes, *The Development of Privacy Norms*, *in* MOD. SOCIO-TECHNICAL PERSPS. ON PRIV. 79–90 (Bart P. Knijnenburg et al. eds., 2022), https://doi.org/10.1007/978-3-030-82786-1_5.

company to construct the world's largest facial recognition database in the recent past. And yet, Clearview AI claims to have done just that, obtaining over three billion biometric holdings by using an image scraper to scour the internet for data. In other words, chops are surveillance and data processing activities that are significantly out of sync with reasonable social expectations about their cost and frequency. Conversely, some encroachments more quietly change or evolve our perspectives towards surveillance without obvious paradigm shifts. Nicks may go completely unnoticed or may only be given attention by vigilant eyes within the privacy community. The societal group perceiving these norms does not heavily matter; whether a privacy scholar or lawyer has different sensitivities than a layperson does not negate the way these norms change for society overall.

Third, privacy encroachments can *endow power*,[48] typically towards surveilling groups or existing institutions, but sometimes can shift power more generally towards the upper tiers of myriad power dynamic relationships. Chops often *significantly* transfer power to certain groups. In these instances, information obtained through surveillance gives others power over us. Such power can manifest in many ways. For example, it is not difficult to imagine a restaurant where bigoted servers harass or refuse to serve a person if digital tools that scan faces or voices purport to detect a non-binary person.[49] To be sure, such a vile directive does not require digital tools to be carried out. Nevertheless, the reduced transaction costs of automating observation and classification make it easier to operationalize and systematize the discrimination and bestow powers upon people they would not otherwise have. Nicks might not transfer this power as noticeably; in some respects, nicks may appear to benefit the surveilled more than the surveiller or may appear to democratize surveillance powers.

Finally, privacy encroachments can be measured by *footprint,* with chops often being made *widely* conductible due to vastly reduced

---

[48] Alessandro Acquisti, Leslie K. John & George Loewenstein, *What Is Privacy Worth?*, 42 J. LEGAL STUD. 249–274 (2013); Andrew Imbrie et al., *Privacy Is Power*, FOREIGN AFFS. (Jan. 19, 2022), https://www.foreignaffairs.com/articles/world/2022-01-19/privacy-power.

[49] Kyle Wiggers, *'Fundamentally Flawed' Study Describes Facial Recognition System Designed to Identify Non-Binary People*, VENTUREBEAT (July 14, 2020, 8:40 PM), https://venturebeat.com/2020/07/14/study-describes-facial-recognition-system-designed-to-identify-non-binary-people/.

transaction costs. This scale can be defined by the number of users or people impacted by a new privacy encroachment, whether directly or indirectly – or by other scale metrics. It might have taken some time for new technologies to be widely adopted in the past. But with the advent of cloud computing and the ability of companies to make instantaneous changes to their services, billions of people can suffer a 'privacy chop' overnight. One reason Apple was criticized for rolling out a child safety feature that scans phones is that an estimated one billion people use iPhones worldwide. This scale means people will experience any changes that Apple makes that impact privacy globally. Such scale was hard to envision merely a few years ago. In 2009, when Apple launched its first smartphone, customers had to purchase it from a single store in San Francisco. By contrast, you could obtain the most recent iPhone in dozens of countries upon release. Nicks, then, often leave smaller footprints. If a particularly egregious, data-guzzling scam app only has five users, its privacy encroachments will revolve mainly around those five users and their extended network.

One way of identifying a privacy nick is to make sure it isn't a chop. The best way to think of a privacy encroachment large enough to be categorized as a chop is to envision dramatic lurches that significantly endanger people in a relatively short amount of time. The risk you face in the world is seemingly manageable one minute, and the next, it is much bigger and suddenly unmanageable. When Clearview AI scraped billions of social media profile photos, law enforcement authorities could effortlessly match people's faces to their identity using facial recognition almost overnight.[50] One minute people who lived in the cities subjected to Clearview A.I. could count on a relative degree of obscurity from law enforcement searches when moving about in public. The next minute they could not.

People have long intuitively distinguished between nicks and chops. Technology consistently makes finding and understanding information easier, famously exemplified by Warren and Brandeis's concern over the hand-held camera. The chop's elder siblings can be compared to peeping-

[50] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

tom style exposures, such as hard-to-detect spy cameras that make surveillance easier by lowering the cost of covert surveillance by decreasing the likelihood of detection. However, adding the chop to the privacy policymaker's vocabulary makes it easier to group historical examples (e.g., the introduction of Facebook's newsfeed, Google's search bar, etc.) into a common category and further differentiate their impact from the contrast class, the nick.

Let's continue to develop Clearview AI as a key example of a chop. For clarity, we restrict our definition of the 'event' of Clearview AI to the period between their successful, at-scale crawls of publicly available images and the January 2020 exposé[51] that revealed them – that is, we refer to their *deployment* of their facial recognition technology. This is distinct from the process of developing said technology (namely, the acts of scraping) prior to release. Chops must be framed within a limited period of time; longitudinal obscurity erosions may result in similarly dramatic outcomes but can result from several nicks rather than one game-changing chop. Similarly, the initial effect of a chop must be time-bound as problems of obscurity can continue to grow as the result of a chop; when the New York Times article was first released, Clearview reportedly had approximately 3 billion images in its database; in an October 2021 interview with WIRED Magazine[52], they claimed to have 10 billion images. While more than doubling the size of the dataset certainly implies greater impact, this continued growth of Clearview's records do not constitute the same alarming traits as a chop – though they are alarming in other ways. We explore this further below.

Had Clearview only trawled for images and done nothing with them, the act of amassing more than 3 billion face images might not have registered with people.[53] But the magnitude of Clearview's database, coupled with the facial recognition intelligence garnered from this incredible source of training data, contributed to a radically significant reduction in transaction costs for identifying individuals with images alone.

---

[51] *Id.*

[52] Will Knight, *Clearview AI Has New Tools to Identify You in Photos*, WIRED (Oct. 4, 2021, 7:00 AM), https://www.wired.com/story/clearview-ai-new-tools-identify-you-photos/.

[53] Kashmir Hill's comprehensive reporting on the topic was also crucial in the public's understanding of the threat. Hill, *supra* note 50.

Then, in distributing their capabilities to law enforcement organizations, Clearview conferred a significant endowment of power to watchers over the watched. Using those images for a machine learning training dataset satisfies the first condition of a chop and secondarily creates an environment for the third condition to arise.

Then we turn to the second variable of privacy encroachments. Clearview's database marks a shocking defiance of mental models and norms. While this defiance was certainly not sudden to Clearview, it was disruptive first to the law enforcement organizations invited to use Clearview as a tool and secondly to the unwitting public that learned about them in January 2020. Prior to Clearview, no such known database of faces existed, even when considering large platforms like Facebook or Google, or government agencies' own records. While people may have understood that facial recognition models were robust and available, privacy scholars and platforms alike did not anticipate that such a dystopically powerful dataset had *already* been collected. People knew their faces were there; they likely did not believe they had already been aggregated to this extent. Facebook and Twitter[54] sent cease-and-desist letters to Clearview, clearly unenthusiastic about the perceived abuse of their users' public data and their own terms of use, and quickly were followed by other titans of technology.[55]

Lastly, Clearview's crawled dataset indicates a vast footprint. 3 billion images have the potential to build low-quality faceprints of 3 billion people or much higher-fidelity faceprints for a subset of that number. At either end of the spectrum, a reach of nearly half the world's population constitutes a considerably vast footprint. However, even if the originally discussed database could accurately identify 1% of 3 billion, that still would include 30 million people – an arguably worrisome scale. But breadth is only one way to view footprint or impact; the adoption of a chop is not dependent solely on the number of users it directly impacts but additionally

---

[54] Igor Bonifacic, *Facebook and Venmo Demand Clearview AI Stops Scraping Their Data*, ENGADGET (Feb, 2, 2020, 10:48 AM), https://www.engadget.com/2020-02-06-facebook-venmo-cease-and-desist-clearview-ai.html.

[55] *Google, YouTube, Venmo and LinkedIn Send Cease-And-Desist Letters to Facial Recognition App That Helps Law Enforcement*, CBS NEWS (Feb. 5, 2020, 6:25 AM), https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/.

includes the potential for further reach. As mentioned before, Clearview's database has only grown since we first learned of it and in fact tripled in size.[56] It is hard to imagine that it ever had the potential to shrink unless heavily and punitively regulated against. But it is much easier to imagine the potential to continue expanding if unchecked.

Based on these four criteria (costs, norms, power, reach), chops usually have a disruptive impact on society. In 2021 Canadian Privacy Commissioner Daniel Therrien called Clearview's activities "illegal,"[57] and intoned that Clearview might "not make the use of the facial images of Canadians" without consent – though this claim was informal, as Canada cannot force the U.S.-based company to delete photographs of Canadian citizens.[58] Therrien's comments came months after Clearview offered opt-out to Canadians.[59] Even with retaliatory comments from government officials and voluntarily halted operations for non-governmental customers,[60] Clearview continues to grow[61] and is likely still in use internationally.[62]

Sometimes chops even have spillover effects. In November 2021, Meta announced that it would "shut down" the Face Recognition system on

---

[56] Knight, *supra* note 52.

[57] Kashmir Hill, *Clearview AI's Facial Recognition App Called Illegal in Canada*, N.Y. TIMES (Feb. 3, 2021), https://www.nytimes.com/2021/02/03/technology/clearview-ai-illegal-canada.html.

[58] Scott Ikeda, *Canada's Privacy Commissioner Rules That Clearview AI Facial Recognition Software Violates Privacy Laws, Must Delete Biometrics From Its Database*, CPO MAGAZINE (Feb. 12, 2021), https://www.cpomagazine.com/data-privacy/canadas-privacy-commissioner-rules-that-clearview-ai-facial-recognition-software-violates-privacy-laws-must-delete-biometrics-from-its-database/; Eyako Heh, *Canada Has Denounced Clearview AI; It's Time for the United States to Follow Suit*, COUNCIL ON FOREIGN RELS. (Feb. 24, 2021, 9:48 AM), https://www.cfr.org/blog/canada-has-denounced-clearview-ai-its-time-united-states-follow-suit.

[59] Thomas Daigle, *Canadians Can Now Opt Out of Clearview AI Facial Recognition, with a Catch,* CBC NEWS (July 10, 2020, 1:51 PM), https://www.cbc.ca/news/science/clearview-ai-canadians-can-opt-out-1.5645089.

[60] Nick Statt, *Clearview AI to Stop Selling Controversial Facial Recognition App to Private Companies*, VERGE (May 7, 2020, 8:29 PM), https://www.theverge.com/2020/5/7/21251387/clearview-ai-law-enforcement-police-facial-recognition-illinois-privacy-law.

[61] Knight, *supra* note 52.

[62] Ryan Mac, Caroline Haskins, & Antonio Pequeno IV, *Clearview AI Offered Free Facial Recognition Trials To Police All Around The World*, BUZZFEED NEWS (Aug. 25, 2021, 10:33 AM), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table.

Facebook, including the deletion of facial recognition templates used to automatically identify users in photos and videos (Meta has not, however, commented on their plans for DeepFace, the algorithm powering Facebook's facial rec tech, which was trained with four million photos of nearly 4,000 users in 2014).[63] While this revelation may seem like a small triumph against the pervasiveness of facial recognition technology, it offers little comfort in the shadow of Clearview's already-trawled, already-used images from Facebook. This points to the severity of Clearview's impact. Had Facebook been the sole proprietor of its users' images, perhaps Meta's announcement might have felt like true mitigation. But with Clearview holding copies of perhaps the same images, its negative impact outlasts even the noblest of efforts from other platforms or parties.

Nicks, on the other hand, fly under the societal and legal radar when do not achieve whatever critical mass for provocation is necessary. Privacy nicks can be hard to appreciate because they can have some of the same indicia as chops. For example, privacy nicks often occur when the transaction costs to finding or understanding information are reduced in smaller increments, at a slower rate, with a milder power dynamic shift, or have a lesser overall impact. Nicks might even result in the same level of exposure as chops, but over a longer period.

Critically, nicks are also distributed unevenly, typically though not exclusively along racial, gender, sexual identity, and ability lines. In other words, one person's nick might be another person's chop, either directly or indirectly, depending on their identities and how they are situated. To the populace, individual nicks may seem like only minor deviations from the norm, and they might not even be perceived as risky or adversarial to people's interests. Those privileged enough to perceive privacy exposures as nicks (or not at all) might value the benefits of a particular technological deployment, say a health tracker like FitBit, over any perceived privacy

---

[63] Jerome Pesenti, *An Update On Our Use of Face Recognition*, META (Nov. 2, 2021), https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/; Tom Simonite, *Facebook Creates Software That Matches Faces Almost as Well as You Do*, MIT TECH. REV. (MAR. 17, 2014), https://www.technologyreview.com/2014/03/17/13822/facebook-creates-software-that-matches-faces-almost-as-well-as-you-do/.

tradeoffs. Christopher Gilliard and David Golumbia call this "luxury surveillance," that is, "surveillance that people pay for and whose tracking, monitoring, and quantification features are understood by the user as benefits they are likely to celebrate."[64] As Salome Viljoen notes, even small and repeated disclosures by people can be used by organizations to make population-level insights that can be used against others that share the same population features (or even those that don't). [65]

What this means is that we're all in this together. Yet our reality is that privacy nicks will be overlooked by privileged populations while simultaneously hitting vulnerable populations like communities of color first and hardest. Gilliard also noted the normalizing effect that luxury surveillance can have, and that buying into the luxury surveillance ecosystem is to tacitly support the oppressive development and use of these systems. Gilliard argued, "Hidden below all of this is the normalization of surveillance that consistently targets marginalized communities….Looking back to Detroit, surveillance cameras, facial recognition, and microphones are supposedly in place to help residents, although there is scant evidence that these technologies reduce crime. Meanwhile, the widespread adoption of surveillance technologies—even ones that offer supposed benefits—creates an environment where even more surveillance is deemed *acceptable*. After all, there are already cameras and microphones everywhere." [66]

This not-quite nature of a nick is best illustrated by the advent of smart doorbell technology, focusing on the Amazon Ring doorbells as a case study. In nearly a decade, Ring grew from a small start-up to an Amazon acquiree supporting "millions" of customers, with impressive sales

---

[64] Chris Gilliard and David Golumbia, *Luxury Surveillance*, REAL LIFE MAG (July 6, 2021), https://reallifemag.com/luxury-surveillance/. ("Only certain people can afford luxury surveillance, but that is not necessarily a matter of money: In general terms, consumers of luxury surveillance see themselves as powerful and sovereign, and perhaps even immune from unwelcome monitoring and control. They see self-quantification and tracking not as disciplinary or coercive, but as a kind of care or empowerment. They understand it as something extra, something "smart.").

[65] Salome Viljoen, *A Relational Theory of Data Governance*, 131 Yale. L. J. 573, 578 (2021).

[66] Chris Gilliard, *The Rise of 'Luxury Surveillance'*, THE ATLANTIC (Oct. 18, 2022), https://www.theatlantic.com/technology/archive/2022/10/amazon-tracking-devices-surveillance-state/671772/.

estimates even after several reports of grave privacy concerns like data breaches and providing heatmaps of device locations to police.[67]

The present-day Ring doorbell deployment seems like a privacy chop according to some of the indicia of privacy encroachments. By placing cameras on unassuming residential doors, it greatly reduces transaction costs for gathering local footage; Rings make the collection of CCTV-styled security video fast, cheap, and relatively 'good' in quality. By corroborating with police[68] (or by having infrastructure enabling inappropriate employee access to user video data and feeds),[69] Amazon significantly conferred power upon law enforcement officials over the people captured by the small cameras. With Amazon's scale and reach, Ring could increase operations and sell more devices – in fact selling over 400,000 devices in December

---

[67] Laura Stevens & Douglas MacMillan, *Amazon Acquires Ring, Maker of Video Doorbells*, WALL ST. J. (Feb. 27, 2018), https://www.wsj.com/articles/amazon-acquires-ring-maker-of-video-doorbells-1519768639; Rani Molla, *Amazon Ring Sales Nearly Tripled in December Despite Hacks*, VOX (Jan. 21, 2020, 1:50 PM), https://www.vox.com/recode/2020/1/21/21070402/amazon-ring-sales-jumpshot-data; Caroline Haskins, *A Data Leak Exposed the Personal Information of Over 3,000 Ring Users*, BUZZFEED NEWS (Dec. 19, 2019, 10:58 AM), https://www.buzzfeednews.com/article/carolinehaskins1/data-leak-exposes-personal-data-over-3000-ring-camera-users; Alfred Ng, *Ring Let Police View Map of Video Doorbell Installations for over a Year*, CNET (Dec. 3, 2019, 9:00 AM), https://www.cnet.com/home/security/ring-gave-police-a-street-level-view-of-where-video-doorbells-were-for-over-a-year/.

[68] Lauren Bridges, *Amazon's Ring Is the Largest Civilian Surveillance Network the US Has Ever Seen*, GUARDIAN (May 18, 2021), https://www.theguardian.com/commentisfree/2021/may/18/amazon-ring-largest-civilian-surveillance-network-us; Kim Lyons, *Amazon's Ring Now Reportedly Partners with More than 2,000 US Police and Fire Departments*, VERGE (Jan. 31, 2021, 11:26 AM), https://www.theverge.com/2021/1/31/22258856/amazon-ring-partners-police-fire-security-privacy-cameras; Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019, 6:53 PM), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/.

[69] Amazon, *Ring Response Letter to the U.S. Senate* (Jan. 6, 2020), https://www.documentcloud.org/documents/6603161-Ring-Response-Letter; Ben Lovejoy, *Ring Fires Employees for Spying on Customer Videos Stored in the Cloud*, 9TO5GOOGLE (Jan. 9, 2020, 4:48 AM), https://9to5google.com/2020/01/09/spying-on-customer-videos/; Kyle Wiggers, *Ring Employees Reportedly Had Access to All Live and Recorded Customer Videos (Updated)*, VENTUREBEAT (Jan. 10, 2019, 12:35 PM), https://venturebeat.com/2019/01/10/ring-employees-reportedly-had-access-to-all-live-and-recorded-customer-videos/; Sam Biddle, *For Owners of Amazon's Ring Security Cameras, Strangers May Have Been Watching Too*, INTERCEPT (Jan. 10, 2019, 12:34 PM), https://theintercept.com/2019/01/10/amazon-ring-security-camera/.

2019,[70] in advance of a pandemic online-shopping boom that led to the sale of over 1.4 million more devices in 2020 (the latter number nearly equating the sales records for their next four competitors, combined).[71] This indicates a large – and growing – footprint.

However, it's not clear whether the Ring technology rapidly surpasses existing consumer expectations. It's deployment doesn't seem to significantly disrupt norms. People are accustomed to being watched in somewhat analogous ways. CCTV technology is known and normalized; security cameras are used widely in banks and government buildings. Owners of small businesses like corner shops can use cameras for peace of mind, self-defense, and future protection. But telling laypeople of a few decades ago that your entire block of neighbors could have cameras to spy on your community at the touch of a button, and you might receive dismissive scoffs or alarmist gasps. The difference is that the slower pace of the Ring's growth made for a slow boil. When factoring for time, the shock factor loses its strength. Clearview shook our expectations seemingly overnight, but the privacy problems accompanying Ring technology are common in other technologies, and we are inured to these abuses when they happen so frequently that we may not notice a paradigm shifting by incremental units.[72] If the advent of Ring tech were so alarming to us, layperson sales would not have experienced the level of growth Amazon saw in 2020, whether that be due to societal disapproval or immediate injunctive measures to respond to a crisis of privacy.

Deployments of a particular technology that are chops in one setting might be nicks in another. A good example is the increasingly widespread deployment of facial recognition technology by summer camps to identify

---

[70] Molla, *supra* note 65.

[71] *Strategy Analytics: Amazon's Ring Remained atop the Video Doorbell Market in 2020*, BUS. WIRE (May 12, 2021, 8:43 AM), https://www.businesswire.com/news/home/20210512005336/en/Strategy-Analytics-Amazons-Ring-Remained-atop-the-Video-Doorbell-Market-in-2020.

[72] Kashmir Hill, *"God View": Uber Allegedly Stalked Users For Party-Goers' Viewing Pleasure (Updated)*, FORBES (Oct. 3, 2014, 11:32 AM), https://www.forbes.com/sites/kashmirhill/2014/10/03/god-view-uber-allegedly-stalked-users-for-party-goers-viewing-pleasure/; Alex Hern, *Uber Employees "Spied on Ex-partners, Politicians and Beyoncé,"* GUARDIAN (Dec. 13, 2016), https://www.theguardian.com/technology/2016/dec/13/uber-employees-spying-ex-partners-politicians-beyonce.

campers in photos sent to the camper's parents and guardians.[73] This technology lowers the cost of identifying campers without an immediate dramatic increase in exposure to risk. The immediate risk is low because parents expect staff to monitor their kids closely. Introducing facial recognition technology does not transform a low surveillance situation into a high one. However, the nick can subtly change parental expectations. If it is acceptable for facial recognition technology to be used at camp, why not in similar environments, such as schools?

Another example of a technology that facilitates privacy nicks is Apple's FaceID system, which uses facial verification technology to authenticate users of Apple iPhones. The initial deployment of FaceID, in itself, a nick. From a standard privacy-by-design perspective, FaceID is excellent. It securely encrypts faceprints and stores them locally on each phone, which does very little to reduce a remote[74] watcher's transaction cost for accessing a user's faceprint. Consequently, Apple is not building a name-face database that other companies or government agencies can use – they don't endow the power of surveillance to watchers. Additionally, FaceID didn't dramatically shift existing norms. At the time of deployment on devices in 2017,[75] facial recognition on smart devices was somewhat known (with Windows Hello and Android's Trusted Face deployed two years prior). FaceID's footprint at the time relied on sales of the new iPhoneX, the first iteration to contain the feature. While Apple reached impressive sales numbers[76] within the first few months of release, older models than the iPhone X did not receive FaceID[77] and relied instead on

---

[73] *Face Finder FAQs*, COMPANION APP, https://campanionapp.com/support/help/facefinder-faq/ (last visited Feb. 7, 2023); Melissa Locker, *Summer Camps Are Using Face Recognition to Keep Track of Camper Photos*, FAST CO. (July 18, 2018), https://www.fastcompany.com/90204346/summer-camps-are-using-face-recognition-to-keep-track-of-camper-photos.

[74] FaceID and similar technologies do, however, significantly reduce transaction costs to the detriment of individuals in cases where law enforcement officers hold devices up to citizens' faces to unlock a device.

[75] Thorin Klosowski, *Facial Recognition Is Everywhere. Here's What We Can Do About It*, N.Y. TIMES: WIRECUTTER (July 15, 2020), https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/.

[76] Todd Haselton, *Apple Sold 46.7 Million iPhones during the Quarter*, CNBC (Nov. 2, 2017, 4:30 PM), https://www.cnbc.com/2017/11/02/how-many-iphones-did-apple-sell-in-q4-2017.html.

[77] iPhone and iPad Models That Support Face ID, APPLE SUPPORT, https://support.apple.com/en-us/HT209183 (last visited Feb. 7, 2023).

the older fingerprint mechanism, TouchID – thus the immediate footprint or reach of FaceID was limited in comparison to the greater iOS user population.

By making FaceID the new standard on all following mobile iOS devices, however, Apple contributed to the material conditions for people to grow accustomed to having their faces frequently scanned every day, which risks normalizing more invasive forms of automated facial analysis.[78] While facial verification and facial recognition are different technical functions, normalizing the former might psychologically predispose people to embrace the latter. Note that the normalization of facial recognition on portable devices cannot be solely blamed on FaceID, nor Apple. Rather, the accumulation of nicks, in which more and more similar features are developed and deployed[79], steadily adjusts our comfort levels with the ubiquity of such technologies.

A third example of a facial recognition technology that facilitates privacy nicks is Amazon's Ring Always Home Cam, a small and light autonomous drone intended for indoor use.[80] The robot is designed to fly through a house and record video on a high-definition camera that can stream to a smartphone. Amazon markets the technology as a tool for

---

[78] Such forms could be from shadier but smaller companies that don't take care to secure faceprints, for example. *See* Arielle Pardes, *Facial Recognition Tech Is Ready for Its Post-Phone Future* (Sept. 10, 2018, 7:00 AM), https://www.wired.com/story/future-of-facial-recognition-technology/. Studies suggest that familiarity with particular technologies is positively associated with the adoption, usage, and acceptance of these technologies. *See* Oliver Buckley & Jason R.C. Nurse, *The Language of Biometrics: Analysing Public Perceptions*, 47 J. INFO. SEC. & APPLICATIONS 112 (2019); Xiaojun Lai, Pei-Luen Patrick Rau, *Has Facial Recognition Technology Been Misused? A Public Perception Model of Facial Recognition Scenarios*, 124 COMPUTS. IN HUM. BEHAV., Nov. 2021, at 106894; Efosa C. Idemudia & Mahesh S. Raisinghani, *The Influence of Cognitive Trust and Familiarity on Adoption and Continued Use of Smartphones: An Empirical Analysis*, 23 J. INT'L TECH. & INFO. MGMT., no. 2, 2014, at art. 6. See PEW RESEARCH CENTER, MORE THAN HALF OF U.S. ADULTS TRUST LAW ENFORCEMENT TO USE FACIAL RECOGNITION RESPONSIBLY (2019), for a survey of Americans' trust and acceptance of facial recognition technology in different situations.

[79] And, potentially, with little oversight, without strong ethical parameters, or without thought-out cybersecurity practices.

[80] *Ring Always Home Cam*, AMAZON, https://www.amazon.com/Ring-Always-Home-Cam/dp/B08YH144XD (last visited Feb. 7, 2023); David Priest, *Always Home Cam: Amazon's Flying Ring Drone Might Be Tricky to Get Your Hands On*, CNET (Sept. 28, 2021, 1:27 PM), https://www.cnet.com/home/security/always-home-cam-amazons-flying-ring-drone-might-be-tricky-to-get-your-hands-on/.

deterring thieves. By itself, the 'deployment' of the device is a nick; focusing solely on the footprint quality, the device is currently only available by invitation and not rolled out to the general public.[81] There are potential harms; the most immediate danger is the technology could potentially be used to further domestic abuse—although it is questionable how effective the drone would be compared to more covert spyware. Still, if we look at the possible future impacts of the drone, a different danger becomes salient, and we can see the potential for future nicks.

As a mobile surveillance system, the Always Home Cam expands the range of surveillance Amazon previously offered with its stationary Ring doorbell cameras. By introducing a camera that moves around, Amazon appears to be trying to get the public comfortable with the idea that mobile surveillance cameras are exciting, cool, and useful—certainly not something to be afraid of, unless, that is, you're a criminal. In other words, these drones may normalize the experience of surrounding people with mobile camera surveillance. Supporting evidence for this hypothesis can be found by critically thinking about what this product has in common with another one that was announced at the same launch in 2020: the still-unreleased (in May 2022) Ring Car Cam.[82] This dashboard security camera was designed for use on moving automobiles.

But why, exactly, would anyone want it? Amazon initially emphasized it has a "traffic stop" feature that starts recording and streaming video data to the cloud when users say, "Alexa, I'm getting pulled over." Ostensibly, this is Amazon's attempt to help protect citizens from police abuse. But given how aggressively Amazon partners with law enforcement to promote Ring, a technology that privacy advocates are deeply concerned about, and given how reluctant it was to pause the sale of its facial recognition system, Rekognition, to police departments despite strong pushback from numerous privacy and civil rights advocacy organizations, it is not overly cynical to view this offering through a marketing lens, especially within the context of the politically fraught current events when the products were announced. While many were

---

[81] AMAZON, *supra* note 80.

[82] Adam Ismail, *Ring Car Cam and Car Alarm: What we know so far*, TOM'S GUIDE (July 1, 2022), https://www.tomsguide.com/news/ring-car-cam-and-car-alarm-price-release-date-features-and-more.

concerned about justice ignited by the Black Lives Matter Movement, Amazon instead sought to strengthen its brand of surveillance as a service. Though the Ring Car Cam is still in its early days, we see a future nick that is simply pre-deployment. As mentioned earlier, this presents an opportunity for regulation, but so far we have not seen the law sweepingly react to such developments to the same degree that it reacted to Clearview AI.

In many cases, prior nicks may lead to new nicks, but the entirety of the technology or product suite might still not garner enough legal attention to be effectively regulated. Privacy nicks have evolved due to increasingly surveillant technologies and reflect changes in our collective surveillance norms. Take the smart camera wearable Google Glass:[83] introduced after much fanfare, the augmented reality spectacles were plagued by bad press and public backlash[84] to myriad privacy concerns over the technology. We seemed victorious in the face of Glassholes and 'creepshots,'[85] collectively rallying against a technology we deemed egregious and *wrong*. But this victory was short-lived, even more so without legal preventions. The privacy landscape has changed since 2013; Glass still exists (though now marketed for enterprise use), Meta teamed up with Ray-Ban to build a new smart glasses product[86], and rumor has it that Google plans to make a smart spectacle comeback with Project Iris.[87]

---

[83] *Glass*, GOOGLE, https://www.google.com/glass/start/ (last visited Apr 5, 2022).

[84] Alyssa Newcomb, *From "Glassholes" to Privacy Issues: The Troubled Run of the First Edition of Google Glass*, ABC NEWS (Jan. 16, 2015, 9:38 AM), https://abcnews.go.com/Technology/glassholes-privacy-issues-troubled-run-edition-google-glass/story?id=28269049; Nick Bilton, *Why Google Glass Broke*, N.Y. TIMES (Feb. 4, 2015), https://www.nytimes.com/2015/02/05/style/why-google-glass-broke.html; Rose Eveleth, *Google Glass Wasn't a Failure. It Raised Crucial Concerns*, WIRED (Dec. 12, 2018, 7:00 AM), https://www.wired.com/story/google-glass-reasonable-expectation-of-privacy/.

[85] Whitney Erin Boesel, *Google Glass Doesn't Have a Privacy Problem. You Do*, TIME (MAY 19, 2014), https://time.com/103510/google-glass-privacy-foregrounding/.

[86] Katie Notopoulos, *Facebook and Ray-Ban Camera Glasses Are Here*, BUZZFEED NEWS (Sept. 9, 2021, 12:01 PM), https://www.buzzfeednews.com/article/katienotopoulos/facebook-is-making-camera-glasses-ha-ha-oh-no.

[87] Florence Ion, *Ready for Google Glass, Round Two?*, GIZMODO (2022), https://gizmodo.com/ready-for-google-glass-round-two-1848393934; Lance Ulanoff, *A Google AR Just It Google Glass 3.0*, TECHRADAR (Jan. 20, 2022),

This time around, smart glasses have more hype than horror – indicating a shift in our normative perspectives of augmented reality technologies, towards greater adoption or interest in them. If such technologies appear in line with our norms, both societal and legal, then why would they attract legal attention for privacy protections?

C. In Defense of Privacy's Slippery Slope

When privacy nicks go unchecked, profound societal ramifications can follow. Adverse consequences include nicks engineering positive beliefs about surveillance devices and practices that lead people to lose sight of how and why privacy protections provide essential checks against power. When nicks contribute to the normalization of surveillance, they contribute to what scholars have called 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. For example, a common fallacious slippery slope argument in tech policy circles is that if we weaken Section 230 even a little, it will eventually dissolve the entire safe harbor framework.[88]

But not all slippery slope arguments are fallacious, which is why we argue that slippery slope dynamics have gotten a bad rap. When it comes to privacy, they are a critical aspect of understanding how our privacy becomes endangered. Philosopher Anneli Jefferson notes that the traditional problem of slippery slopes is that "[o]bjections to infringements on civil liberties…frequently point to the fact that we take the status quo as normal and may not mind small restrictions being added. However, once we have gotten used to new restrictions, a further slight restriction might be introduced. In the end, so the thought goes, individuals will put up with restrictions they would never have accepted had they been all introduced

---

https://www.techradar.com/news/a-new-google-ar-headset-just-dont-call-it-google-glass-30; Joe Gvora, *Google Glass: What Happened to the Smart Glasses?*, SCREENRANT (Jun. 15, 2022), https://screenrant.com/google-glass-smart-glasses-what-happened-explained/.

[88] S*ee* Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401 (2017).

at once."[89] To illustrate this point, consider a counterfactual. Imagine if, in the United States, facial surveillance was introduced to the public at the same time as CCTV. The combination likely would have been seen as too significant of a departure from status quo expectations and widely rejected as too invasive.

What makes nicks that normalize surveillance so pernicious is that people do not always experience them as infringements as disconcerting, much less infringements upon liberty. Julie Cohen wrote that in our modulated world, "surveillance is not heavy-handed; it is ordinary, and its ordinariness lends it extraordinary power."[90] She argues that new surveillance technologies "do not have as their purpose or effect the 'normalized soul training' of the Orwellian nightmare. They beckon with seductive appeal. Individual citizen-consumers willingly and actively participate in processes of modulation, seeking the benefits that increased personalization can bring. For favored consumers, these benefits may include price discounts, enhanced products and services, more convenient access to resources, and heightened social status."[91] People also can perceive nicks inconsistently. For example, privileged populations are less likely to feel the immediate effects of certain surveillance practices. Given the diversity of experience and uneven distribution of harms, one person's chop might be felt as a nick by another.

Nicks can seem trivial and innocuous when they occur. And yet, over time, their impact on how we think about privacy and make decisions that impact privacy can be enormous. Indeed, enough privacy nicks can lead to societal changes that current versions of ourselves would deem unacceptable—changes we would so deeply regret we would wish we did not take the first steps down the slippery slope.

Amazon's use of a technology called Just Walk Out in select Whole Foods stores illustrates why privacy nicks cause gradual and subtle harm that masks long-term dangers. The surveillance and billing technology enables pilot program grocery store shoppers to efficiently complete their purchases—what, in technological and business terms, is called optimizing

---

[89] Anneli Jefferson, *Slippery Slope Arguments*, 9 PHIL. COMPASS 672–680, 675 (2014).

[90] Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1916–17 (2013).

[91] *Id.*

design to minimize friction. Here is how a *New York Times* reporter describes her grab and go experience of avoiding checkout lines and not spending time having items scanned at checkout. "I picked up a bag of cauliflower florets, grapefruit sparkling water, a carton of strawberries and a package of organic chicken sausages. Cameras and sensors recorded each of my moves, creating a virtual shopping cart for me in real-time. Then I simply walked out, no cashier necessary. Whole Foods—or rather Amazon—would bill my account later."

To make this cutting-edge shopping experience, one that uses computer vision, deep learning algorithms, and lots of cameras and sensors, as pleasant as possible, Amazon avoids putting Whole Foods customers in situations that are likely to cause stress or trigger resistance. Although customers can sign into the store with their palms, Amazon minimizes the likelihood that people will worry about this novel point of entry. It allows customers, presumably ones with privacy concerns about biometric data, to enter the store by scanning a QR code.

Furthermore, since surveillance can make people anxious when personal information gets used for personalized advertising, Amazon tries to avoid this tripwire. The company claims it does not "plan to use video and other Whole Foods customer information for advertising or its recommendation engine." Suppose Amazon sticks to this commitment and does not use it as a manipulative foot-in-the-door technique. In that case, customers have some assurance that a thoughtful policy underwrites the Just Walk Out program—one that protects privacy by limiting data use to necessary functions. Finally, since consent is viewed as a privacy prerequisite, Amazon allows customers to opt-out of the automated data collection process. Those who want to forgo hyper-convenience "can enter the store without signing in and pay at self-checkout kiosks with a credit card or cash."

But do all these safeguards mean Amazon respects consumer privacy? No. They have started us down the path of a *slippery slope*, inevitably desensitizing and acclimating an entire population to practices decried as oppressive and corrosive of our autonomy.

There are different varieties of slippery slope statements, and none of them have good reputations. The one we are proposing here forecasts the likelihood of a future where privacy is reduced dramatically. Since we are

making claims that will turn to be to true or false based on real-world events related to how nicks impact privacy outlooks and outcomes, the pronouncement is an empirical (not logical) slippery slope projection. As suggested above, empirical slippery slope assertions tend to be viewed as fallacious—as overly fearful guesses that exaggerate how badly the future will turn out. Thus, 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.

Eugene Volokh provides the best response to this objection, arguing that slippery slope advocates can identify precise mechanisms that modify the behavior of institutions, groups, and individuals in the direction of slippery slope outcomes.[92] For example, Volokh contends the "cost lowering slippery slope driver" can greatly impact long-term surveillance outcomes and undermine immediate approaches to policy-making.[93] Take a variation of the situation we mentioned above: a community deciding whether to adopt CCTV cameras to deter crime. If police use of the technology is restricted by fair policy, it might be widely supported, even by people who do not want law enforcement to engage in facial surveillance. But since the cost of surveillance technologies drops over time, the price of integrating plug-and-play facial recognition technology into the CCTV infrastructure eventually will become minor, ultimately insignificant. When that happens, facial recognition critics will have difficulty making a persuasive case against adding the upgrade. Since the community already made the initial investment in cameras, public safety proponents will find it easy to frame expanding their power for little cost as a bargain.

This example and others show that empirical slippery slope claims are not definitive assertions about how the future will take shape. They are claims about expected outcomes—outcomes that can be prevented if the power of the slippery slope mechanisms (what philosopher Douglas Walton

---

[92] Eugene Volokh, *The Mechanisms of the Slippery Slope*, 116 HARV. L. REV. 1026 (2003).

[93] *Id.*

calls" slippery-slope drivers") can be muted.[94] Thus, to make a valid empirical slippery slope argument, one must specify the causal mechanisms and explain why their influence is not likely to be dampened adequately in time to prevent disaster. We will do this by clarifying why the law is configured to ignore nicks in Section II and identifying mechanisms that normalize surveillance in Section III.

II. HOW THE LAW IGNORES NICKS

This part explores how lawmakers and judges systematically overlook privacy nicks. Privacy nicks are everywhere. They happen when you are spotted by doorbell cameras, targeted by algorithms for an uncomfortably specific ad, or have your geolocation tracked by an acquaintance. But they lacked a proper name. Nicks can be slightly unsettling, prompting a cringe, a momentary hesitation, or an eye roll. For example, many people might feel discomfort, like when people momentarily forget about being in the presence of Internet of Things devices with virtual assistants and accidentally say their "wake" word. People might even call them "creepy," the first time they realize they have been targeted by a personalized ad based on their browsing history or identified solely by their face[95] Or, nicks can impact our sensibilities without us even noticing they are changing our hearts and minds. Nevertheless, industry, government, strangers, and friends are constantly nicking people's privacy.

Yet the law plays very little role in these small exchanges because our privacy rules generally do not intervene unless someone's activity crosses a threshold of significance. Lawmakers and judges generally consider privacy nicks to be *de minimums* encroachments, and the law does not deal with trifles. There are a few bedrock behaviors that modern information privacy law cannot abide by: breached confidences, the unauthorized collection of sensitive information, the disclosure of highly offensive information collection, lies about data practices, identity theft

---

[94] Douglas Walton, *The Slippery Slope Argument in the Ethical Debate on Genetic Engineering of Humans, 23* SCI. & ENG'G ETHICS 1507 (2017).

[95] Selinger, *supra* note 28.

leading to financial harms, denial of informational self-determination, and failure to follow proper procedure before snooping.[96]

Outside of this threshold, U.S. privacy law typically tolerates all sorts of problematic activity and outcomes. This includes increased risk of financial harm, careless data practices that cause anxiety, subtle attempts to manipulate people into sharing more information, and, most relevant to this article, small personal exposures facilitated by the affordances of technologies.

There are three reasons the law ignores nicks: Lawmakers' intense focus on 1) concrete harms, 2) waiver, and 3) proximity. Since these three features of information privacy law render nicks permissible, legal frameworks function as an engine to render inevitable the slow and steady normalization of surveillance and data collection efforts that, if they happened quickly, would probably be considered privacy invasive. Let us explore these drivers of normalization a little more.

A. Harms Focus

Above all, privacy law is preoccupied with harms—injuries, setbacks, losses, or impairments to well-being.[97] Lawmakers, judges, and regulators intensely scrutinize the kind of harm, the severity of harm, and the concrete nature of harm when creating, interpreting, and enforcing privacy rules. Harm has become the gatekeeper to remedies, with courts requiring harms to be cognizable to meet the threshold for redress. Unfortunately, as Danielle Citron and Daniel Solove note, "Law's treatment of privacy harms is a jumbled, incoherent mess. Countless privacy violations are left unaddressed because courts refuse to recognize harm that has been suffered."[98]

When lawmakers and judges go looking for harms related to the use of new technologies, what they typically find are what we're calling chops: significant and immediate negative effects on an individual facilitated by the affordances of a tool. Many kinds of laws that regulate privacy-invasive activity, such as torts, contracts, and U.S. Constitutional law demand proof

---

[96] *See* Citron & Solove, *supra* note 27; Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011); Cofone & Robertson, *supra* note 27.

[97] Citron & Solove, *supra* note 27.

[98] *Id.*; Cofone & Robertson, *supra* note 27.

of this kind of intense and localized adverse effect.[99] In *TransUnion LLC v. Ramirez*, the Supreme Court further narrowed an already restrictive reading of Article III standing precedent by requiring that plaintiffs in federal court demonstrate a "concrete harm" that bears a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts, even where Congress has created an explicit cause of action without a harm requirement.[100]

But it is not just Article III standing law that demands significant and demonstrable privacy harm. Without a recognizable injury like physical harm, economic loss, diminution of reputation, or emotional distress or offense, courts will not impose liability under the common law against those who acted negligently, fraudulently, or intentionally.[101] The Federal Trade Commission might file a complaint against a company that engaged in unfair data security practices. Still, they are compelled to ask if the resulting data breach (or vulnerability to a data breach) injured (or is likely to injure) consumers in a way that is not reasonably avoidable by consumers themselves and not outweighed by benefits to the consumer or to competition.[102] This has traditionally meant some kind of financial or otherwise significant and articulable injury.[103]

Courts, lawmakers, and administrative agencies have recognized that a significant enough diminution of privacy in terms of personal exposure should suffice as harm. But the catch is that in the search for *significant* harms, lawmakers and courts overlook relatively minor

---

[99] *See* Citron & Solove, *supra* note 27; Smith v. Trusted Universal Standards In Elec. Transactions, Inc., No. 09–4567, 2010 WL 1799456 (D.N.J. May 4, 2010); Rudgayzer v. Yahoo! Inc., 5:12-CV-01399 EJD, 2012 WL 5471149 (N.D. Cal. Nov. 9, 2012), appeal dismissed (Dec. 13, 2012); Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).

[100] TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2200 (2021); Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).

[101] RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 26 cmt. a (Am. L. Inst. 2010).

[102] 15 U.S.C. § 45; Daniel J. Solove & Woodrow Hartzog, *The FTC and Privacy and Security Duties for the Cloud*, 13 BNA PRIV. & SEC. L. REP. (2014); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. (2014); Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. (2015); Daniel J. Solove & Woodrow Hartzog, *The Ultimate Unifying Approach to Complying with All Laws and Regulations*, 19 Green Bag 2d 223 (2016).

[103] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737 (2018).

disruptions to individuals due to the affordances of new technologies.[104] From one perspective, the occlusion is reasonable. Perhaps no single nick causes a sufficient level of harm to, on its own, deserve redress. And yet, as the harms of nicks build and aggregate, over time the collective harm of privacy nicks, like the ubiquitous deployment of surveillance cameras or the mass collection of data to create sophisticated ad targeting profiles can be overwhelming and result in privacy losses akin to the proverbial death by a thousand cuts.

B. Waiver Focus

The second legal focus that helps normalize surveillance concerns the concept of a privacy waiver. 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 "[T]here can be no privacy in that which is already public."[105] Their opinions are littered with statements like "Users would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting."[106] The FBI alleged it does not need permission to conduct surveillance using powerful technologies like cell-site simulators (often called Stingrays), so long as

---

[104] *Id.* ("For many privacy harms, the injury may appear small when viewed in isolation, such as the inconvenience of receiving an unwanted email or advertisement or the failure to honor your expectation that your data would not be shared with third parties. But when done by hundreds or thousands of companies, the harm adds up. Moreover, these small harms are dispersed among millions (and sometimes billions) of people. Over time, as numerous people are each inundated by a swarm of small harms, the overall societal impact can be significant. Yet, these types of injuries do not fit well into judicial conceptions of harm, which have an individualistic focus and heavily favor tangible physical and financial injuries that occur immediately.").

[105] *See* Gill v. Hearst Pub. Co., 253 P.2d 441, 444 (Cal. 1953) ("The photograph of plaintiffs merely permitted other members of the public, who were not at plaintiffs' place of business at the time it was taken, to see them as they had voluntarily exhibited themselves. Consistent which their own voluntary assumption of this particular pose in a public place, plaintiffs' right to privacy as to this photographed incident ceased and it in effect became a part of the public domain.... In short, the photograph did not disclose anything which until then had been private, but rather only extended knowledge of the particular incident to a somewhat larger public then had actually witnessed it at the time of occurrence.") (citing Melvin v. Reid, 297 P. 91, 93 (Cal. Ct. App. 1931)); *see also* Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 862 (2009), as modified (Apr. 30, 2009).

[106] Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001).

they are conducting surveillance in public places.[107] Judges have refused to punish people for taking "upskirt" photos because the women photographed have no reasonable expectation of privacy "in public," no matter how fleeting their exposure.[108]

For example, in *California v. Greenwood,* the Supreme Court concluded that "respondents exposed their garbage to the public sufficiently to defeat their claim to Fourth Amendment protection. It is common knowledge that plastic garbage bags left on or at the side of a public street are *readily accessible* to animals, children, scavengers, snoops, and other members of the public."[109] The Court in *Greenwood* seemed to equate making something freely accessible with the waiver of privacy rights, holding that "respondents placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents' trash or permitted others,

---

[107] David Kravets, *FBI Says Search Warrants Not Needed to Use "Stingrays" in Public Places*, ARS TECHNICA (Jan. 5, 2015), https://arstechnica.com/tech-policy/2015/01/fbi-says-search-warrants-not-needed-to-use-stingrays-in-public-places/; Press Release, Senator Chuck Grassley, Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program, (Dec. 31, 2014), https://www.grassley.senate.gov/news/news-releases/leahy-grassley-press-administration-use-cell-phone-tracking-program; David Kravets, *Feds: Privacy Does Not Exist in 'Public Places'*, Wired (Sept. 21, 2010), https://www.wired.com/2010/09/public-privacy/.

[108] Order to Suppress Physical Evidence and Statements, United States of America v. Cleveland, at 2, 3 (2014), http://pdfserver.amlaw.com/nlj/Cleveland%20motion%20to%20suppress%20order.pdf.

[109] California v. Greenwood, 486 U.S. 35, 40–41 (1988) ("[O]f those state appellate courts that have considered the issue, the vast majority have held that the police may conduct warrantless searches and seizures of garbage discarded in public areas.") (citing Commonwealth v. Chappee, 492 N.E.2d 719, 721–722 (Mass. 1986); Cooks v. State, 699 P.2d 653, 656 (Okla.Crim.), cert. denied, 474 U.S. 935, 106 S.Ct. 268, 88 L.Ed.2d 275 (1985); State v. Stevens, 123 Wis.2d 303, 314–317, 367 N.W.2d 788, 794–797, cert. denied, 474 U.S. 852, 106 S.Ct. 151, 88 L.Ed.2d 125 (1985); State v. Ronngren, 361 N.W.2d 224, 228–230 (N.D.1985); State v. Brown, 20 Ohio App.3d 36, 37–38, 484 N.E.2d 215, 217–218 (1984); State v. Oquist, 327 N.W.2d 587 (Minn.1982); People v. Whotte, 113 Mich.App. 12, 317 N.W.2d 266 (1982); Commonwealth v. Minton, 288 Pa.Super. 381, 391, 432 A.2d 212, 217 (1981); State v. Schultz, 388 So.2d 1326 (Fla.App.1980); People v. Huddleston, 38 Ill.App.3d 277, 347 N.E.2d 76 (1976); Willis v. State, 518 S.W.2d 247, 249 (Tex.Crim.App.1975); Smith v. State, 510 P.2d 793 (Alaska), cert. denied, *43 414 U.S. 1086, 94 S.Ct. 603, 38 L.Ed.2d 489 (1973); State v. Fassler, 108 Ariz. 586, 592–593, 503 P.2d 807, 813–814 (1972); Croker v. State, 477 P.2d 122, 125–126 (Wyo.1970); State v. Purvis, 249 Ore. 404, 411, 438 P.2d 1002, 1005 (1968). But see State v. Tanaka, 67 Haw. 658, 701 P.2d 1274 (1985); People v. Krivda, 5 Cal.3d 357, 96 Cal.Rptr. 62, 486 P.2d 1262 (1971)).

such as the police, to do so."[110] As a result of "having deposited their garbage 'in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it,'", the Court found that the defendants had no reasonable expectation of privacy in the inculpatory items they threw out in the trash.[111]

In *United States v. Knotts*, the Supreme Court similarly held that "A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." [112] The rationale for the Court's reasoning is that when a person travels on public streets he voluntarily conveys "to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property."[113] Courts' quick embrace of privacy waivers was bluntly typified by Judge Sciarrino in his decision rejecting any privacy interest in posts made on the social media service Twitter.[114] The judge wrote "If you post a tweet, *just like if you scream it out the window*, there is no reasonable expectation of privacy. There is no proprietary interest in your tweets, which you have now gifted to the world."[115]

The idea of waiver also guides "notice and choice" and consent frameworks that justify many different kinds of data processing, including both nicks and chops.[116] As once interpreted by the FTC under its Unfair and Deceptive Trade Practices authority, this has meant that consumers

---

[110] *Id.*

[111] *Id.* (citing United States v. Reicherter, 647 F.2d 397, 399 (3d Cir. 1981)) (emphasis added).

[112] United States v. Knotts, 460 U.S. 276, 281-82 (1983).

[113] *Id.*

[114] People v. Harris, 949 N.Y.S.2d 590 (Crim. Ct. 2012).

[115] *Id.* (emphasis added). Though for those that study modern electronic surveillance, the notion of emails and direct messages as "private" might be so dubious as to elicit a snicker.

[116] Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461 (2019); Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROT. L. REV. 423 (2018); Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020); Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOY. L. REV. 101 (2019).

are presumed to have consented (and thus waived objections) to data practices as long as there has been some kind of "notice" to the consumer about what is happening and some kind of "choice" about whether they want it to happen.[117] The guiding rationale behind notice and consent regimes is that so long as a company provides people with essential information about how their information will be used and offers a basic level of choice to accept or refuse a service, privacy due diligence is met. 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.

Unfortunately, waiver and consent also operate to legally justify activities that remain intrusive because the consent is not informed, incomplete, or ineffective at mitigating the sting of the activity.[118] For example, people famously do not and cannot at scale read the terms of use and privacy policies of all the apps they use, yet they still click the "I Agree" button.[119] While "clicking and cringing" can seem reasonable given the limited options available, it will not do enough to blunt the negative impact of invasive technologies.[120] Indeed, in mediated environments, our choices are constrained and engineered by the user interfaces.[121] Control over personal information is impossible at scale because the sheer amount of information and labor necessary for the exercise of binary "take it or leave it" choices to even approach providing agency overwhelms people and, in

---

[117] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), https://www.ftc.gov/sites/default/files/documents/reports/federaltrade-commission-report-protecting-consumer-privacy-era-rapid-changerecommendations/120326privacyreport.pdf. We note, however, that the FTC has recognized that his strategy is not adequate to protect consumers.

[118] Richards & Hartzog, *supra* note 116.

[119] *See* Selinger & Hartzog, *supra* note 116; NANCY S. KIM, WRAP CONTRACTS: FOUNDATIONS AND RAMIFICATIONS (Oxford Univ. Press 2015); MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (Princeton Univ. Press 2013); Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 6 (2011); Woodrow Hartzog, *The New Price to Play: Are Passive Online Media Users Bound by Terms of Use?*, 15 COMMC'N L. & POL'Y 405 (2010).

[120] *See* Nancy S. Kim, *Clicking and Cringing*, 86 OR. L. REV. 797 (2007).

[121] WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (2018).

reality, leaves them few options.[122] We all eventually relent. Consent regimes fail to interrogate whether consented-to activities remain a nick. They do not consider effect that nicks have on the consenting individual, third parties, and society as a whole. This is to say nothing of the fact that rote, uniformed, and formalistic consent is not meaningful.

In order for consent to data and surveillance practices to be knowing and voluntary, at least three 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.[123] In previous work, we have argued, "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."[124]

C. Proximity Focus

Finally, the law ignores nicks due to its focus on two different kinds of proximity: a self-oriented focus (not downstream effects on others) and a focus on discrete and immediate actions (not a series of actions over time). The self-oriented focus of the law helps normalize surveillance practices by ignoring the effect that a person's exposure to surveillance and data practices can have on third parties. The focus on discrete actions instead of a series of actions over time helps normalize surveillance by

---

[122] Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROT. L. REV. 423, 429 (2018).

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

[124] Selinger & Hartzog, *supra* note 116, at 116.

diluting the aggregate potency of nicks by evaluating them in isolation and without reference to systems and structures.

First, let us consider privacy law's self-oriented focus. Most privacy laws are narcissistic. They are preoccupied with how particular surveillance and data practices can harm the person being watched or whose data is being processed. Data protection regimes are built around the concept of informational self-determination. It is the data subject, not third parties, who get to control their own data destinies. Notice, choice, and consent regimes seek to mandate disclosure of all the risks that are relevant to the person clicking the "I Agree" button. Warrant requirements are focused on whether the person targeted has a reasonable expectation of privacy in *their* persons, papers, or effects. Almost every aspect of privacy is law is designed to force people to contemplate the questions "what is in it for *me*" or "what is the worst that can happen to *me*?"

But our actions are far too interconnected to justify this myopic focus on the self. Companies leverage people's data to refine their searches and teach their systems to use their tools more efficiently and harmfully on other people. And even when people or governments approve of surveillance and data practices because they do not jeopardize one person's privacy, those practices can be seen by others and can become common over time, imperiling a future person's expectation of privacy in those same practices.

Consent is inherently individualistic. But our actions have impact on others like never before. The law has done a poor job of recognizing when people waive their own privacy rights, it has an impact on others.[125] People adversely affected by the consent of others to data practices are often members of more vulnerable and marginalized communities than the person waiving their rights. In other words, as we have argued, "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.... In practice, this means if citizens are not members of minority communities, they might not be sufficiently concerned with how their gain from facial

[125] *See* Salome Viljoen, *A Relational Theory of Data Governance*, 131 YALE. L. J. 370 (2021).

recognition comes at other people's expense."[126] We argued that this dynamic would normalize harmful practices, because "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."[127]

Tort law is also inherently individualistic. Negligence is assessed on the basis of whether the individual defendant's conduct met or deviated from the required standard of conduct. Moreover, in terms of causation, actual causation requires showing that the individual defendant's conduct, not someone else's, was a necessary link in the chain of events that caused the plaintiff's harm. For example, "but for this defendant's conduct, defendant would not have been harmed." All of these requirements contribute to the fact that the law is constructed to overlook the possibility that harms may be felt by the collective, rather just individuals themselves, and risk can be created by many actors, not just the indispensable parties in causal chains of harm.

Privacy laws also focus on the individual at the expense of a collective. For example, California's privacy law, California Consumer Privacy Act (CCPA) and subsequently, its California Privacy Rights Act (CPRA), grant its residents the right to request, correct, and/or request deletion of their personal information held by a company, subject to certain exceptions. As for the right to request deletion, the CCPA provides that consumers "… have the right to request that a business delete any personal information about the consumer *which the business has collected from the consumer* [emphasis added]."[128] A similar right to deletion, often referred to as "the right to be forgotten," is granted under EU's GDPR. However, these rights are problematic as they put the onus on the individual to monitor organizations in order to ensure their information is accurate and complete.[129] Moreover, businesses are allowed to deny a deletion request in certain circumstances. Therefore, the individual must be aware of a

---

[126] Selinger & Hartzog, *supra* note 116, at 119.

[127] *Id.*

[128] Cal. Civ. Code § 1798.105 (2020).

[129] Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. (forthcoming 2023). *But see* Margot E. Kaminski, *The Case for Data Privacy Rights (Or 'Please, a Little Optimism')*, 97 NOTRE DAME L. REV. REFLECTION 385 (2022).

business' legal obligations and attempt to verify when these conditions are truly met.

HIPAA violations and time periods for filing complaints for alleged violations also pose problems for being able to adequately address privacy nicks. HIPAA requires that individuals file a complaint with the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) for alleged HIPAA violations within "180 days of when you knew that the act or omission complained of occurred."[130] This focuses on the immediate harm felt by the individual but does not address the smaller harms that are felt collectively and may take longer to materialize.

State breach notification laws may also ignore smaller privacy violations through their notification requirements. Most state breach notification laws only require notification to individuals whose personal information has been compromised rather than to larger groups of individuals who may have also been affected. This requirement of notification to only particular, and often small group, of individuals, disregards the reality that such unauthorized use or disclosures of personal information may also affect others associated with that individual (spouses, children, parents, etc.).

Privacy law is also generally atomistic. That is, nearly every rule looks to the immediate impact of a single individual or organization's discrete actions on people's privacy. Whereas privacy's self-interested focus is inward-looking, asking individuals to look out for themselves, its atomistic focus results in a very limited and proximate view of possible upstream wrongdoing and downstream consequences. Judges and other government actors ask whether specific requests for information or deployment of tools on a particular date and time constitute a "search" or otherwise trigger privacy concerns. However, they less frequently interrogate patterns of searches or procurement of surveillance technologies and relationships with third-party vendors as contributing factors to violations of surveillance laws. When deciding tort claims of privacy, judges typically look to the immediate harm to a plaintiff resulting

---

[130] *How to File a Health Information Privacy or Security Complaint*, OFF. FOR CIV. RIGHTS (last updated Dec. 23, 2022), https://www.hhs.gov/hipaa/filing-a-complaint/complaint-process/index.html.

from a defendant's specific disclosures or collections of information like isolated posts on social media or particular photos taken by one individual of another. But judges frequently fail to interrogate whether a practice is widespread enough to make a societal footprint and the cumulative effect of many different individual actions, like the viral sharing of a mildly embarrassing video that makes people a prominent target for online shaming. This atomistic focus limits the scope of inquiry because only those isolated actions that pass the threshold required to affect people on an individual level significantly will trigger scrutiny. Privacy nicks rarely raise such scrutiny and, as such, proliferate in part due to the law's atomized focus.

III. THE HARM FROM NICKS NORMALIZING SURVEILLANCE

This part examines the fallout from lawmakers overlooking privacy nicks. First, privacy nicks normalize surveillance in a way that undermines our autonomy. Second, lawmakers guarantee our expectations of privacy will be perpetually eroded. With no clear value-based backstop, society's ongoing exposure to privacy nicks creates a slippery slope trajectory for perpetually eroding resistance to the gradual diminution of structural protections and practical costs of surveillance. The end-point of the slope is a transparent society. People living in that future will be deprived of crucial avenues for human flourishing. Consequently, failing to take privacy nicks seriously is fundamentally a problem of intergenerational justice that ensures future generations will have little to no obscurity. Finally, normalizing surveillance will gradually but inevitably and completely disempower people, depriving them of the ability to resist event any privacy invasion through democratic accountability and surveillance countermeasures.

A. Distorting and Bypassing Critical Reflection

Our ability to act freely is often limited by internal and external constraints. Nevertheless, the idea of personal autonomy remains essential to the structure of U.S. law and Western conceptions of the good life.[131] The law's failure to recognize and respond to privacy nicks creates conditions for autonomy harms to occur. Specifically, the mundanity of privacy nicks

[131] BRETT FRISCHMANN & EVAN SELINGER, RE-ENGINEERING HUMANITY (Cambridge Univ. Press 2018); BEATE ROESSLER, AUTONOMY: AN ESSAY ON THE LIFE WELL-LIVED (2021).

can both distort and bypass our ability to critically reflect upon the danger of exposure. To clarify the distortive and invisible effects of privacy nicks, this part begins by explaining what the normalization of surveillance entails. By clarifying how surveillance becomes normalized, we can better explain how normalization dynamics preconsciously shape our beliefs about privacy and dispositions towards protecting privacy in ways most people are unaware of.

There are several causes of surveillance becoming normalized. Some of them have to do with economics, legal, and social factors. When privacy protections are weak, the infrastructure for conducting surveillance makes it possible for agents of the state and private corporations to expand their power in an unprecedented manner. As is widely noted, all around us, in public and private spaces, the number of cameras and sensors is growing. The expansion of cameras is happening alongside a growing societal dependency on online, data-intensive interactions. The transaction costs are greatly diminishing for capturing, aggregating, analyzing, sharing our personal information and acting upon it. Such costs are set to further decline because so-called "smart" systems saturated with artificial intelligence have the potential to significantly enhance the power and efficiency of automated surveillance activities. Under these circumstances, the following factors *predictably lead to surveillance becoming so deeply normalized as an essential component of 21st century life that it perpetually expands*:

1. strong incentives for conducting surveillance across all major sphere of life;
2. decreased financial, financial, time costs for upgrading surveillance tools;
3. deep regulatory gaps in privacy law, including the U.S. trend to prioritize limiting data use over data collection;
4. ongoing secrecy that prevents the public from being well-informed about surveillance activities despite tenacious reporters, litigators, and commissions aiming for transparency;
5. disproportionate surveillance harms being inflicted on people of color, members of the LGBTQ+ community, and other marginalized

communities that the majority of a population don't regularly consider, due to the dynamics that fuel privilege and heightened self-concern;

6. emergencies, like terrorist attacks and public health crises, creating justifications for temporary surveillance measures that end up creating enduring legacies;

7. surveillance advocacy and salesmanship that promote privacy myopia by making it far easier for people to perceive the touted immediate benefits of surveillance than the medium and long-term societal harms.[132]

Other causes of surveillance becoming normalized are psychological. Psychologists have made interesting discoveries about exposure that potentially add additional reasons to expect surveillance creep to be continually normalized. Research on the "mere exposure effect" suggests repeated exposure to something (e.g., physical things, people, ideas, et cetera) creates a sense of familiarity that arbitrarily increases positive evaluations of them.[133] For example, just sitting next to people without conversing with them can motivate you to like them more than the strangers across the room. Similarly, research on the "illusory truth effect" shows that repeated exposure to a false claim can, by itself, increase the perception that claim is true.[134] Two normalization dynamics that revolve around repeated exposure, "unexceptional habituation" and "favorably disposed normalization," might also play important roles in shaping how people view surveillance.

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.[135] Just as it has become an unremarkable occurrence in the digital age that people to communicate over text messages, write school assignments and business reports on computers,

---

[132] Evan Selinger & Judy Rhee, *Normalizing Surveillance*, 22 N. EUR. J. PHIL. 49 (2021); *see also* ARI EZRA WALDMAN, INDUSTRY UNBOUND (2021).

[133] Robert B. Zajonc, *Attitudinal Effects of Mere Exposure*, 9 J. PERSONALITY & SOC. PSYCH. 1 (1968).

[134] Gordon Pennycook et al., *Prior Exposure Increases Perceived Accuracy of Fake News*, 147 J. EXPERIMENTAL PSYCH. 1865 (2018).

[135] Selinger & Rhee, *supra* note 132.

and navigate with the assistance of human-sounding automated GPS systems, so too has it become commonplace to install cameras widely and a massive amount of consumer electronics and online applications to run on vast troves of personal data. From an external perspective, most of the people around seem unconcerned about the possibility of bad actors, like authoritarian leaders or even more ruthless corporations, brazenly abusing the infrastructure. Of course, the seeming indifference might be a façade or explained by other attitudes. For example, if someone believes they lack the agency to make meaningful choices about when and how surveillance is conducted, it is reasonable for them to stoically accept there are things they cannot control.

While privacy scholars have not studied unexceptional habituation as prominently as other issues, they have analyzed a related issue: how social media affordances elicit habitual disclosures. In one study that examines how "young people" regain a sense of comfort after experiencing trust violations on social media, the authors conclude core aspects of social media design—such as personalization, quantified engagement metrics, and interfaces encouraging constant updating and refreshing—incentivize "habitual and repeated…engagement…which…reduces awareness of the intense surveillance of the platform."[136] From this perspective, at least one demographic finds it uncomfortable to focus on surveillance problems, even when a spotlight is shined on them. This outcome arises because pausing to consider the issues creates "friction" that disrupts "their otherwise seamless routines of connection through the platforms".[137] In other words, social media companies do more than allow people to exchange information. They actively shape how users feel, what they desire, and what behavioral patterns they adopt. Such a profound intervention into the cognitive and affective dimensions of mind arguably is a literal re-engineering of our humanity.[138]

The psychological dynamic of *favorably disposed normalization*, whereby the routine experience of being surveilled inclines people to view

---

[136] Clare Southerton & Emmeline Taylor, *Habitual Disclosure: Routine, Affordance, and the Ethics of Young Peoples Social Media Data Surveillance*, SOC. MEDIA & SOC'Y, Apr.-June 2020, at 1, 7.

[137] *Id.* at 8.

[138] *Id.*

surveillance as acceptable, if not desirable, might significantly influence what people believe is appropriate privacy policy.[139] To be sure, questions remain about whether this dynamic exists, how widespread it is, how deeply it impacts the mind, and the extent to which it generalizes across contexts. Nevertheless, the idea is so intuitively plausible 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 comparable, if not more expansive varieties, after the crises end.[140]

One plausible psychological basis for favorably disposed normalization is the impact of believing something is normal. Thinking something is normal does not necessarily entail a commitment to deeming that thing ethical. Nevertheless, normality judgments often are accompanied by positive affective experiences.[141] For example, imagine someone believes using Facebook is ethically problematic but normal. That person might feel less badly about using Facebook than someone who believes the practice is ethically problematic and abnormal. The difference in how people feel has implications for governance. The person with a stronger felt sense of discomfort might have a greater incentive to quit the platform. After all, people frequently complain about ethical violations. But taking the next step of committed action can require more than intellectual awareness that change is needed. Given the practical value of heightened moral motivation for rectifying injustice, in some circumstances, "beliefs about normality might be more important than moral beliefs".[142]

But how do people develop the belief something is normal? According to experiments conducted by philosophy and cognitive science professor Joshua Knobe and psychology professor Adam Bear, both prescriptive and descriptive information matter if people know how good something is perceived and how prevalent it is. Nevertheless, simply "increasing the frequency of something occurring," such as surveillance

[139] Selinger & Rhee, *supra* note 132.
[140] Selinger & Rhee, *supra* note 132.
[141] Selinger & Rhee, *supra* note 132.
[142] Selinger & Rhee, *supra* note 132.

more becoming more prevalent, can lead people to perceive it as "more normal," not just increasingly widespread.[143] Supporting evidence for this thesis exists in the experimental literature on environmental messaging.[144]

Alternatively, one might explain the dynamic of favorably disposed normalization through the psychological process of rationalization.[145] From this perspective, 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.[146] 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.

People might be driven to rationalize frequently using Facebook because they want to avoid uncomfortable experiences associated with being thrust into an unjust situation. For example, Facebook claims it is free for people to use. But people who follow the news know this is not the best description of the actual cost.[147] One price to pay is fear. Using Facebook leaves one vulnerable to disconcerting surveillance. Additional prices are disappointment and guilt. Using Facebook makes one complicit in perpetuating a surveillance system that harms others. Rationalizing can render inert these unpleasant thoughts and foster positive emotional experiences. Through rationalization, people feel better about finding

---

[143] Selinger & Rhee, *supra* note 132, at 62.

[144] Noah J. Goldstein et al., *A Room with a Viewpoint: Using Social Norms to Motivate Environmental Conservation in Hotels*, 35 J. CONSUMER RSCH. 472 (2008); Robert B. Cialdini et al., *Managing Social Norms for Persuasive Impact*, 1 SOC. INFLUENCE 3 (2006).

[145] Justin P. Friesen et al., *System Justification: Experimental Evidence, Its Contextual Nature, and Implications for Social Change*, 58 BRITISH J. SOC. PSYCH. 315 (2019).

[146] Leon Festinger, *A Theory of Social Comparison Processes*, 7 HUM. RELS. 117 1957.

[147] *See* Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. Rev. 606 (2014).

themselves caught in the distressful circumstance of being bound by a powerful surveillance capitalist company's term of service—terms that highlight a gap between the world they want to live in and the one they actually inhabit.

Two management professors applied rationalization theory to explain behavior like staying on Facebook despite having reservations. In this context, they emphasize the limited social media options available.[148] Due to factors like network effects, the market heavily favors incumbent platforms, such as Facebook, and offers few popular alternatives. The lack of choice makes people feel stuck, unable to live authentically and select options that reflect their values. Rationalization is useful here; it helps people feel better about being dependent on a service widely associated with unpopular values, like greed, manipulation, and exploitation.

The mind can easily rationalize staying on Facebook even during cultural moments of backlash against the company due to the following factors. First, people are frequently told privacy is declining or dead. Hence, they can convince themselves escaping surveillance is impossible. Privacy fatalism bolsters rationalization. It justifies the belief it is better to benefit from being surveilled on services like Facebook than to be a sucker—someone constantly monitored by government and private actors who do not capitalize on the maximum benefit inescapable datafication provides.[149] Second, it is easy for people to convince themselves that privacy is overrated. Privacy harms are more challenging to grasp than the benefits platforms like Facebook provide.[150] Furthermore, platforms like Facebook design their interfaces to nudge users away from thinking about the data collection and processing occurring on the back end.[151]

Other psychological theories might explain favorably disposed normalization. Here are two of many possible examples. According to self-perception theory, people often benefit from forming convincing narratives

---

[148] Nathanael J. Fast & Arthur S. Jago, *Privacy Matters…or Does It? Algorithms, Rationalization, and the Erosion of Concern for Privacy*, 31 CURRENT OP. PSYCH. 44 (2020).
[149] Fast & Jago, *supra* note 148.
[150] Fast & Jago, *supra* note 148.
[151] Fast & Jago, *supra* note 148.

of their own behavior after introspecting to find their inner motives.[152] Although introspection feels like reviewing the contents of one's mind, it often fails to render transparent the mind's opaque processes. Hence, introspection is an unreliable method for acquiring self-knowledge. But rather than admit introspection does not reveal underlying mental states, the mind comes up with self-serving stories that resemble Jonathan Haidt's popularized definition of rationalization. He compares it to a vigilant "press secretary" keen to "praise or defend" our behavior.[153]

The theory of rationalization as representational exchange expands upon this classic insight into the biases of self-examination.[154] From this perspective, which focuses on how people interpret their own behavior to try and better understand themselves, three processes are essential. First, people act unsure of what, exactly, is motivating them. Second, people introspectively infer what their motivating beliefs and desires are and convince themselves they were spurred on by good ones. Finally, they explicitly adopt their presumed beliefs and desires and use them as guides for making future decisions. Due to adaptive dynamics, the explanations can lead to positive outcomes, even though they are fictional and do not capture the underlying catalysts. From this perspective, someone might convince themselves that staying on Facebook is essential to maintain valued connections, even if that's not the real reason. Perhaps they continually log on because they are motivated by the dopamine rush triggered by having their posts liked.

Additional psychological research is required to understand normalization dynamics in a privacy context. Unfortunately, the ideal studies are longitudinal. Consequently, they will take time to conduct. If the law waits for more research before addressing nicks, it risks permitting normalization to go too far. In our opinion, the various explanations of how the normalization of surveillance can occur suffice to show that the law's

---

[152] Daryl J. Bem, *Self-Perception Theory*, 6 ADVANCES EXPERIMENTAL SOC. PSYCH. 1 (1972).

[153] JONATHAN HAIDT, THE RIGHTEOUS MIND: WHY GOOD PEOPLE ARE DIVIDED BY POLITICS AND RELIGION 92 (Vintage 2013).

[154] Fiery Cushman, *Rationalization is Rational*, 43 BEHAV. & BRAIN SCIS. 1 (2020).

failure to regulate surveillance normalization through privacy nicks creates the conditions for autonomy to be routinely compromised.

First, in cases where the incentives for ongoing surveillance are high, the benefits of surveillance are easy to understand (e.g., convenience and safety), and non-concrete surveillance harms surveillance are hard to grasp (e.g., conformity through chilling effects), people will find it hard to make informed decisions about what privacy-protecting restrictions to enact. The reason for this cognitive hardship is that it is far too easy to underestimate how easily surveillance creep can occur and to overestimate the likelihood of implementing effective governance procedures once the creep goes too far. While scholars write about the causal power of things like technological affordances and lock-in effects, there is no reason to believe the average person or the typical regulator living in a free society that prizes a free-market economy and valorizes innovation will be inclined to look at privacy risks through these prisms. This outcome is especially likely in a society that widely deems slippery slope claims to be fallacious. In short, social biases prevent citizens from making informed decisions about privacy that corresponds to values they hold dear.

Consider the following thought experiment about the hypothetical future of elementary school education. Capitalizing on the enthusiasm for using fitness trackers in gym class to monitor students' heart rates and the number of steps they take, a school introduces a pilot program to improve mental fitness. Deploying new technology developed for the classroom, teachers start monitoring students' brain activity. At first, they only use the neural data for one purpose, to better assess student engagement. But after test scores improve and other schools replicate the initiative, it introduces a new program. This time, students receive comprehensive brain scans, and the data feeds into a machine-learning system designed to enhance personalized instruction. As time progresses, the momentum for neuro-education continues, and more expansive approaches roll out.

Normalization, mission creep, and other closely related factors could lead actual schools to follow this trajectory in the real world. Indeed, the spark of inspiration might already have been lit. Presently, BrainCo, a startup company, markets a headband that allegedly identifies when students are concentrating based on their brain signal activity with the slogan, "It's like a heart-rate monitor for your mind," and schools in the

United States and China have begun testing it.[155] Given the potential for an ongoing slippery slope, one that might yield educational benefits and is fraught with highly invasive privacy pitfalls, parents, teachers, and administrators should consider potential long-term impacts when deciding whether schools should equip all students with technologies like Fitbits. Unfortunately, without a scholarly understanding of normalization dynamics and nicks, they lack the tools to critically consider the possible slippery slope and identify and assess salient costs and benefits.

Second, when dynamics of favorably disposed normalization or rationalization occur, people's beliefs and dispositions about surveillance are shaped by psychological mechanisms that appear below their level of conscious awareness. This form of persuasion means people are blind to the hidden influences that re-engineer their privacy outlooks. As a result, "people tend to form beliefs about surveillance under one of two conditions: either without having any reason for developing the beliefs or without having a good reason for developing them."[156] In short, to prevent the psychological mechanisms that fuel normalization from undermining autonomy and intensifying surveillance, psychological research needs to be better integrated into privacy law. Also, further psychological research into the normalization of surveillance urgently needs to be conducted.

B. Constantly Eroding Expectations of Privacy

By failing to recognize nicks, the law allows society to constantly renegotiate expectations of privacy without the protection of a firm backstop. When nicks proliferate unchecked, the nick and the chop work together to create a vicious inevitability cycle - companies that want to profit by engaging in obscurity-corrosive behavior use the fact that we have been normalized to a certain degree of loss of obscurity by a thousand nicks to engage in a "chop" that is unchallenged. The chop sets the new floor and

---

[155] Bryan Walsh, *Elon Musk's Neuralink Wants to Read Your Brain*, AXIOS (Aug. 29, 2020), https://www.axios.com/2020/08/29/elon-musk-neuralink-brain-computer-interface; Paula Ebben, *Catholic Memorial Students Use Headbands to Harness Brainpower*, CBS NEWS (Dec. 16, 2019, 5:35 PM), https://www.cbsnews.com/boston/news/catholic-memorial-brainco-headset-technology/; Jane Li, *A "Brain-Reading" Headband for Students Is Too Much Even for Chinese Parents*, Quartz (Nov. 5, 2019), https://qz.com/1742279/a-mind-reading-headband-is-facing-backlash-in-china.

[156] Selinger & Rhee, *supra* note 132, at 67.

the nicks gradually reaching deeper than ever before continue to proliferate. This situation sets up the next big chop, which will also meet less resistance due to the proliferation of nicks. And so, the cycle continues. By ignoring privacy nicks, the law *facilitates* the inevitability cycle of increasingly invasive surveillance.

People are endangered and made worse off when their expectations of privacy are being consistently eroded. They become less likely to speak out and engage in important expressive activities. Neil Richards wrote, "surveillance threatens the intellectual privacy we need to think, read, and communicate with others so we can make up our minds about political and social issues. Just as surveillance can drive our identities to the mainstream, being watched when we think, read, and communicate can cause us not to experiment with new, controversial, or deviant ideas."[157] Julie Cohen has explored over a large body of work how privacy is essential for the process of identity formation, because it provides breathing room though boundary management for us to explore, play, and figure out who we are, who we want to be, and how we relate to everyone else.[158]

Cohen's work on configuring the networked self is critical to understand the danger from constantly eroding expectations of privacy. To Cohen, "The self has no autonomous, precultural core, nor could it, because we are born and remain situated within social and cultural contexts. And privacy is not a fixed condition, nor could it be, because the individual's relationship to social and cultural contexts is dynamic."[159] Therefore expectations about the world around us, particularly how exposed we are, who might be watching, and what their intentions might be, are major forces defining (and likely constraining) our ability to flourish as humans. Privacy nicks will continue to slowly chip away at our breaching room for self-exploration until we are completely deprived of space.

---

[157] RICHARDS, *supra* note 26, at 134.

[158] JULIE E. COHEN, CONFIGURING THE NETWORKED SELF (2014); Julie E. Cohen, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (2019); Cohen, *supra* note 90; Julie E. Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQUIRIES L. 1 (2019).

[159] Cohen, *supra* note 90, at 1908.

C. A Disempowerment Death Spiral

When governments and organizations gain power through surveillance, people increasingly lose the ability to resist that surveillance through countermeasures and democratic means. In this article, we have agreed with the many scholars who have argued that privacy is about power.[160] Neil Richards wrote that human information is power because it "confers power over the very humans from whom it is collected by powerful entities. It gives those entities that amass and exploit human information economic, social, and political power, in ways that are magnified by preexisting power asymmetries."[161] In other words, privacy nicks dampen our ability to resist surveillance not only through psychological invisibility as argued above, but also through power disparities.

When people are exposed, they are vulnerable to the watchers. Richards wrote that "the power of personal information lies at the heart of why surveillance happens and how its products are used. The power effects of surveillance illustrate three additional dangers of surveillance beyond its threat to intellectual privacy: *blackmailing and discrediting*, *discrimination*, and *persuasion*." With every exposure, the consequences for resistance get incrementally greater. Countermeasures such as obfuscation and sousveillance ("watching the watchers") become more dangerous given how vulnerable people become through surveillance to blackmailing, discrediting, discrimination, persuasion, and the use of government force.[162]

But normalized and pervasive surveillance doesn't just disempower people through negative consequences. The more we are exposed, the less

---

[160] *Id.*; RICHARDS, *supra* note 26; Lisa M. Austin, *Enough About Me: Why Privacy is About Power, not Consent (or Harm)*, *in* A WORLD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO? 131 (Austin Sarat ed., 2014); CARISSA VÉLIZ, PRIVACY IS POWER: WHY AND HOW YOU SHOULD TAKE BACK CONTROL OF YOUR DATA (2021).

[161] RICHARDS, supra note 26, at 50.

[162] For more information on resistance and opposition to surveillance, *see* BERNARD HARCOURT, EXPOSED: DESIRE AND DISOBEDIENCE IN THE DIGITAL AGE (2015); COLIN J. BENNET, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE (2008); FINN BRUNTON & HELEN NISSENBAUM, OBFUSCATION: A USER'S GUIDE FOR PRIVACY AND PROTEST (2015); Laura Huey et al., *Cop Watching in the Downtown Eastside: Exploring the Use of (Counter) Surveillance as a Tool of Resistance, in* SURVEILLANCE AND SECURITY 149 (Torin Monahan ed., 2006); Torin Monahan, *The Right to Hide? Anti-Surveillance Camouflage and the Aestheticization of Resistance*, 12 COMMC'N & CRITICAL/CULTURAL STUD. 159 (2015).

capacity we have for democratic resistance. Julie Cohen has argued that "critical subjectivity shrinks in conditions of diminished privacy," and with it, the capacity for democratic self-governance.[163] According to Cohen, "the liberal self and the liberal democratic society are symbiotic ideals. Their inevitably partial, imperfect realization requires habits of mind, of discourse, and of self-restraint that must be learned. Those are the very same habits that support a mature, critical subjectivity, and they require privacy to form. The institutions of modulated democracy, which systematically eradicate breathing space for dynamic privacy, deny both critical subjectivity and critical citizenship the opportunity to flourish."[164] Richards noted that "surveillance and interference chill activities and beliefs that are dissident, eccentric, or unpopular, driving them toward the boring, the bland, and the mainstream. Government surveillance can also threaten our political freedom by chilling our ability to think, read, or communicate politically unpopular ideas or associate with people who hold those ideas." [165] He argued that "[w]ithout privacy—without a space between our political selves and the always-on notification pings of surveillance-based media—we may never have the time or capacity to think critically about the direction in which our world is heading."

A death spiral is a "a period of continuous deterioration that leads ultimately to catastrophic failure or destruction."[166] If lawmakers and judges continue to ignore privacy nicks, they risk a death spiral for democratic resistance and countermeasures to surveillance because the law has no back stop. Society will become increasingly exposed past the point where meaningful and peaceful resistance is possible.

IV. HOW LAWMAKERS SHOULD RESPOND TO PRIVACY NICKS

This part explores how lawmakers should respond to privacy nicks in order to avoid normalizing surveillance. We propose that lawmakers and judges embrace relationships and collectives, rules shaping the design of

---

[163] Cohen, *supra* note 90, at 1912 ("A society that permits the unchecked ascendancy of surveillance infrastructures cannot hope to remain a liberal democracy.").

[164] Cohen, *supra* note 90, at 1918.

[165] RICHARDS, supra note 26, at 144.

[166] *Death Spiral*, COLLINS DICTIONARY, https://www.collinsdictionary.com/us/dictionary/english/death-spiral (last visited Feb. 26, 2023).

technologies, and targeted bright-line prohibitions. But first, we argue that some other popular approaches aren't a great fit to respond to privacy nicks.

A. What Won't Work

Over the past twenty years, privacy scholarship has flourished with critical and analytical work that explains how privacy law works and where it falls short.[167] Many of these works prescribe approaches and frameworks to help get the right balance between privacy and competing values like security, innovation, or free expression. These proposals are well developed and forward looking. Unfortunately, they do not sufficiently contend with surveillance law's ignorance of the normalizing role played by privacy nicks.

1. Future-Proofing the Law

When considering Fourth Amendment abuses in surveillance, an interesting framing for understanding how surveillance issues might be 'future-proofed' against. Andrew Ferguson inspects *Jones*[168]*, Carpenter*[169]*,* and *Riley*[170] to highlight a "digitally-aware Fourth Amendment and… Supreme Court."[171] Ferguson argues that these cases recognize privacy threats from 'technology-enhanced police surveillance' as something distinctly different from traditional surveillance.[172] Encouraged by this recognition, Ferguson proposed six 'future-proofing principles'[173] that structure an analytical framework by which to review future surveillance technologies.[174] Ferguson theorizes that the more a surveillance technology violates these principles, the more likely the technology "will be seen as

---

[167] *See, e.g.,* Woodrow Hartzog, *What is Privacy? That's the Wrong Question*, 88 U. CHI. L. REV. 1677 (2021); Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087 (2006); Maria P. Angel & Ryan Calo, Privacy After Taxonomy (draft on file with authors); Meg Jones, Karen Levy, Ellen Kaufman & Jessie Taft, Methods to Our Madness: An Interdisciplinary Reflection on 10 Years of Privacy Scholarship (Privacy Law Scholars Conference, 2018) (draft on file with authors).

[168] United States v. Jones, 565 U.S. 400 (2012).

[169] Carpenter v. United States, 138 S. Ct. 2206 (2018).

[170] Riley v. California, 573 U.S. 373 (2014).

[171] Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1132(2021).

[172] *Id.* at 1129.

[173] *Id.* at 1132.

[174] *Id.*

violating a reasonable expectation of privacy," and therefore the more likely it will "be struck down on Fourth Amendment grounds."[175]

These principles thus reflect a desirable set of traits for surveillance technologies that would theoretically fit within a reasonable expectation of privacy. Among the principle are 'anti-equivalence,' which recognizes that 'digital is different' and therefore digitized surveillance is meaningfully inequal to traditional methods; 'anti-aggregation,' which corresponds to Justices Sotomayor and Alito's recognition of harms to individual liberty as a result of at-scale public data collection; 'anti-permanence,' which covers long-term storage and retrievability of collected information; 'anti-tracking,' which highlights concerns over 'associational' freedoms impacted [by] tracking [technologies]; 'anti-arbitrariness,' which 'involves the desire to prevent arbitrary police actions;' and finally 'anti-permeating surveillance,' which represents general worries over pervasive surveillance.[176]

External to Fourth Amendment or law enforcement contexts, these principles, as applied to any emergent technology that advances surveillance, still provide an excellent blueprint by which to judge that technology. When we consider the gap between people's lived privacy experiences today against the privacy laws meant to protect them, we can turn to Ferguson's principles to understand what is necessary to improve protections against surveillance in future years. We want regulations that acknowledge the difference that digital makes (anti-equivalence); we know we need regulations to combat mass data collection (anti-aggregation) and unnecessary longitudinal record-keeping (anti-permanence). We sorely need new understandings of law that limit tracking (anti-tracking) and naturally don't want such technologies to pervade substantial parts of our lives (anti-permeating surveillance). Ferguson's framework is therefore a promising step towards improving how we regulate and approach up-and-coming surveillance technologies.

Future-proofing can certainly help mitigate surveillance problems, but these principles are much better suited to handling privacy chops that harm people quickly and viscerally as opposed to the privacy nicks we

---

[175] *Id.* at 1141.
[176] *Id.* at 1132–1140.

normalize to over time. The anti-permeating principle requires a threshold of scale (though this has yet to be defined by courts) for when something becomes 'too permeating;' this corresponds well to regulating chops, as chops tend towards reaching the sort of scale or *footprint* that captures legal attention (like with Clearview AI). And all six principles are built from Fourth Amendment cases, which are intrinsically quite concerned with *endowments of power*. Ferguson's future-proofing theory is a much-needed framework for regulating surveillance technologies of today and tomorrow.

However, we think it falls short of completion towards that goal. This shortcoming stems primarily from future-proofing theory's dependence on thresholds; to qualify as a Fourth Amendment violation, a technology must be determined as permanent, pervasive, or arbitrary, or must meaningfully aggregate data, store data for long periods of time, or track an individual. Similarly, not all six of the principles need to be violated by a technology for the technology to be determined a Fourth Amendment violation, suggesting that there is a critical mass to reach in terms of how many principles are broken in order to qualify. Thresholds, we find, are part of the law's blind spot with regards to effectively regulating surveillance technologies. When a threshold of severity is required to consider a privacy encroachment worthy of legal action, we fail to account for the unidirectional nature of privacy erosion.

Lawmakers and court justices use technologies in their day-to-day lives like all of us to. Their assumptions about what is an egregious privacy violation will be shaped by public norms set by the current level of technological advancement. Unlike a layperson, however, a regulator seeking to curb the growth of surveillance technologies must be cognizant of how shifting norms push the collective 'comfort zone' or window. As an example how easy it is for nicks to flourish in threshold-based frameworks, consider situations where lawmakers are compelled 'temporarily' disregard futureproofing principles. We recently lived through (and are still living through) one: the COVID-19 pandemic. Governments and private companies around the world scrambled to build tools that in any other case would have been egregiously invasive and might have garnered legal scrutiny. Infection information was integral to saving lives and 'stopping the spread.' People surrendered data they likely would

have been less willing to give to governments pre-pandemic. Such health technologies offer an interesting example of how surveillance technologies are 'allowed' or even encouraged to proliferate.

Throughout the pandemic, governments were forced to make decisions and create solutions that attempted to balance the trade-offs between public health and citizens' privacy. While health tracking apps were rolled out at-scale, with vast footprints, significant endowments of power to governments and greatly reduced transaction costs in collecting critical infection data, the public health crisis did not necessarily warrant shifting people's privacy sensitivities into a 'new normal' of mass surveillance. People installed these apps and placed trust in their governments, and the law did not prevent the dissemination of public health technologies for the purpose of defeating COVID-19. Compared to the reaction to Clearview AI, the law was largely silent – if there were privacy thresholds to be met, the conditions of the global pandemic overrode them. And yet these technologies would violate most of the future-proofing principles; they aggregated vast quantities of tracking data and permeated throughout civil society. While the motivation for these surveillant technologies was not arbitrary, the pandemic-necessary features of these tools would be extremely concerning out of a life-saving context.

As the crisis improves, such technologies (which would otherwise be seen as chops worthy of legal attention) risk becoming normalized if nothing is done to shut them down. Toronto Star writer Bianca Wylie discusses three types of 'democratic harms' resulting from the government of Canada's failure to sunset a nationwide COVID alert app following the cessation of public access to PCR tests.[177] The first describes the potential of a government to escape accountability by failing to 'publicly communicate' when the app might be shut down (and additionally following through with shutting the app down).[178] The second discusses

[177] Bianca Wylie, *Health Canada Needs to Shut Down the COVID Alert App*, THE TORONTO STAR (April 25, 2022), https://www.thestar.com/opinion/contributors/2022/04/25/health-canada-needs-to-shut-down-the-covid-alert-app.html.

[178] *Id.*

how the normalization of invasive technologies incorporates them into 'digital public infrastructure,' and the third highlights further reduction of trust in the technologies that might actually be beneficial for citizens.[179] These 'harms' offer two main insights: firstly, privacy law's overreliance on legal thresholds for individual harms undervalues other harms that are yet to be clearly identified within regulation and fails to appreciate how such nicks and smaller privacy encroachments aggregate towards larger, collective privacy harms.

2. "Reasonable Expectations of Privacy"

The most popular test for identifying legal surveillance violations is whether a watcher has violated an observed person's "reasonable expectation of privacy."[180] This test was enshrined with Justice Harlan's concurring opinion in *Katz v. United States* in 1967 and has since become the polestar for privacy protections in tort law and a host of statutes and regulations.[181] Unfortunately, privacy nicks ensure that the "reasonable expectations" test is doomed to fail. While there is explicit normative value in aspiring to meet the ideal of reasonableness, the problem is that threshold set by this test is reliant upon norms and people's expectations. When those expectations are incrementally but inevitably whittled away, the debate over what reasonable people should believe in context doesn't matter. In the long term, surveillance will win.

Widely shared practices and beliefs are a poor calibration point for impartial and fair privacy rules.[182] Lawmakers hitching surveillance rules exclusively to norms can lead to well-known problems, such as embracing moral relativism and believing it is permissible to violate fundamental human rights if one happens to live in a society that routinely ignores, demeans, or disregards these principles. Indeed, one might be able to avoid

---

[179] *Id.*

[180] Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. Rev. 1511, 1511 (2010).

[181] Katz v. United States, 389 U.S. 347, 389 (1976) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

[182] *See* Karen Eltis, *Can the Reasonable Person Still Be 'Highly Offended'? An Invitation to Consider the Civil Law Tradition's Personality-Rights Based Approach to Tort Privacy*, 5 UNIV. OTTAWA L. & TECH. J. 199 (2008).

committing the naturalistic fallacy by understanding the ideal of reasonable expectations with sufficient nuance. Simply because some behavior is commonly presumed to be good or acceptable does not necessarily mean it should be considered normatively justified.

To illustrate, consider an example concerning privacy from George Orwell's *1984, a* novel that functions as shorthand dystopian reference for talking about an authoritarian society powered by panoptic government surveillance. Within the Orwellian narrative, how should we understand protagonist Winston Smith's decision to keep a journal that includes ideas the government finds sufficiently subversive to be punishable offenses? Although Smith should have anticipated getting caught for committing "thoughtcrimes" because privacy is effectively dead in his society, according to one philosophical account his desire to document his ideas nevertheless remains reasonable. In other words, even in a police state where privacy preferences are taboo, and individuals realize there are no effective techniques for preventing government snooping, it nevertheless remains reasonable to reject the government's total incursion on what Julie Cohen has called the breathing room necessary for human flourishing.

> Given the nature of his society, he [Smith] could not realistically expect that no one would ever find his journal. Although he might hope to evade discovery, he certainly realizes that the probabilities are high that whatever he writes will be read by the authorities and that he will be duly punished for this breech…In such cases we should *not* say there is nothing reasonable about Winston's desire to be able to freely write his most personal thoughts in a private fashion: a reasonable person *should* be able to expect privacy from his journal. The mere likelihood of discovery (or certainty in Winston's case) does not eliminate a fundamental right of privacy.[183]

The key to claiming Winston should be entitled to limit who has access to his intimate thoughts is to characterize his desire as reasonable based on substantive principles his society does not recognize as valid, such as human rights. Unfortunately, within Fourth Amendment law, the idea of "reasonable expectations of privacy," one that provides a check against

---

[183] Robert McArthur, *Reasonable Expectations of Privacy*, 3 ETHICS & INFO. TECH. 123, 125 (2001).

unreasonable government searches and seizures, is not primarily based on substantial principles that guarantee society is free and operational as surveillance technologies become more powerful and more thoroughly integrated into daily life. For example, in *Katz*, the defendant met the reasonable expectation standard by conducting illegal activity in a telephone booth whose booth door he closed to prevent outsiders from listening in. Closing the door demonstrated the intention to conduct a private conversation. By the early 1960s, closed-off telephone booths located in public areas customarily were understood as locations that society deemed reasonable places to communicate discreetly. But the more we expose ourselves, the more we are deemed to have waived or consented to being watched, even when the truth is there simply are fewer places for solitude and seclusion.[184]

There are two fundamental problems with the *Katz* test. First, the test fails to consider how easily subjective expectations about privacy degrade. Matthew Tokson and Ari Waldman have compellingly claimed that judges in Fourth Amendment cases have adopted the mistaken belief that norms can be permanently settled—what they refer to as the closure principle.[185] Treating norms as static ignores how they change and are constantly being contested. Governments can accelerate a degradation of a subjective expectation of privacy through the exercise of power. Anthony Amsterdam goes so far in 1974 as to insist "an actual subjective expectation of privacy obviously has no place…in a theory of what the Fourth Amendment protects."[186] To illustrate the problem, he constructs a hypothetical, Orwellian scenario. "[T]he government could diminish each person's subjective expectation of privacy merely by announcing half-hourly on television that 1984 was being advanced by a decade and that we were all forthwith being placed under comprehensive electronic surveillance."[187] By today's standards, such blunt and dramatic government action seem unnecessary. As we argued in the discussion of nicks, mundane

---

[184] *See, e.g.,* Woodrow Hartzog, *The Public Information Fallacy*, 99 B.U. L. REV. 459 (2019).

[185] Matthew Tokson & Ari Waldman, *Social Norms in Fourth Amendment Law*, 120 MICH. L. REV. 265 (2021).

[186] Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974).

[187] *Id.*

normalization dynamics appear to be re-engineering beliefs about privacy through dynamics that lead people to become more favorably disposed to surveillance or resigned to it occurring.

Indeed, Justice Stevens makes this point in the dissent to *Kyllo v. United States*.[188] In this case, the majority opinion determined the although the police did not enter a home, they still searched it through the warrantless use of a thermal imaging device deployed to detect the presence of marijuana. Notably, Justice Scalia suggested it is not reasonable for people to expect the police to search their homes with this technology because the device was not "in general public use" at the time of the ruling. In other words, Justice Scalia articulated the danger of allowing a privacy chop to be legally permissible. Justice Stevens, however, rightly points out that such logic fails to clarify how frequently a technology has to be deployed to qualify for general use. Perhaps more poignantly, he observes that over time many surveillance technologies that begin as cutting-edge and limited to use by early adopters will become democratized and mundane, likely for reasons we discuss in our analysis of normalization. Tokson and Waldman have also noted this problem when looking to social norms to set privacy rules, writing, "Courts relying heavily on social norms may be less likely to regulate invasive uses of familiar and generally accepted technologies."[189]

Despite the Court's attempt to draw a line that is "not only firm but also bright," the contours of its new rule are uncertain because its protection apparently dissipates as soon as the relevant technology is "in general public use." Yet how much use is general public use is not even hinted at by the Court's opinion, which makes the somewhat doubtful assumption that the thermal imager used in this case does not satisfy that criterion. In any event, putting aside its lack of clarity, this criterion is somewhat perverse because it seems likely that the threat to privacy will grow, rather than recede, as the use of intrusive surveillance equipment becomes more readily available.

---

[188] 533 US 27 (2001).

[189] Tokson & Waldman, *supra* note 185, at 301. "Surveillance creep has a subtle yet powerful impact on sociotechnical norms because it normalizes surveillance as ordinary, routine, and expected." *Id.* at 302.

Scalia's reasoning looks surprising when examined considering comments he made in later cases. For example, in Scalia's dissent to *Maryland v. King* he warns that most justices established a precedent for collecting DNA that will lead to an unacceptable outcome over time.[190] According to the majority opinion, police officers with probable cause can procure a DNA sample from someone suspected of committing a serious crime. The Court reasoned those Constitutional protections, specifically those expressed in the Fourth Amendment prohibition against unreasonable government searches, do not prohibit police from swabbing a suspect's cheek any more than they do fingerprinting and photographing them. Scalia found this reasoning unsettling because he believed it failed to draw a firm boundary at the intended threshold. At face value, the current standard might seem straightforward. After all, it only applies to a person suspected of committing a "serious offense." However, Scalia worried the standard is imprecise. Due to vagueness and the possibility of norms shifting over time, he predicted the Court eventually would permit law enforcement agents who lack a warrant to obtain DNA from someone only suspected of minor infractions.

The second problem with the *Katz* test is that it provides little guidance for judges to determine what society should accept as reasonable.[191] This issue is critical since the *Katz* test constructs judges a societal proxy. Focusing on the problem of judges being placed in the challenging position of determining how paternalistic or laissez-faire to be about future surveillance threats, Mathew Tokson and Ari Waldman highlight biases within the law's design that influence judicial reasoning.[192] The scholars highlight how dominant proposal for judges to refrain from taking an interventionist approach by "regulating the government's use of a new surveillance technology until the social norms and practices involving the technology become stable," structurally creates the conditions for surveillance creep to continually occur.[193] More specifically, they contend "by relying on precedents involving older technologies to justify the use of newer, more advanced surveillance, courts unwittingly fall

[190] 569 US 435 (2013).
[191] *See, e.g.*, Solove, *supra* note 180.
[192] Tokson & Waldman, *supra* note 185.
[193] *Id.* at 296.

prey to the normalization effect of surveillance creep in Fourth Amendment cases. That is, courts may focus only on the marginal change to an existing technology, which will often seem anodyne or minimal. That narrow focus obscures the new practice's entire effect on privacy interests. Therefore, courts may allow intense surveillance to escape Fourth Amendment scrutiny."[194] As a result, the legal system predictably facilitates the intensification of surveillance rather than slowing it down. [195]

Scholars have argued that this process begins when certain individual practices or behaviors start being repeated by others in the community, eventually developing into social norms.[196] Norms become custom, which ultimately become enshrined in law.[197] Laws supported by

---

[194] *Id.* Tokson and Waldman show how courts look to norms in their Fourth Amendment jurisprudence. As an example, they discuss how reliance on "customary social usage," will typically permit police officers to enter a house with the permission of only one co-tenant, but if another tenant is present and objects to entry, "commonly held understanding[s] about the authority that co-inhabitants may exercise" will likely not allow the officer to enter because such entry would "violate social norms of propriety." *Id.* at 275.

[195] *Id.* at 272. Tokson and Waldman contend that legally relevant social norms "arise from social practices that are eventually accepted, repeated and routinized over time. When people consider a prevalent social practice to be justified and beneficial, it gains a normative edge, and may be associated with social pressures to comply and information sanctions for non-compliance." *Id.* at 272.

[196] *See* Michael J. Zydney Mannheimer, *Decentralizing Fourth Amendment Search Doctrine*, 107 KY. L.J. 169, 195 (2018). As acceptance and adoption of a social norm spreads, social norms become customs, which are likely ultimately attain the force of law. Mannheimer reasons that the impulse to conform one's actions to dominant norms achieves something close to "consensus," which leads to expectations that norms will be adhered to, in addition to pressures to abide by them and informal sanctions for non-compliance. *See also* CARLTON K. ALLEN, LAW IN THE MAKING 56 (2d ed. 1930) ("In the earliest stages of society, practice plays the greater part and custom grows by the force of concrete example…").

[197] Mannheimer, *supra* note 196. Many scholars believe that judicial intervention also plays a significant role in the shaping of social norms. While some caution that judicial intervention too early may be inappropriate in certain cases were social norms and practices have "not yet reached maturity" (e.g., new technologies that pose Fourth Amendment questions), others feel it is necessary for the law to alter social norms if they diminish well-being (e.g., encourage people to shorten their lives by driving very fast) or autonomy (e.g., discouraging people from becoming educated). In cases where social norms are not yet settled, scholars, and even the courts, believe it is more prudent for courts to wait before "elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." Tokson & Waldman, *supra* note 185, at 159; Cass R. Sunstein, *Social Norms and Social Roles*, 96 COLUMB. L. REV. 909, 910 (1996).

social norms are likely to be more durable and enforceable.[198] This is how, rather than merely becoming regular or habitual, imitation of certain behaviors becomes normative. Furthermore, this process of practice and imitation has been found to be largely automatic and not consciously driven.[199] What's worse is that these norms aren't always rational.[200] Etzioni highlights a common view that norms usually tend to be nonrational:

> Although some group norms appear calculated to further the interests of group members, many group norms seem to be adopted without reflection and appear instead to be driven mainly by imitation and group identification.…No individual has the resources to evaluate thoroughly all of the choices he must make, so by conforming to the status quo he takes advantage of the cumulative wisdom of the community. In effect, he operates on the assumption that existing practices have survived the trial and error test.[201]

As norms are passed down from one generation to the next, they gain their authority and legitimacy from this sense of tradition rather than intentional, individual reflection or consideration.[202] In the end, laws

---

[198] Amitai Etzioni, *Internalization, Persuasion, and History*, 34 L. & SOC'Y REV. 157, 159 (2000) (stating that it is "widely held" that "laws supported by social norms are likely to be significantly more enforceable" and that "laws that are formulated in ways that are congruent with social norms are much more likely to be enacted than laws that offend such norms.").

[199] Mannheimer, *supra* note 196, at 195-196. Mannheimer reasons that this makes sense due to the fact that customs and norms were typically shaped at the societal, rather than personal, level, and "coordination problems would have hindered any conscious formation and spread of norms." Therefore, Mannheimer states, "In its earliest manifestations, therefore, custom grows by the force of practical example far more than by the impulse of reasoned conviction." Mannheimer did note that there were instances where conscious choice may have played a part in the formation and spread of certain social norms; in other words, instances where formation of a custom entailed "a selection between two different alternatives." However, he states, once the selection had been made, it would be "followed and tended to become obligatory by repetition." *Id.*

[200] Etzioni, supra note 198, at 174-75.

[201] *Id.* (quoting Dennis Chong, *Values Versus Interests in the Explanation of Social Conflict,* 144 U. Pa. L. Rev. 2079, 2101-02 (1996).

[202] *Id.* Etzioni notes that while some social norms are rational, others are undoubtedly affected by other "historical" forces, including include tradition, institutions, custom, and habit. Etzioni makes clear that the term "historical" here is understood to mean not only past events, but the narratives of those past events, which are "interpreted in ways that help transmit social norms." *Id.* at 173-175.

reflecting norms will shape people's predispositions and preferences, further entrenching acclimation to being watched.[203]

One surveillance becomes the norm, it is quite difficult to change. Etzioni notes that at first, before norms become truly internalized, people obey them "to avoid external sanctions made possible by the desire for esteem, though the sanctions may in fact include material punishments."[204] After a norm becomes internalized, "there is yet another cost to violating a norm: guilt. The individual feels psychological discomfort whether or not others detect her violation."[205] In other words, once norms become internalized, they have a tendency to stick better. The reasonable expectations of privacy test ignores how privacy nicks work to internalize the norm of being watched and, as a result, is self-eroding.

B. Better Options

In this part, we explore how lawmakers and judges can better confront how privacy nicks acclimate people to surveillance. Our recommendations are meant to mitigate three misguided approaches of current privacy law. First, instead of focusing on individuals, privacy law should focus more on the collective good. Next, instead of exclusively creating rules that regulate people's behavior, lawmakers should also target the design of information technologies. Finally, instead of creating procedural frameworks that merely require jumping through hoops to justify surveillance, lawmakers should outright prohibit the most dangerous and unjustified surveillance practices.

1. Focusing on Collectives

Privacy law is largely built around protecting individual autonomy and individual rights that individuals can exercise one right at a time.[206] 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

---

[203] *See id*.

[204] *Id*. at 167 (quoting Richard McAdams, *The Origin, Development, and Regulation of Norms,* 96 Mich. L. Rev. 338, 381 (1997).

[205] *Id*.

[206] *See, e.g*. Solove, supra note 129; Ari Ezra Waldman, *Privacy's Rights Trap*, 117 NW. U.L. REV. ONLINE 88 (2022). *But see* Kaminski, *supra* note 129; Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020).

only on the trees. This myopia causes lawmakers to miss some of the most harmful aspects of surveillance, including the 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, what Salome Viljoen highlighted in her relational approach to privacy rules.[207]

Feminist scholarship in privacy and data protection law has noted the consequences of this failure. In an introduction to feminist data protection, Jens Theilen and co-authors observed "Data from one individual might lead to conclusions that affect all members of an artificially created group. The effect of individuals being sorted following their individual data into groups, leading to group categorisations that become the basis of how individuals are treated, might be called statistical discrimination. Since the group and collective aspect of personal data processing becomes more important in big data and machine learning environments, scholars began to increasingly focus on group and collective aspects of data protection beyond the individual."[208]

There are several ways lawmakers and judges could shift their focus to collectives. At a theoretical level, lawmakers could look to preserve what Nancy Kim has called our "collective autonomy" instead of our "individual autonomy."[209] According to Kim, since people have little control over the circumstances they are born into, the fairest way to foster and protect everyone's autonomy is to configure a social order that promotes liberty for all citizens. Autonomy interests are usually conceptualized at the personal level. But Kim also identifies collective autonomy interests, which she

---

[207] Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573 (2021) ("What makes datafication wrong is not (only) that it erodes the capacity for subject self-formation, but instead that it materializes unjust social relations: data relations that enact or amplify social inequality.").

[208] Jens T. Theilen, *Feminist Data Protection: An Introduction*, 10 INTERNET POL'Y REV. 1, 6 (2021) (citing Keith Guzik, *Discrimination by Design: Predictive Data Mining as Security Practice in the United States' 'War on Terror'*, 7 SURVEILLANCE & SOC'Y 1, 10 (2009); Tobias Matzner, *Why Privacy Is Not Enough Privacy in the Context of "Ubiquitous Computing" and "Big Data,"* 12 J. INFO., COMMC'N, & ETHICS SOC'Y 93 (2014); Alessandro Mantelero, *Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection*, 32 COMPUT. L. & SEC. REV. 238 (2016); GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES (Linnet Taylor et al. eds., 2017).

[209] NANCY KIM, CONSENTABILITY: CONSENT AND ITS LIMITS (2019).

defines as "the interest that all members of a society have in a particular right."[210] Under this approach lawmakers should structure their rules such that if a clash occurs over comparable autonomy interests, "the collective autonomy interest prevails over the individual autonomy interest."[211]

As a first step away from individuals toward groups, lawmakers could better recognize threats to collective and social wellbeing as a privacy harm to satisfy damage and standing requirements.[212] They could also abandon the "reasonable expectation of privacy" test to focus on collective wellbeing or unjust uses of power, similar to calls for data collectors to be bound by duties of loyalty to trusting parties.[213] Dislodging individual expectations and individual harm as the center of privacy law would guide lawmakers to systematically examine the danger of privacy nicks.

2. Targeting Design

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 interception of aural signals or information but ignores how spycams

---

[210] *Id.* at 84, 88.

[211] *Id.*

[212] *See, e.g.*, Joshua A.T. Fairfield & Christoph Engel, *Privacy As A Public Good*, 65 DUKE L.J. 385, 387 (2015) ("Your privacy is not yours alone. The data that a person produces concerns both herself and others. Being cautious with personal data is therefore not enough. Individuals are vulnerable merely because others have been careless with their data. As a result, privacy protection requires group coordination. Failure of coordination means a failure of privacy."); Citron & Solove, *supra* note 27, at 831 (creating a typology groups individual privacy harms including seven basic types: (1) physical harms; (2) economic harms; (3) reputational harms; (4) psychological harms; (5) autonomy harms; (6) discrimination harms; and (7) relationship harms).

[213] *See, e.g.,* Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985, 1012 (2022) ("For years, lawmakers have avoided the hard questions of whether privacy law should serve any goal beyond giving people control over their personal information and respecting their choices about their data. But informational capitalism is jeopardizing so much more than that, including our civil rights, intellectual self-development, mental well-being, life opportunities, relationships, capacity for self-governance, and even our environment. A myopic approach prioritizing individuals' [often illusory] choices obscures these larger, collective harms. An approach to data loyalty that required fealty only to individual choice would doom us to the same fate. Not only must any data loyalty framework explicitly exist alongside deeper, structural, collective changes imposed by public governance, but also any determination of people's "best interests" must include a consideration of the common good."); Woodrow Hartzog & Neil Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 356 (2022); Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U.L. REV. 961 (2021).

hidden in everyday objects practically encourage surreptitious monitoring. The privacy torts limit the ways in which people can disclose private facts or intrude upon our seclusion, but ignore how facial recognition tools make these actions so easy.

It's a mistake for lawmakers to ignore the design of information technologies. Woodrow Hartzog has argued that design is everywhere, design is power, and design is political.[214] When lawmakers ignore the design of information technologies, they allow companies to escape accountability for malicious and negligent design decisions that encourage privacy harms and an overall degradation of privacy.[215]

Lawmakers and judges could better confront the design of information technologies to limit privacy nicks by creating specific rules that limit certain design decisions like tools that use biometrics or are designed to be hidden in bathrooms undetected. State legislators have already started to regulate biometric tools and require certain apps and websites to have "eraser buttons" and buttons that say "Do Not Sell My Personal Information."[216] California has recently directly confronted the design of information technologies by passing the Age-Appropriate Design Code Act (ADCA), which, among other things dictates that "should consider the best interests of children when designing, developing, and providing that online service, product, or feature" and requires that businesses subject design decisions to impact assessments and configure default privacy settings to the highest level of privacy.[217]

Consumer protection agencies have also taken design seriously by targeting "dark patterns," which are interface elements and designs that trick users into unwanted or unintentional behavior against their best interests.[218] The FTC has filed complaints against companies for "unfair

---

[214] WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 279 (2018).

[215] *See generally id.*

[216] Cal. Civ. Code § 1798.99.31 ("Configure all default privacy settings provided to children by the online service, product, or feature to settings that offer a high level of privacy.").

[217] *Id.*

[218] *See, e.g.,* Gunawan et al., *Understanding Dark Patterns in Home IoT Devices*, 2023 PROC. CHI CONF. ON HUM. FACTORS COMPUTING SYSTEMS (forthcoming); *see also*

default settings," design choices that unfairly risk the security of personal data, and design choices that unfairly interfered with a technological privacy safeguard.[219]

Another way to target design to minimize privacy nicks 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. These theories should be greater utilized 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 products liability, can be leveraged to check the starting point for virtually all privacy nicks: the tools of surveillance.

3. Implementing Bans

Privacy law's favorite tool is procedure.[220] 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.[221] People are given privacy when they have "control" over personal information and rights of transparency, access, and

---

HARTZOG, *supra* note 214; Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014); Gregory Conti & Edward Sobiesk, *Malicious Interface Design: Exploiting the User*, 2010 PROC. OF WWW CONF.; Linda Di Geronimo et al., *UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception*, 2020 PROC. CHI. CONF. ON HUM. FACTORS COMPUTING SYSTEMS; Colin M. Gray et al., *End User Accounts of Dark Patterns as Felt Manipulation*, 5 PROC. ACM ON HUM.-COMPUT. INTERACTION 372:1 (2021); Jennifer King & Adriana Stephan, *Regulating Privacy Dark Patterns in Practice—Drawing Inspiration from the California Privacy Rights Act*, 5 GEO. L. TECH. REV. 251 (2021); Jamie Luguri & Lior Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43 (2021).

[219] *See, e.g.,* Complaint, Zoom Video Communications, Inc., FTC Matter/File Number 192 3167 (Nov. 9, 2020); *see also* Daniel Solove & Woodrow Hartzog, *The FTC Zoom Case: Does the FTC Need a New Approach?*, LINKEDIN (Nov. 10, 2020), https://www.linkedin.com/pulse/ftc-zoom-case-does-need-new-approach-daniel-solove/.

[220] *See, e.g.,* COHEN, *supra* note 158; Hartzog & Richards, *supra* note 206, at 1722; WALDMAN, *supra* note 132; Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 CAL. L. REV. 1221 (2022).

[221] Hartzog & Richards, *supra* note 206, at 1722.

deletion.[222] 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 is justified. This is a recipe for privacy nicks to flourish.[223]

Scholars have long noted the problem of procedural frameworks that end up justifying the practices they seek to mitigate.[224] Woodrow Hartzog and Neil Richards have argued that "Data protection advances fair processing rules at the same time as it conditions us to a world and society in which data processing is inevitable-- and inevitably good. The FIPs set the preconditions for processing, but ultimately, they fail to question the implications of the processing itself."[225] James Rule and his colleagues argued that the FIPS were mere "efficiency" principles do little to limit surveillance and data collection against the interests of data controllers.[226]

Rule and his colleagues were critical of this FIPs efficiency goal because it legitimized surveillance systems and also gave them moral privacy cover.[227] Graham Greenleaf noted that lawmakers considering data protection rules are still rarely asking "to what extent do and should data privacy principles and laws go beyond attempting to ensure the 'efficiency' of personal information systems, and provide means to limit and control the expansion of surveillance systems?"[228] Theilen and co-authors wrote "there is a risk that notions like transparency, fairness or accuracy, which

---

[222] Ari Ezra Waldman, *The New Privacy Law*, 55 U.C. DAVIS L. REV. ONLINE 19, 39–40 (2021).

[223] *See supra* Part III; *see also* Julie E. Cohen, *How (Not) to Write a Privacy Law*, KNIGHT FIRST AMEND. INST. 2, 8 (Mar. 23, 2021), https://knightcolumbia.org/content/how-not-to-write-a-privacy-law [https://perma.cc/Z7ZN-F5P9].

[224] *See, e.g.* Waldman, *supra* note 222, at 39–40 ("[Current data privacy law] conceptualizes privacy as personal control over data and tries to achieve that goal by laying down "rules of the road" for data use rather than restructuring a data-extractive business model to rein in information industry power. But informational capitalism creates population-level harms, not merely atomistic ones. It puts marginalized populations at unique risks.110 It *40 normalizes surveillance and attendant behavior manipulation.").

[225] Hartzog & Richards, *supra* note 206, at 1722.

[226] JAMES RULE ET AL., THE POLITICS OF PRIVACY 93 (1980).

[227] *Id.* (writing that under the FIPs' criteria, "organisations can claim to protect the privacy of those with whom they deal, even as they demand more and more data from them, and accumulate ever more power over their lives").

[228] GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS: TRADE AND HUMAN RIGHTS PERSPECTIVES (2014).

play a prominent role in liberal data protection discourse, may function merely as a distraction from more foundational feminist concerns about the way technologies such as automated gender recognition both entrench cisnormative views of gender as 'readable', normalise mass surveillance along gendered and racialised lines, and expand the reach of the carceral state at the expense of already oppressed groups." [229] The scholars argued that "at least in the legal conceptualisation of data protection, such practices will largely continue to be legitimated."[230]

What is needed are substantive prohibitions for dangerous activities that no amount of procedure can justify.[231] This might take be modeled on Title III's prohibition on spyware or the proposed American Data Privacy Act's prohibition of particular practices seen as disloyal and rule against cross-contextual behavioral advertising.[232] Even better, lawmakers might join cities like Portland, San Francisco, Oakland, Sommerville, and others that have banned facial and biometric surveillance by law enforcement or in places of public accommodation.[233] Or perhaps

---

[229] Theilen, *supra* note 208, at 11.

[230] *Id.*

[231] *See, e.g.* Cohen, *supra* note 223, at 2 ("The European General Data Protection Regulation (GDPR) imposes a substantive duty of data protection by design and default, but it does not specify the sorts of design practices that such a duty might require. There is a hole at the center where substantive standards ought to be…").

[232] *See, e.g.* Danielle Keats Citron, *Spying Inc.*, 72 WASH. & LEE L. REV. 1243, 1263–64 (2015) ("In passing Title III, legislators recognized that private spies would be difficult to identify. After all, eavesdropping equipment is designed to ensure that those under surveillance do not know about it. To enhance Title III's deterrent effect, Congress included a provision covering those involved in the manufacture, sale, and advertisement of covert surveillance devices. The idea was to "dry up the source of equipment highly useful for surveillance." Section 2512 made it a crime to intentionally manufacture, sell, or advertise a device knowing or having reason to know that its design renders it "primarily useful" for the surreptitious interception of wire, oral, or electronic communications."); Cameron Kerry & Mishaela Robinson, *Rulemaking in Privacy Legislation Can Help Dial In Ad Regulation*, BROOKINGS (Dec. 5, 2022), https://www.brookings.edu/blog/techtank/2022/12/05/rulemaking-in-privacy-legislation-can-help-dial-in-ad-regulation/.

[233] *See, e.g.,* Rachel Metz, *Portland Passes Broadest Facial Recognition Ban in the U.S.*, CNN (Sept. 9, 2020), https://www.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html; Shannon Flynn, *13 Cities Where Police Are Banned From Using Facial Recognition Tech,* INNOVATION & TECH TODAY, https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/ (last visited Mar. 2, 2023).

they will follow the proposal of Representatives Eshoo and Schakowsky to outright ban surveillance advertising.[234]

All of these proposals are strong and bright-line prohibitions that 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. 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, we think it is necessary.[235] As we argued elsewhere, "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."[236] Compromises to fall back on procedure and "individual control" will end up compromising the entire endeavor.

CONCLUSION

In this Article, we have proposed a theory of privacy nicks to explain the law's fundamental failure to protect people from extensive surveillance. Our main goal has been to explain how the law normalizes surveillance and acclimates people to long-term privacy harms one small diminution at a time. Privacy nicks like Iot doorbell cameras and auto-tagging of summer camp photos using facial recognition are easy to gloss over. They are subtle,

---

[234] Press Release, Anna G. Eshoo, Congresswoman, Eshoo, Schakowsky, Booker Introduce Bill to Ban Surveillance Advertising (Jan. 18, 2022), https://eshoo.house.gov/media/press-releases/eshoo-schakowsky-booker-introduce-bill-ban-surveillance-advertising.

[235] *See, e.g.,* Selinger & Hartzog, *supra* note 116, at 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.").

[236] *Id.*

dispersed, and delayed and people tend to perceive them as mere annoyances or fail to notice them at all.

Our theory of privacy nicks is meant to provide lawmakers, judges, advocates, and even those in industry a language to better identify and stop surveillance creep. When people think about significant privacy violations—voyeurism, government spying, and betrayal of intimacies—they usually think about privacy chops: intense, immediate, and individualized setbacks, injuries, and exposures. Privacy law in the U.S. adopts a similar approach. While there is no shortage of significant privacy violations or "chops," privacy nicks are far more frequent, and far more overlooked in the law. By realizing how the law is designed to ignore privacy nicks by focusing on harms, waiver, and proximity, lawmakers and judges can better craft substantive remedies that recognize collective and social harms, target the design of technologies, and outright prohibit the most dangerous practices.

The stakes are high. Over time, the slippery slope of normalizing surveillance stands to change fundamental social beliefs about and dispositions towards privacy. The endpoint of the slope is the widescale degradation of obscurity 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 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 fundamental liberties.