PRIVACY'S AUTONOMY THICKET: DISENTANGLING CHOICE, CONSENT AND CONTROL

JORDAN FRANCIS,[†] WOODROW HARTZOG,[††] & NEIL RICHARDS[†††]

ABSTRACT

When it comes to talking about autonomy, privacy law could use a little clarity. Its discourse uses terms like "choice," "consent," and "control" to evoke autonomy, but these terms are too rarely defined and too often used interchangeably, even though they can mean very different things. The three terms have become entangled in a way that has become confusing and counterproductive. We call this problem "privacy's autonomy thicket," and it matters because it encourages talking past each other in policy debates, enabling the redefinition of these terms in misleading ways that produce weak and disempowering "notice and choice" regimes.

In this essay, we argue that choice, consent, and control are often conflated in ways that weaken individual autonomy. We distinguish between mere choice—simply selecting among options—and meaningful choice, which requires real, substantive alternatives. Consent, while legally authorizing data use, is different from having actual power to negotiate terms. Control, as currently understood in privacy law and theory, tends to narrowly focus on managing personal data rather than empowering individuals in broader relational contexts. Disentangling these concepts shows how current privacy frameworks fail to provide individuals with true agency.

This conceptual confusion has led to flawed privacy rules that offer a mere illusion of empowerment—such as "consent at scale" and fragmented opt-out mechanisms—while reinforcing vulnerability. Neither consent nor control alone can offer meaningful autonomy or achieve any of privacy law's other goals. Instead, we call for a reorientation of privacy law's autonomy goals toward fostering meaningful choice—the ability to make significant life decisions unburdened by significant privacy risks. Doing so will require not just better definitions of choice, consent, and control, but additional legal protections (many of them grounded in trust and loyalty) that safeguard the vulnerable parties in informational relationships.

[†] Nonresident Fellow, Cordell Institute for Policy in Medicine and Law at Washington University. Senior Policy Counsel, Future of Privacy Forum (FPF). The views expressed in this article are reflective solely of his affiliation with the Cordell Institute and do not represent the views of FPF, its supporters, or its advisory board. The authors would like to thank Michael Birnhack, Laura Moy, Jessica Silbey, and the participants of the 2025 Privacy Law Scholars Conference for their feedback. The authors would also like to thank Kabbas Azhar, James Sheldon, and Emily Clegg for their research assistance.
[††] Andrew R. Randall Professor of Law, Boston University School of Law.
[†††] Koch Distinguished Professor in Law and Director, Cordell Institute, Washington University.

TABLE OF CONTENTS

INTRODUCTION 38

I. DISENTANGLING THE AUTONOMY THICKET 42

II. THE PROBLEMS WITH IDEALIZING CONSENT AND CONTROL 44
- A. Letting People Make Choices Is not the Same as Giving Meaningful Choices 45
- B. Consent Is Illusory and Fails to Scale 46
- C. Control is Overwhelming and Insufficient 50
- D. Control May Be Beyond Rehabilitation 52

III. HOW MEANINGFUL CHOICE BETTER PROMOTES PRIVACY AUTONOMY 55
- A. Reframing Meaningful Choice: Personal and Collective Choice 56
- B. Providing Meaningful Choice Requires Substantive Duties and Rules Prohibiting Privacy-Invasive Practices 58
- C. Disentangling Privacy's Autonomy Thicket is Necessary for Navigating a World Increasingly Reliant on Artificial Intelligence 60

INTRODUCTION

Autonomy has long been a key goal of privacy law, but the way we talk about it can be confusing. For decades, policymakers have used the terms "choice," "consent," and "control" to assert that people should have autonomy over the extent to which their information is known or used. This goal is typically articulated as either (1) letting individuals make "choices" about how their personal data becomes known or used (often with some kind of thin "notice"), (2) requiring "consent" before people's information can be collected or used, or (3) empowering individuals to put them in "control" over their data. These terms are load-bearing concepts for data privacy, but they often bleed together in unhelpful, misleading, or confusing ways.

Done right, implementation of choice, consent, and control ostensibly protects autonomy by allowing people to determine their own informational destinies.[1] Done poorly, these concepts get defined down or misconstrued in ways that are legally permissible but normatively dangerous.[2] The mass proliferation of artificial intelligence systems has ratcheted up the intensity of the debate around personal data collection and surveillance without consent, control, or choice. This has played out with industry bombarding people with endless 'I agree' buttons, cookie banners, and privacy settings ostensibly to obtain their 'consent,' put them 'in control' of their data, and give them 'choices' about how they expose themselves.[3] But the deluge of options isn't working. If anything, when it comes to privacy, we have less autonomy than ever as ordinary people are on the wrong side of a massive power disparity with those who want to know and use their information. This produces the irony of countless options and selections to make, but with little actual agency—autonomy in theory and resigned vulnerability in reality.[4]

Such digital disempowerment has multiple causes, but we believe that one element of the

---

[1] *See* Michael Birnhack, *In Defense of Privacy-as-Control (Properly Understood)*, 65 JURIMETRICS J. 143 (2026).

[2] *See, e.g.*, Daryl J. Levinson & David E. Pozen, *Disconsents*, 126 COLUM. L. REV. (forthcoming 2026), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5113308; *see also* MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW 158 (2013); WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 211 (2018); IGNACIO COFONE, THE PRIVACY FALLACY: HARM AND POWER IN THE INFORMATION ECONOMY 90 (2023); Joshua Fairfield, *The Cost of Consent: Optimal Standardization in the Law of Contract*, 58 EMORY L.J. 1401, 1456 (2009); Elettra Bietti, *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*, 40 PACE L. REV. 310, 321–23 (2019); Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U.L. REV. 593 (2024) [*hereinafter* Solove, *Murky Consent*]; Daniel J. Solove & Woodrow Hartzog, *Kafka in the Age of AI and the Futility of Privacy as Control*, 104 B.U.L. REV. 1021 (2024) [*hereinafter* Solove & Hartzog, *Kafka*]; Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U.L. REV. 1461 (2019) [*hereinafter* Richards & Hartzog, *Pathologies*]; Woodrow Hartzog, *The Case Against Idealizing Control*, 4 EUR. DATA PROT. L. REV. 423 (2018) [hereinafter Hartzog, *Idealising Control*]; Ari Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World,* 69 U. MIAMI L. REV. 559, 563 (2015) ("[F]ree choice is not the shibboleth of privacy in the information-sharing context."); Dennis Hirsch, *New Paradigms for Privacy Law,* 79 MD. L. REV. 439, 462 (2019) (arguing for a "shift from a liberalist regulatory approach that seeks to facilitate individual choice, to one that empowers public officials to make choices about which . . . practices are safe for individuals and consistent with social values, and which are not").

[3] *See* Ed Bayley, *The Clicks That Bind: Ways Users "Agree" to Online Terms of Service*, ELEC. FRONTIER FOUND. (Nov. 2009), https://www.eff.org/wp/clicks-bind-ways-users-agree-online-terms-service [https://perma.cc/VJB7-6S5M]; Joao Vitor Sales, *The Mighty "I Agree to the Terms and Conditions" Checkbox*, WEBSITE POLICIES: BLOG (Apr. 24, 2025), https://www.websitepolicies.com/blog/i-agree-terms-and-conditions [https://perma.cc/W6TA-2KHN]; David A. Zetoony, *How many websites now have cookie banners?*, GREENBERG TRAURIG (Dec. 7, 2022), https://www.gtlaw-dataprivacydish.com/2022/12/how-many-websites-now-have-cookie-banners/ [https://perma.cc/ST48-UKFM]; Joseph K. Nwankpa, *Complicated app settings are a threat to user privacy*, THE CONVERSATION (Aug. 16, 2024, 8:35 AM), https://theconversation.com/complicated-app-settings-are-a-threat-to-user-privacy-235842 [https://perma.cc/ZTC6-9AQ5].

[4] We use "agency" in the sense of having the capacity to act in a given environment.

problem is privacy law's failure to properly clarify and distinguish between different concepts that evoke informational autonomy. The terms *choice*, *consent*, and *control* are too often used interchangeably, even though they can mean very different things. The three terms have become entangled and muddled in a way that has become confusing and counterproductive. This is a problem we call "privacy's autonomy thicket,"[5] and it matters because it enables dialogue at cross purposes, enables the deployment of weak "notice and choice" regimes in misleading ways, and misses the possibilities of focusing privacy law on human flourishing and wellbeing beyond narrow conceptualizations of informational autonomy.

Simply put, if the terms we use to describe a problem are muddled, contradictory, and misleading, any solutions to the problem are likely to be as well. The problem is not so much that we define these key words badly, but rather that our conceptual muddle creates opportunities for the most powerful corporations on the planet to further disempower and exploit people on the receiving end of unequal digital relationships.

This paper attempts to disentangle privacy's autonomy thicket, clarifying the conceptual murkiness of choice, consent, and control in the digital context. Drawing on existing critiques of notice-and-choice, privacy self-management, consent regimes, and privacy-as-control, we suggest that at the most basic level, *"choice" should be understood as the mere act of deciding when faced with multiple possibilities*. But being given choices isn't the same thing as getting to dictate which choices you are given. Choice in this sense is just descriptive—it says nothing about whether those choices are meaningful (or not) or desirable (or not). Meanwhile, "*consent" adds the element of legal authorization to a choice*.[6] It works "moral magic" to make that which was formally prohibited now legitimate under law, such as by turning an unlawful invasion of privacy into a legally consented to data transaction.[7] But the act of waiving legal rights is itself distinct from having the power to control (i.e. dictate) the terms of a deal. This is where control comes in, which in our view adds a practical heft to mere descriptive choice and legal consent. "*Control" is our capacity to do something effectively according to our developed preferences*. Certainly, influential scholars have seen control as something more—as a way of conceptualizing privacy or as the main goal of privacy law.[8] We are skeptical of this approach because it acts as a subtle misdirection that puts our focus on the *data* and away from what really matters, which is the *people* exposed by the processing of their data.

Privacy's autonomy thicket has led to lawmakers becoming lost in the clutter, making misguided policy choices that seem facially empowering in theory but that ultimately fail to

---

[5] Not to be confused with a "privacy thicket," a term used by Michael Birnhack to refer to certain instances of relational privacy. Birnhack, *supra* note 1, at 40.

[6] *See* Solove, *Murky Consent*, *supra* note 2, at 593.

[7] *See* Elizabeth Edenberg & Meg Leta Jones, *Analyzing the Legal Roots and Moral Core of Digital Consent*, 21 NEW MEDIA & SOC'Y 1804 (2019); *see also* Meg Leta Jones, *The Development of Consent to Computing*, 41 IEEE ANNALS OF THE HIST. OF COMPUTING 34 (2019).

[8] *See* Birnhack, *supra* note 1 (arguing that privacy should be conceptualized as "continuous control"); ALAN WESTIN, PRIV. & FREEDOM 7 (1967) (defining privacy in terms of control).

provide meaningful autonomy in practice.[9] The result has been a suite of state "comprehensive privacy laws" offering procedural rights that are practically difficult to use and which are insufficient to counteract the power of data collectors—much less put people in control of how their data is processed.[10] This has enabled a fantasy of "consent at scale" and offers just an illusion of meaningful choice through data subject rights, opt-outs, and other narrow procedural trinkets.[11] Such watered-down frameworks both disempower citizens and consumers under the fiction of "control" and distract us from important conversations about the allocation and use of power derived from surveillance and data processing.[12]

The confusion and conflation of these three concepts have also stifled our public debate around privacy.[13] People end up talking in circles insisting on "consent" or "control" when what they really want is to maintain a wide variety of choices for people to author their own fate and be protected against dangerous data practices like exposure, manipulation, and poor security.[14] Or they risk wrongfully dismissing "choice" as an important aspect of our privacy rules when their real target of criticism is the goal of "control" or mandatory "consent" requirements.[15] Or perhaps they risk wrongfully lionizing "control" by assessing the adequacy of consent without meaningfully assessing the adequacy of the choices being offered.[16] Our public debates around privacy will not improve until we distinguish choice, consent, and control in ways that promote human empowerment rather than creating the confusion that enables data-based exploitation and manipulation.

We must separate choice, consent, and control in privacy debates and in law for clarity, comparison, and compatibility. These concepts are certainly related, but they should be seen as distinct. For example, consent requirements can ostensibly give people some modicum of control over information.[17] But consent can also reduce choice to a binary "yes" or "no." Control can be more than legalistic consent requirements; it can instead be backed up by legal duties on companies that prevent harm and promote trust like duties of loyalty or obedience. Perhaps most critically, people can have significant and numerous choices regarding the extent to which their information is known or used without placing control at the center of a data privacy framework or without looking to (often fictitious) consent to justify data practices and surveillance. Ideally, consumers dealing with powerful corporations that hold their data should be protected no matter what they

---

[9] *See* Caitriona Fitzgerald et. al, *The State of Privacy: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better,* ELEC. PRIV. INFO. CTR. 4 (Jan. 2025), https://epic.org/documents/the-state-of-privacy-2025-how-state-privacy-laws-fail-to-protect-privacy-and-what-they-can-do-better [https://perma.cc/J2UF-5WVB] (critically reviewing the many deficiencies of recent state "comprehensive" privacy laws centered on "control").

[10] *See id.*

[11] *E.g.*, JOSEPH TUROW ET AL., U. PENN., AMERICAN'S CAN'T CONSENT TO COMPANIES' USE OF THEIR DATA 2 (2023), https://ssrn.com/abstract=4391134 [https://perma.cc/9WMK-CVGR].

[12] HARTZOG, *supra* note 2, at 65; ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER (2021); JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 59 (2019); NEIL RICHARDS, WHY PRIVACY MATTERS 166 (2022).

[13] WALDMAN, *supra* note 12, at 24.

[14] *See, e.g.*, COHEN, *supra* note 12, at 73.

[15] RICHARDS, *supra* note 12, at 166.

[16] HARTZOG, *supra* note 2, at 65.

[17] This is also highly contested.

choose.

While our argument is about conceptual clarity, its goal is not merely definitional. Other scholars have recognized that choice, consent, and control are distinct terms with their own respective meanings.[18] Ari Waldman, for example, in calling for the development of new privacy discourses, argued that

> [t]alking about privacy law in terms of consent, choice, freedom, control, and even autonomy is incompatible with actually protecting privacy. Undoubtedly, those words don't all mean the same thing. But it is easy to collapse robust conceptions of autonomy into flat or bastardized versions of consent and control.[19]

This illustrates precisely why we believe privacy's autonomy thicket must be disentangled. While we agree with Waldman's critique of "consent" and "control," "choice" is too frequently unfairly lumped in with those concepts and dismissed. We believe this is a mistake that sacrifices a powerful discursive tool for the proponents of a more robust, protective privacy law. Our analysis not only provides an explanation as to how these concepts are different, but seeks to elevate choice as a virtue worth pursing in a robust privacy legal regime.

Normatively, we argue that lawmakers should pursue meaningful choices for people that are about more than just our data without making consent or control the keystone of a legal privacy regime. To protect individuals' autonomy, policymakers should privilege the power to dictate *meaningful life choices* instead of narrower concepts of consent as legal waiver and control as instructions for data processing. In other words, lawmakers should seek to give people the capacity to make meaningful choices that are not fraught with unreasonable privacy risks. Untangling privacy's autonomy thicket can be helpful in this endeavor because it lets privacy scholars reclaim the concept of choice, and it provides a framing for policymakers to identify where and when to pursue substantive interventions that go beyond consent and control.

Lawmakers should do this by considering meaningful choice at both the personal and the collective levels. Meaningful choice on a personal level might mean working to create more agency for people to impose their will in contexts where it would be ideal to dictate their own choices, particularly in mediated environments. Meaningful choice at the collective level requires placing substantive limits on excessive and harmful data practices, thereby enabling us to make choices in daily life that are unburdened by undue privacy risk.[20] Lawmakers should promote both types of choice simultaneously and, where they are in conflict, they should prioritize collective choice. After all technology companies process data at scale, and our law should meet the problem where it is—at the level of structure that affects us all rather than on fictions of control in billions of digital micro-transactions.[21]

---

[18] *See, e.g.*, WALDMAN, *supra* note 12, at 234.
[19] *See id.* at 234.
[20] *See* Levinson & Pozen, *supra* note 22, at 68 ("[E]nhancing the voices of individual consenting agents through collective action may entail restricting some of their choices.").
[21] *See, e.g.*, Mark. P. McKenna & Woodrow Hartzog, *Taking Scale Seriously in Technology Law*, 61 WAKE FOREST L. REV. 7 (forthcoming 2026); Solove & Hartzog, *Kafka*, *supra* note 2.

To design privacy law to give people meaningful agency would require rules meant to give people quality choices backed by substantive protections (whether GDPR-style or loyalty-based) in the information-rich environments that affect every aspect of their lives. Meaningful agency is distinct from a take-it-or-leave-it set of data choices (the facile notion of choice), the legal recognition of such a choice (consent), or the practical ability to choose among a limited set of data processing instructions (control or informational self-determination). In other words, we argue that the goal of an autonomy-focused privacy law should be to ensure that people have meaningful life choices unburdened by undue privacy risks. We then apply this framework to existing legal rules and explain why untangling the autonomy thicket could open the way for a more empowering, substantive conception of privacy law. By disentangling privacy's autonomy thicket, privacy scholars can reclaim choice and provide a positive framing for policymakers to identify where and when to pursue substantive interventions that go beyond consent and control. The two examples we highlight are ongoing changes to data minimization requirements in state privacy laws and the mass adoption of artificial intelligence.

I. DISENTANGLING THE AUTONOMY THICKET

Discussions about privacy by scholars, lawmakers, regulators, and corporations are rife with imprecise and often interchangeable uses of the terms *choice*, *consent*, and *control*. This imprecision has consequences. Advocates of notice-and-choice[22] or privacy-as-control[23] regimes that give people procedural choices over how their data is processed have criticized proposed privacy rules that would go further and place substantive limitations on data processing. From the perspective of these advocates, privacy is about giving people choices and control that consent to proposed data practices and anything more than that deprives them of agency and is regime is anti-choice paternalism.

Concepts of control have long dominated information privacy law. Historically, control over personal information has been seen as the foundation of information privacy law.[24] Some academics articulate that control over personal information should be seen as the aspiration of privacy law. Often this mixing of terms follows a certain logic: Requiring people to consent to data practices enables them to exercise control over their data; empowering them to exercise control over their data allows them to make choices. Other times, the conflation may be less

---

[22] "Notice and Choice" is the view that privacy rights are best protected when people have *notice* of privacy practices (perhaps by reading a company's privacy policy) and are then given the opportunity to *choose* their privacy preferences (either by using privacy dashboards and opt-outs provided by the company or not using the company's services at all). This term is most commonly used in policy conversations and has been the default view of U.S. companies about the best kind of privacy regulation throughout the Internet era. As we explain in greater detail below, we believe that this view is deeply flawed because notice in practice can be the fiction of fine print in dense privacy policies few read or understand, and choice can be illusory—little more than the choice whether or not to use technologies or not. *See, e.g.*, Richards & Hartzog, *Pathologies*, *supra* note 2, at 1471; RICHARDS, *supra* note 12, at 93.

[23] By contrast, privacy-as-control is the idea that privacy law can and should seek to put people in control of their data. *See* Birnhack, *supra* note 1, at 1.

[24] *See* Birnhack, *supra* note 1, at 146 (describing how information privacy has a foundation in the FIPs which are, in turn, "based on the idea of control"); Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U.L. REV. 357 (2022) ("Information privacy protections today, especially in the United States, center on individual control over personal information as a way to promote individual autonomy.").

intentional. It may well be that if one were to go through any privacy academic's body of scholarship, they would find examples of these terms being used synonymously. For example, Omer Tene & Jules Polonetsky have interpreted consent as synonymous with individual control: "Legal frameworks all over the world continue to emphasize consent, *or individual control*, as a fundamental principle of privacy law."[25] We note in all honesty that we ourselves have been guilty of such imprecision in prior work and used the terms interchangeably.[26]

Policymakers also make imprecise use of choice, consent, and control. One of the most notable consumer privacy efforts coming from the executive branch in recent years was the Obama Administration's landmark Consumer Privacy Bill of Rights, which also conflated choice and control: "[T]he use of personal data begins with individuals' decisions to choose privacy settings and to share personal data with others. . . . Control over the initial act of sharing is critical."[27]

Companies, too, often equate consent and control with meaningful choice. Meta, across its suite of apps and services, routinely emphasizes the controls it offers to enable users to make choices with respect to their privacy.[28] Google, likewise, in describing "Your privacy *controls*" notes that "You have *choices* regarding the information we collect and how it's used."[29] Amazon similarly equates control and choice in its materials concerning its data practices.[30]

At this stage, our critique might seem pedantic or quaint. These terms are related to each other and so they are used synonymously. But we believe that the casual entangling of choice, consent, and control means that the way we talk about privacy and the choices we make about our data is muddled. In turn, this makes it harder for us to talk about the problems with choice, consent and control and the ways in which the theory of privacy-as-control and the policy of notice-and-choice have the effect of using the language of autonomy to disempower digital consumers and citizens. When we idealize control as the goal of privacy policy and conflate it with different kinds of choice and consent, we end up with magical thinking about privacy that makes individuals

---

[25] Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 260 (2013) (emphasis added).

[26] *E.g.*, Richards & Hartzog, *Pathologies*, *supra* note 2, at 1498–99 ("The shortcomings of consent and transparency are particularly visible in the United States. . . . In spite of the failures of control and transparency, some lawmakers are considering doubling down on this failed strategy."); *see also id.* at 1500 ("The control that consent regimes promise us ends up being illusory and overwhelming.").

[27] THE WHITE HOUSE, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* 13 (Feb. 2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf [https://perma.cc/XW8X-SJYZ] (discussing dimensions of individual control and mistakenly referring to control rather than choice regarding the initial act of sharing).

[28] Erin Egan, *Giving You More Control of Your Privacy on Facebook*, FACEBOOK (Jan. 28, 2018), https://about.fb.com/news/2018/01/control-privacy-principles ("We give you control of your privacy. You should be able to make the privacy choices that are right for you."). This equates the existence of privacy controls, such as choosing which audience(s) may see certain posts, with having choice over privacy. Facebook also refers to its privacy choices as privacy controls: "We want to make sure you know where your privacy controls are and how to adjust them.".

[29] *Google Privacy Policy*, GOOGLE, https://policies.google.com/privacy?hl=en-US [https://perma.cc/GUZ9-XWBT] (last visited Feb. 4, 2025) (emphasis added). *See also* Google Safety Center, *Your privacy is protected by responsible data practices,* GOOGLE, https://safety.google/privacy/data [https://perma.cc/52T9-6VSP] (last visited Feb. 4, 2025) ("It's your choice to make a copy of your data, back it up, or even move it to another service. You are always in control of the data saved to your Google Account.").

[30] Under "Customer control," the company's promotional content regarding its data practices provides that, "[i]n addition to transparency, we know that customers want a choice in how their personal data is used." *Amazon is earning and maintaining customer trust through privacy*, AMAZON NEWS (Jan. 28, 2022), https://www.aboutamazon.com/news/how-amazon-works/amazon-is-earning-and-maintaining-customer-trust-through-privacy [https://perma.cc/HV65-Q7V5].

worse off at the expense of the powerful companies that collect and process enormous amounts of their personal data. It is to those problems that we now turn.

II. THE PROBLEMS WITH IDEALIZING CONSENT AND CONTROL

Privacy and autonomy are certainly related. In the physical, or pre-Internet context, the relationship between them can be an intuitive one. When we meet someone new, we might act with some reserve, concerned that we might weird them out if we shared Too Much Information with them from the off, or otherwise that we might make ourselves vulnerable to them by sharing our secrets. Over time, if our relationship with our new friend deepens and trust between us grows, we might share more and more information with them. Indeed, at a certain point, the sharing of secrets with our dearest, most trusted friends can serve to deepen our friendship and produce intimacy, whether romantic or otherwise. In this way, the sharing of information can strengthen relationships. But at that point, we would expect a certain level of loyalty from our friend, that they would not use our secrets or our vulnerabilities against our interests. But in these intuitive ways familiar even to children of a certain age, our control over our privacy (and the thoughtful choices we make about our information) is an exercise in social autonomy – our capacity to act in a given environment free from external interference. Indeed, one might even say that in contexts like these, privacy makes having a social life with other people possible.[31] In other less personal contexts, background privacy rules like fiduciary duties of loyalty and confidentiality enable us to share secrets with specialist professionals like doctors and lawyers, even those we might have just met a few minutes before.[32] But note that when there is no social (and socially-sanctionable) norm of confidentiality or loyalty, the law supplied them to enable the sharing of information in confidence.[33]

The Internet and digitally-mediated commerce disrupted all that, and not in a good way. When our social and economic lives became entangled with and mediated by digital tools, the simpler pre-digital relationship between privacy and autonomy changed in important ways.[34] What used to be face-to-face human interactions have increasingly become mediated by computers of shrinking size—from desktop to laptop to smartphone.[35] Instead of a few choices in social settings, we have many choices with every digital platform and merchant in our lives.[36] Data about us inherently collected in these transactions, and we have barely any idea what is being collected and

---

[31] *See* James Rachels, *Why Privacy Is Important*, 4 PHIL. & PUB. AFFAIRS 323, 326 (1975) ("I want now to give an account of the value of privacy based on the idea that there is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people. According to this account, privacy is necessary if we are to maintain the variety of social relationships with other people that we want to have and that is why it is important to us.").

[32] *Id.* at 328 ("In each case, the sort of relationship that people have to one another involves a conception of how it is appropriate for them to behave with each other, and what is more, a conception of the kind and degree of knowledge concerning one another which it is appropriate for them to have.").

[33] *See* Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 174 (2007).

[34] *See* Marcel Becker, *Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy*, 21 ETHICS AND INFO. TECH. 307, 307 (2019).

[35] *Id.* at 313.

[36] *Id.* at 310.

what it's being used for. Instead of fallible human memories, we have the permanency of digital hard drives and cloud storage. Instead of human brains on the other side, we have data brokers driving targeted advertising and algorithmically determined dynamic pricing, debatably and only incidentally to our benefit. In commercial contexts, we share our secrets (our reading habits, our sexual preferences, our location, our passwords) with companies that are not constrained by the fiduciary duties of loyalty and confidentiality that the common law placed on the pre-digital people to whom we had that level of exposure. This form of unequal exposure of risk is called "notice and choice" or a weak version of "Privacy as Control," and it is the terrain in which laws giving us "rights" to "control" our data operate, placing few if any limits on what the data can be used for.

Yet far too much of Internet-era policy discussions of privacy involve poorly defined notions of choice, consent, and control, even though these terms have come to have radically different meanings in those discussions. While consent and control can act as sufficient proxies for autonomy in some contexts, they are inadequate for managing modern information relationships. Consent in digital environments suffers from many well-known pathologies that render it inadequate for providing individuals with meaningful choices. Control over personal data, too, is overwhelming, illusory, and myopic. The consequence of all this is that words and ideas that are ostensibly about empowering our autonomy have been used to have the opposite effect—and to our detriment.

A. Letting People Make Choices Is not the Same as Giving Meaningful Choices

The root of privacy's autonomy thicket is the indeterminacy of the word "choice." Taken literally, choice can mean "the act of choosing" or "selection."[37] In that sense, it is natural to equate consent and control with choice. Every act of consent or the withholding of consent is an act of choosing, whether clicking an "I agree" button on a cookie banner, passively accepting a pop-up alert notifying you that visiting the current website indicates acceptance of various click-wrap, or choosing to navigate away or not use a service. Similarly, all of the various privacy controls we get in apps and websites offer choices, whether that be a "data subject right" of access to our data, an opt-out of marketing, or the various toggles, switches, and radio buttons offered for us to "control" our privacy. Each of those acts or non-acts that affect our data or leave it to the default setting is an act of choosing, at least if we think of "choice" at the thin level of selecting (or not selecting) options.

But when people attach importance to individuals' ability to make *choices* with respect to their privacy, surely this must mean something deeper than the trivial ability to make such decisions like clicking a button on a cookie banner to either "accept all cookies" or "manage my privacy," which often leads to a bewildering hellscape of buttons attached to confusing labels. Such a surface-level conception of choice fails to be autonomy-promoting because it does little if anything to empower people. Instead, it leaves them as disempowered and reactive deciders facing

---

[37] *See Choice*, MERRIAM-WEBSTER, https://www.merriamwebster.com/dictionary/choice [https://perma.cc/6CJK-4A4M] (last visited Feb. 16, 2025).

a limited array of options they may only dimly understand. This approach—what the host of this Symposium has called "Privacy self-management"—is a failure that leads to disempowerment rather than control or autonomy.[38]

We can do better in defining choice, at least if we want to empower people rather than leave them at the mercy of the companies that design the interfaces that mediate their lives. First, choice can mean instead the "power of choosing,"[39] or it can mean "a number and variety to choose among."[40] In other words, choice can involve a range of meaningful options, rather than the failure to uncheck a check box buried in the fine print.

Second, we can be attentive to what the choices related to; specifically, whether they are choices about how computers process data or choices about how people want to live. Conceptualizing choice as an array of options for people allows lawmakers to then focus on the *kinds* of options that should be available to us. This is where we would encourage lawmakers to focus less on an array of choices about our data and more on a slate of good choices within an information relationship which means that people will not have to worry about privacy at all. Meaningful choice exists where individuals are faced with the practical state of having *multiple safe and productive possibilities* to choose from.[41] And when those choices are framed in terms of human life rather than computer science, they are easier to understand. "Do not sell my data" is much clearer than a button offering "opt-out of offers from our partners." This is not just more comprehensible; it is closer to the "liberal conception of private choice" offered by Anita Allen as meaningful decisional privacy over important life decisions.[42]

Eliminating trivial and confusing notions of choice is an important first step in untangling privacy's autonomy thicket. But we need to go further and unpack the failures of consent and control.

B. Consent Is Illusory and Fails to Scale

Consent is arguably the easiest member of privacy's autonomy thicket to pin down; after all, it boils down to a choice that makes a legally sufficient change in legal status. Definitions of "consent" include "to give assent or approval: agree," "compliance in or approval of what is done or proposed by another: acquiescence," and "agreement as to action or opinion."[43] In this way, we should think of consent as a choice that is legally binding, or which changes our legal status. *Consent, therefore, adds the additional element of legal authorization to a choice*.

---

[38] *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1900 (2013).
[39] *See Choice*, *supra* note 37.
[40] *Id.*
[41] Our proposed definition of "meaningful choice" is similar to that proposed by Lisa Austin, who argues in favor of shifting privacy law's focus from individual control towards meaningful choice. *See* Lisa Austin, *Re-reading Westin*, 20 THEORETICAL INQUIRIES L. 53 (2019) ("Meaningful choice requires that our informational infrastructure, and the social practices that it enables, make states of privacy available for choice along with the means of attaining them.").
[42] Anita Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 724 (1999).
[43] *Consent*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/consent [https://perma.cc/99LM-YJEB] (last visited Feb. 16, 2025).

In the context of privacy law, however, consent exists on a spectrum.[44] This makes it difficult to discuss consent in broad strokes. On one end of the spectrum is *implied consent*, which is typified by the weak notice-and-choice model in which consumers might be presumed to consent to data practices based upon privacy policies they have not read, or where they have been prompted by corporate designers to lie and tick a check box stating "I have read the privacy policy and terms and conditions."[45] On the other end of the spectrum are the various kinds of affirmative, explicit, or *informed consent* requirements under various laws.[46] These are the sorts of consents required before buying a house, getting married, or having surgery,[47] in which we have the capacity to ask questions and even negotiate terms, and in which the other party has the burden of making sure we actually understand what is going on before we agree. The kind of consent that suffices for most American privacy regimes lies somewhere in the middle between informed consent and notice-and-choice. Disentangling choice from consent is difficult in part because consent satisfies the most technical definition of choice. Each act of consent, or non-consent, is a choice. Examining the failures of consent as a regulatory model, however, demonstrates that consent-choices are not the kinds of choices which privacy law should seek to promote. Consent should be seen as a means, rather than an end. We need to ask which kinds of choices the law *should* recognize and promote and why, rather than merely what kinds of formal elements are legally necessary to get over the consent line.

The easiest way to distinguish choice and consent is to start with the weakest form of consent, the implied consent that underlies notice and choice. (In its weakest form, this is something like "I did not read the terms and conditions, but I did not stop using the service.") Drifting far from its origins in the Fair Information Principles, notice-and-choice is the default regulatory regime which has long characterized American privacy law in practice, to a chorus of scholarly critique.[48] The normative justification for notice-and-choice has been that humans, as rational actors, should be given the opportunity to decide for themselves the risks and benefits of a given data use.[49] But the reality is far from that ideal, in a way that causes notice-and-choice to make a mockery of any reasonable notion of legally-binding consent. In practice, notice-and-choice is overwhelming and ineffective. Rather than providing meaningful choice, notice-and-choice manufactures consent through manipulative design, too frequent requests, and a lack of alternative choices, as individuals have neither the time to read lengthy, indecipherable privacy notices nor the free choice to decline and continue using the product or service.[50] As Bernard

---

[44] *See* Solove, *Murky Consent*, *supra* note 2, at 632.

[45] *See id.* at 597, 599.

[46] *E.g.*, 45 C.F.R. 164.508 (establishing HIPAA's authorization requirements); WASH. REV. CODE § 19.373.070 (LEXIS through 2025 Sess.) (establishing the rigorous requirements for "valid authorization" to sell health data under the My Health My Data Act).

[47] *See* Solove, *Murky Consent*, *supra* note 2, at 614 n. 98.

[48] Solove, *supra* note 38.

[49] Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 WAKE FOREST L. REV. 261, 268–69 (2014).

[50] For critiques of notice-and-choice, see Solove, *supra* note 48; Solove, *Murky Consent*, *supra* note 2; Richards & Hartzog, *Pathologies*, supra note 2; Hartzog, *Idealising Control*, *supra* note 2; Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C.L. REV. 1687, 1734–36 (2020); Neil Richards, Woodrow Hartzog, & Jordan Francis, *Comments of the Cordell Institute Cordell on Proposed Trade Regulation Rule on Commercial Surveillance and Data Security* 47–59 (Nov. 21, 2022),

Harcourt observed, there is no way to get things done in the digital age without exposing our data to third parties: "No other way to reserve the hotel room or seat on the plane, to file the IRS form, to recall the library book, or to send money to our loved one in prison."[51] And as Schwartz and Peifer warned some years ago, "[n]o one has ever read a privacy notice who wasn't paid to do so."[52] Under notice-and-choice regimes that foist implied consent upon individuals, privacy law fails to create the practical state of having multiple possibilities to choose from. The "choice" on offer is just an illusion.

Disentangling privacy's autonomy thicket makes this more salient. Whereas choice means merely the act of choosing (and no more), consent is legally consequential; it works moral magic, and any failure to object can legitimize data uses.[53] This implied consent that notice-and-choice relies upon furthers extractive data practices. Rather than providing individuals with meaningful choice, notice and consent becomes a take-it-or-leave-it proposition whereby the act of choosing a product or service comes with a non-negotiable, bundled set of data practices which may or may not have a reasonable connection to the product or service being offered, let alone align with an individual's subjective preferences and risk tolerance. Thus, as we have explained elsewhere, rejecting "notice and choice" is not a rejection of either notice or choice.[54] Rather, it is a rejection of an overreliance on consent in general, and on a weak form of fictitious consent that makes a mockery of informed consent in particular.

To the extent consent does load-bearing work in privacy law, it needs to mean more than the weak, fictitious implied consent that characterizes notice-and-choice. While this would be a significant change in U.S. privacy law, it would not be a radical one by any means. Various types of informed consent are common in legal frameworks, like informed consent to medical treatment, but they require the parties to know what they are actually agreeing to.[55] People struggle to read lengthy legal disclosures, but there are other tools that can work, including layered notices, dashboards, and just-in-time prompts.[56] But even gold standard consent will not work in all contexts and it certainly won't scale. Still, tech companies have little trouble getting our attention when there is something they want us to see, or agree to, but they have not taken that approach towards effectively informing us about their data.

---

https://papers.ssrn.com/abstract_id=4284020; Neil Richards, Woodrow Hartzog & Jordan Francis, *A Concrete Proposal for Data Loyalty*, 37 HARV. J.L. & TECH. 1335, 1358–59 (2023); RICHARDS, *supra* note 12, at 93;WOODROW HARTZOG, PRIVACY 'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (2018); Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 564 (2008).

[51] BERNARD E. HARCOURT, EXPOSED: DESIRE AND DISOBEDIENCE IN THE DIGITAL AGE 14 (2015).

[52] Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 150 (2017).

[53] For more on the history of consent in privacy, see MEG LETA JONES, THE CHARACTER OF CONSENT: THE HISTORY OF COOKIES AND THE FUTURE OF TECHNOLOGY POLICY (2024); Edenberg & Jones, *Analyzing the Legal Roots and Moral Core of Digital Consent*, *supra* note 7; Jones, *The Development of Consent to Computing*, *supra* note 7.

[54] Neil Richards, Woodrow Hartzog & Jordan Francis, Cordell Inst., Comment on Proposed Trade Regulation Rule on Commercial Surveillance and Data Security 48 (Nov. 21, 2022), https://www.regulations.gov/comment/FTC-2022-0053-1071 [https://perma.cc/DC2Z-33BG].

[55] *See, e.g.*, Levinson & Pozen, *supra* note 2.

[56] *What Methods Can We Use to Provide Privacy Information?*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information (last visited Feb. 13, 2025).

Nevertheless, it is still a significant challenge for even the most informed individuals to achieve any meaningful understanding of a company's data practices in that moment in which notice is offered. We have elsewhere explained how three pathologies collectively undermine consent in digital contexts. Consent is often *unwitting*, such as when individuals fail to understand (1) the legal agreement that is being established, (2) the technolog(ies) being used, (3) the potential consequences of their consent, or all three. Consent can also be *coerced*, either because of the mediated nature of digital environments or the unequal bargaining power between individuals and companies. And in many cases, consent is often unachievable due to *incapacity*.[57] Collectively, these pathologies undermine even stronger forms of consent that have heightened requirements as compared to notice and choice. For this reason, in the model privacy statute we have elsewhere offered, consent plays no first-order role—it is best as a backstop to other substantive duties that protect vulnerable consumers from manipulation and unwitting data extraction.[58]

None of this is to say that consent has no value in a regulatory regime. Gold standard "informed consent" has a role to play in important choices where it (1) happens infrequently; (2) the consent must be freely given such that there are meaningful alternatives to the choice being made; (3) any harms that the consent risks are foreseeable and made vivid; and (4) the person has the right incentives to choose thoughtfully, rather than being nudged by choice architecture or disloyal design.[59] Strong informed consent standards can also be useful as default prohibitions. For example, Illinois' Biometric Information Protection Act requires, among other things, informed consent before a faceprint can be captured by a device.[60] This means that in practice, facial recognition can be used by a person to unlock their iPhone or to board a plane, because informed consent can be obtained under such one-to-one circumstances. However, it also means that one-to-many uses of facial recognition, like ones that scan faces indiscriminately to look them up against a database are *de facto* prohibited because informed consent cannot be obtained in advance as a practical matter. In this way, consent requirements can operate to make certain practices difficult or impossible.[61] But when consent has value as friction, then it still remains the case that choice and consent are not only distinct terms, but also that consent is not functioning as an exercise of one's autonomy. Rather, it is acting as a substantive intervention that, by making certain high-risk data practices difficult to legitimize, protects individuals' autonomy indirectly by taking those practices off the table.[62]

The pathologies of digital consent may be diminishing somewhat over time as legal regimes adapt and account for structural power disparities in digital contexts. The heightened consent standard introduced by Europe's General Data Protection Regulation requires that consent

---

[57] Richards & Hartzog, *Pathologies*, *supra* note 2, at 1490–91.

[58] Richards, Hartzog, & Francis, *supra* note 50, at 1358–59 (introducing a model statute that would enact a duty of data loyalty).

[59] *See* Richards & Hartzog, *Pathologies*, *supra* note 2, at 1466.

[60] Biometric Information Privacy Act (BIPA), ACLU OF ILL. (last updated Aug. 26, 2025), https://www.aclu-il.org/campaigns-initiatives/biometric-information-privacy-act-bipa [https://perma.cc/HQS5-GPNE].

[61] *See* Nikolas Guggenberger, *Consent as Friction*, 66 B.C.L. REV. (forthcoming 2025).

[62] Similarly, such consent can be serving as an expression of will. *See* Meg Jones & Paul Ohm, *Voting for Consent*, 104 BOSTON U.L. REV. 1107 (2024).

be freely given, specific, informed and unambiguous,[63] and it has arguably moved the needle away from the farce of notice-and-choice and closer to gold standard consent. Versions of its heightened consent standard has been incorporated into most of the twenty U.S. state "comprehensive" privacy laws, and were a key element in the first lawsuit brought under one of these laws.[64] The requirement that consent be "freely given" makes consent closer to an exercise of free choice, and the requirement that consent be "specific" expands the array of choices available to individuals. Both of these things bring consent closer to meaningful choice. Even considering these virtues, however, consent regimes still fail to scale, do not empower people in information relationships to impose their will and dictate their own terms, and can result in consent fatigue.[65] Thus, making consent more meaningful runs headlong into another problem with privacy's autonomy thicket: the overwhelming nature of control.

C. Control is Overwhelming and Insufficient

Control, too, can mean a range of different things, which further muddles public debate over control's role in safeguarding privacy and promoting autonomy. For example, control as a verb can mean "to exercise restraining or directing influence over."[66] This definition is likely what most people mean when they sincerely say that control over personal information should be the goal of privacy law. The most robust version of this notion only exists in theory, however, because it often depends upon a notion of individuals as perfectly rational actors. This assumes that each of us can deftly understand and manage our information relationships and direct the collectors and processors of personal data to act in accordance with our set of subjective preferences. Such assumptions are not only contradicted by the reality of life as a situated digital consumer,[67] but also suggest that each of us are fully and rational formed individuals when in reality we are in constant development.[68] Another definition that gets closer to the reality of individuals faced with privacy controls is "a device or mechanism used to regulate or guide the operation of a machine."[69] In that sense, privacy controls encompass the various devices and mechanisms by which we as individuals regulate our information relationships. In the consumer privacy context, this entails consent (both implied and explicit), individual rights (e.g., access, correction, deletion, and portability), and the various settings, toggles, switches, banners, and control centers companies

---

[63] Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119), Art. 4(11).

[64] Press Release, Off. Tex. Att'y Gen., *Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies* (Jan. 15, 2025), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-allstate-and-arity-unlawfully-collecting-using-and-selling-over-45 [https://perma.cc/99AZ-3GLQ]. For an overview of consent requirements in state comprehensive privacy laws, see JORDAN FRANCIS, ANATOMY OF STATE COMPREHENSIVE PRIVACY LAW: SURVEYING THE STATE PRIVACY LAW LANDSCAPE AND RECENT LEGISLATIVE TRENDS, FPF (Nov. 2024), https://fpf.org/wp-content/uploads/2024/11/REPORT-Anatomy-of-State-Comprehensive-Privacy-Law.pdf [https://perma.cc/5Y32-J2WF].

[65] Solove, *Murky Consent*, *supra* note 2, at 597.

[66] *Control*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/control [https://perma.cc/Y7WB-TVXH] (last visited Feb. 16, 2025).

[67] *See* Richards, *supra* note 12, at 168–77.

[68] *See generally* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF (YALE UNIV. PRESS 2012).

[69] *Id.*

offer to us to adjust our privacy settings on their platforms and services.[70]

Privacy scholars have long noted control's many faults, in theory but particularly in practice.[71] Control as an ideal is illusory, overwhelming, and myopic.[72] The mediated and constructed nature of digital environments means that companies have the opportunity and incentive to deploy the power of design and choice architecture to shape our behavior, which means that in practice, control is too often an *illusion*.[73] Control is often *overwhelming* in that too frequent requests lead us to relent, and inaction can be seen as acquiescence, placing the burden of action on individuals.[74] And control is often *myopic* in that it is inconsistent with "privacy as a collective value."[75] We can make a series of "rational" individual decisions not to read the hundreds of privacy policies we face and to accept default privacy settings, but end up exposed and uninformed.

We are not advocating against giving individuals interface controls with respect to their data—whether in the form of settings companies offer voluntarily or when required to by law. Individual rights (including causes of action) are important tools that empower individuals to hold the entities collecting and using their personal data accountable.[76] Providing *privacy controls* to people, however, is not the same thing as giving those people *control over their privacy*. Privacy controls (the tool) might be necessary, but they are by no means sufficient. Under our theory, we would say that people using "privacy controls" are making choices (choosing among options), but making choices is not the same thing as exercising control, and to say otherwise would be a lie. This is the case because, protestations of tech company marketers to the contrary, most interface "controls" do not put people *in control* of their data.[77] Moreover, as scholars have long pointed out, giving people a granular choice over every use of their data (and thus to putting them "in control") would be impossible because humans have limited resources of time, energy, and cognitive bandwidth.[78] Merely navigating the various layered, circular, and intertwined privacy

---

[70] *Id.*

[71] *Supra* note 50 and accompanying text; *see also* Daniel J. Solove, *The Limits of Privacy Rights*, 98 NOTRE DAME L. REV. 975 (2022); Solow-Niederman, *supra* note 24.

[72] Hartzog, *Idealising Control*, *supra* note 2, at 426–32; RICHARDS, *supra* note 12, at 90–100.

[73] Hartzog, *Idealising Control*, *supra* note 2, at 426–27.

[74] *Id.* at 428–30.

[75] *Id.* at 430.

[76] *See generally* Margot E. Kaminski, *The Case for Data Privacy Rights (Or, Please, a Little Optimism)*, 97 NOTRE. DAME. L. REV. REFLECTION 385 (2022); Hartzog, *Idealising Control*, *supra* note 2, at 428 ("[L]awmakers and companies should preserve user choice in the form of data subject rights like access and deletion. In the right regulatory environment, features like privacy dashboards and control panels can empower people while minimising the risk of inaction."); Richards, Hartzog & Francis, *supra* note 50, at 1345–46 (2023) ("Although the aim of substantive data privacy rules is to shift the focus away from privacy law's historical focus on atomistic privacy rights and privacy self-management, the [model] statute nevertheless incorporates some traditional individual data subject rights. These rights have several virtues, such as enabling people to ensure that companies are complying with their duty loyalties as well as appealing to common and historical understandings of why privacy matters."). *But see* Ari Ezra Waldman, *Privacy's Rights Trap*, 117 NW. U. L. REV. 88 (2022).

[77] *See, e.g.*, Justin Sherman, *Meta's Privacy Policies: Designed Badly, by Design?*, TECH POL'Y PRESS (Nov. 25, 2024), https://www.techpolicy.press/metas-privacy-policies-designed-badly-by-design [https://perma.cc/5JFG-8NUD] (discussing the importance of how privacy policies are displayed to individuals).

[78] *Id.*

notices for one online product or service can be beyond most consumers in isolation.[79][80] To that end, by distinguishing choice from control, we hope to help highlight how some policies value control at the expense of alternative duties and substantive interventions that better promote meaningful choices.

One of the best articulations of the distinction between control and choice is what Paul Schwartz's early work called the "autonomy trap," which explains how technological and market constraints create a "lock-in" of individual choice. As Schwartz put it:

> The autonomy trap ignores the extent to which the use of personal data helps set the terms under which we participate in social and political life and the meaning that we attribute to information-control. . . . The reality is, however, that individuals can be trapped when such glorification of freedom of action neglects the actual conditions of choice. . . . [P]rivacy-control either leads to empty negotiations that fall into the autonomy trap, or collapses completely in the face of the weighty reasons in support of revealing personal information. The danger is one that a belief in the virtue of self-reliant data control cannot acknowledge: information processing itself can undermine an individual's ability to participate in social and political life.[81]

This kind of voluntary participation in social and political life that control undermines is precisely what we argue should be considered "choice." Our claim is that when we discuss choice in the context of privacy, we should discuss choice in its ideal sense: *Meaningful choice*, in which individuals have valuable options among which to choose, and choice in daily life that is unburdened by undue privacy risk.

D. Control May Be Beyond Rehabilitation

While most U.S.-based privacy scholars writing in recent years have been deeply critical of privacy-as-control, a recent thoughtful paper by Michael Birnhack has sought to rehabilitate and defend control "properly understood" in the face of such criticism.[82] As Birnhack puts it, while most discussions of privacy-as-control cause U.S. privacy scholars to "roll their eyes," because of its "failure to capture the essence of privacy and for failing us by legitimizing the collection, processing, and use of our data . . . [privacy as control] is still the best analytical framework to understand privacy."[83] Birnhack's defense of privacy-as-control (what he calls "PaC") offers an account of control by providing a history of information privacy law and data protection, situating consent's relationship to control, identifying opportunities for improving control, and rebutting or redirecting criticisms of control.[84] Beginning with the advent of modern privacy law in the early 1970s and carrying his account through to modern regulations like the GDPR and the CCPA, Birnhack identifies how the Fair Information Practices, with control as their goal, have been the

---

[79] *Id.*
[80] *Id.*
[81] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1661–64 (1999).
[82] Birnhack, *supra* note 1, at 2.
[83] *Id.*
[84] *See id*. at 6–7 (Birnhack identifies that the two leading regulatory models for privacy law—European Data Protection, which is universal in nature, and America's sectoral information privacy laws—"build on the conception of privacy as control, and translate PaC into more concrete rules, namely, FIPs, with important variations.").

basis of most modern regulatory approaches to information privacy.[85] In Birnhack's telling, control is "the beating heart of privacy law," and he offers several potential reforms to save PaC.[86] Key to his defense is the argument that we should think of privacy-as-control as operating across the lifecycle of data, from the creation of data, to its collection by entities, to the processing of the data, to its access by data subjects, to the keeping of data by entities, to its transfer to others, and finally to its deletion.[87] Birnhack terms this "continuous control," and he calls each of these points in the data life cycle "*data meeting points*," which are places at which rules, rights, and opportunities for data subjects to interact with the data can offer control across the data life cycle.[88]

While we agree with many of the normative policy suggestions in Birnhack's sincere and erudite article, we believe his account could benefit from the disentangling of control, consent, and choice that we offer as this Article's descriptive contribution. Although Birnhack thoughtfully distinguishes between consent and control, there is room to continue separating choice and control. Thus, in refuting critiques of PaC, Birnhack distinguishes control from consent and identifies instances of privacy scholars criticizing control when consent is the specific target of their ire.[89] In particular, he argues that the problem is not PaC (properly understood) but the thin gruel of notice-and-choice: "[I]n the course of their critique, the critics (unintentionally) reduce PaC to notice-and-choice/consent."[90] Birnhack contends that critics of PaC are succumbing to the naturalistic fallacy by reducing control (which has a thick, useful potential) to the thin notions of the notice-and-choice they see in practice.[91] This is consistent with what we have articulated here—consent is a type of control, but control is ultimately broader than consent, representing not just the minimum legal sufficiency for a contract, but larger notions of being able to dictate meaningful life choices.

We would go further in clearing up privacy's autonomy thicket than Birnhack does, however, by taking the additional step of clarifying the role of choice as distinct from consent and control. For example, he writes about "notice-and-choice/consent" and "Choice/Consent."[92] Although we agree with Birnhack's critique of notice-and-choice and consent, we also think there is a normative account of choice distinct from privacy as control or privacy as consent. This account has less of an emphasis about choices related narrowly to what happens with our data and more of an emphasis on providing individuals with meaningful choices about their whole lives and the ability to make these choices without taking on unreasonable privacy risks.[93] Birnhack also at least implicitly supports this notion in his critique of notice-and-choice, when he notes that consent often takes the form of "a 'take it or leave it' deal, leaving no room for negotiations, and if the user

---

[85] *Id.* at 4–9.
[86] *Id.* at 4.
[87] *See id.* at 20–21.
[88] *Id.* at 17–19 (emphasis added).
[89] *Id.* at 16–20.
[90] *Id.* at 20.
[91] *Id.*
[92] *Id.* at 10.
[93] *Infra* Part III.

takes it, it is 'as is,' leaving little room for *free* choice."[94] Separating out choice from consent and control gives space for the concept to be better developed with different versions like "free choice" or "meaningful choice" without reference to dictating what happens to your data.

While it might be descriptively true that for many, control is "the beating heart of privacy law" and "the hallmark of current data protection and its backbone," we think choice gets short shrift in this account.[95] The confusion wrought by privacy's autonomy thicket introduces a tension in Birnhack's defense of privacy-as-control. Birnhack is careful to deemphasize control's role as merely a justification, rationale, or aspiration of privacy:

> [Privacy-as-control] is not a justification of privacy or a rationale thereof, neither is it a definition of privacy. Rather, PaC is a conception of privacy, an overarching privacy theme, serving as the common denominator of several theoretical justifications.[96]

Like this article, Birnhack summarizes the criticisms of consent and control, and he advocates for supplemental measures to address consent's and control's many failings.[97] However, looking to strengthen control over personal data could cause lawmakers to overlook other, more promising justifications for pursuing non-control based reforms that still seek to promote autonomy.[98] Adding to this the (im)practical burdens that even sincere PaC places on consumers, we believe that the better strategy, acknowledging the practical impossibility of individual control at scale, is to recognize control's limits and pursue meaningful life choices free from unreasonable privacy risk instead.

Lest we overstate our differences with Professor Birnhack, we emphasize that his own account seems consistent with the goal of meaningful choice. At multiple points, Birnhack identifies opportunities for additional reforms to supplement and strengthen privacy-as-control.[99] For example, in discussing privacy's relational aspect, Birnhack notes how privacy with respect to regulated professions facilitates trust and promotes human flourishing:

> Privacy facilitates trust also in professional settings, such as in a patient-physician relationship. Without privacy, patients may not reveal all relevant data, either for fear of negative effects or because of shame and stigma, unfortunate as they may be. Privacy entrusts the power in the hands of the patient, granting the patient some power to construct the relationship.[100]

What makes information sharing in such relationships possible, however, is the existence of substantive requirements that are not based on consent or control.[101] Regulated professions such as medicine and law impose fiduciary duties of care, confidentiality, and loyalty on professionals. These duties have little to do with control, but they do free people to reveal what they want to their doctor because they are protected by a layer of rules no matter what they choose to share. Choices

---

[94] Birnhack, *supra* note 1 at 13.
[95] *See id.* at 5, 9, 20 (leveling the same criticism at critiques of consent).
[96] *Id.* at 46.
[97] *Id*.
[98] *See id.* at 16.
[99] Birnhack, *supra* note 1.
[100] *Id.* at 33.
[101] Julie E. Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQUIRIES IN L. 1 (2019).

in such circumstances about information disclosure are thus protected by substantive limits rather than the thin proceduralism or notice-and-choice or even consent.

Thus, while we agree with many of Birnhack's suggested improvements to control, we disagree with his normative conclusion that "the emphasis on the social aspects of privacy should and can supplement PaC rather than supplant it."[102] Moving towards a social model of privacy that promotes meaningful choice does not necessarily require abandoning all attempts at control over data, but any such control rights should be second-order at best and recognize both the pathologies of consent and the social dimensions of privacy which mean that privacy should be more than an aggregation of billions of individual choices, even "rational" ones.[103] Even Birnhack's demand that control needs to be continuous will not be meaningful if it does not create the conditions for individuals to have multiple desirable outcomes to choose from, or if it places unreasonable monitoring or choosing obligations on people in order for them to protect themselves. Meaningful choice or continuous control will in any event require substantive limits on data processing separate and apart from those that individuals choose to exercise through their control rights. After all, one of the great shortcomings of control models is that rights that have to be exercised to take effect have no effect if they are not (or cannot) be exercised meaningfully by people in practice. In such circumstances, a right that you cannot exercise is arguably worse than no right at all.

***

What privacy law should idealize, above consent and control, is having meaningful choices for significant life opportunities. This means more than just having choices about whether and with whom to share information about yourself, but the ability to make choices free of undue privacy risks by there being substantive rules that curtail exploitative data practices by default.[104] And those choices should not just be meaningful, but exercised in an environment of protective rules that take unsafe choices off the table and protect privacy (and human autonomy) by default. To promote individuals' autonomy, a privacy legal regime should idealize choice by fostering trust in digital markets through flexible, substantive duties and bright-line rules and prohibitions that prevent harmful or coercive data practices. We have teased this idea in the previous sections, but now is the time to spell it out. It is to that framework of substantive, protective rules for digital consumers that we now turn.

III. How Meaningful Choice Better Promotes Privacy Autonomy

Recall that in Part II, we distinguished thin and technical definitions of *choice* from *meaningful choice*, which we defined as creating the conditions for individuals to be presented

---

[102] Birnhack, *supra* note 1, at 45.

[103] For recent scholarship articulating theories of privacy in social terms, see, e.g., Priscilla Regan, *Privacy and the Common Good: Revisited*, *in* Social Dimensions of Privacy 50 (Beate Roessler & Dorota Mokrosinska eds. 2015); Priscilla M. Regan, Legislating Privacy: Technology, Social Values, and Public Policy (1995); Joshua A. T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 Duke L.J. 385–457 (2015); Solove & Hartzog, *Kafka*, *supra* note 2; Neil Richards, Privacy's Social Dimensions, (unpublished manuscript) (on file with author).

[104] *See* Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 Wash. U.L. Rev. 961 (2021) (providing more information on exploitative practices).

with multiple desirable choices to fulfill the purpose of an information relationship in contrast to the kind of binary take-it-or-leave it options that are frequently offered by consent or control. Moreover, we argued that meaningful choice at the collective level requires placing substantive limits on excessive and harmful data practices, thereby enabling people to make choices in daily life that are unburdened by undue privacy risk. In that way, people would be able to choose in a digital environment without worrying about betrayal or having one hand on their proverbial wallet.[105] We then explored how consent and control, as they exist today in practice, fail to deliver meaningful choice. Disentangling privacy's autonomy thicket, however, requires more than merely rehashing the insufficiency of consent and control. At the risk of pushing the metaphor too far, clearing the brush leaves a gap for a new planting. In this section, we fill the gap we have created and sketch out what a regime of meaningful choice for digital consumers might look like.

A. Reframing Meaningful Choice: Personal and Collective Choice

For reasons we have already explained, relying on the overwhelming scholarly evidence, modern technologically-mediated commercial relationships cannot deliver on their promises of control and gold standard consent at scale. But the failure of these concepts presents an opportunity to ask better questions with respect to choice and privacy.

Privacy's autonomy thicket—the muddled and inconsistent articulation of consent, control, and/or choice as the goal of privacy law—is often grounded in the idea that individuals should have autonomy *over their privacy*, which entails making choices with respect to their data, exercising control over their information, or consenting to data practices. This takes the broad liberal concept of private choice and, in the context of privacy, whittles it down into the narrow set of choices we make with respect to how entities collect, use, and share information about us. But we would suggest that if we really care about empowering people, a first-order strategy of *trying to maximize choices with respect to what is done with our data is the wrong approach entirely*, as it focuses on the trees rather than the forest as a whole. Rather than focusing so narrowly on the data that companies are so keen to collect and use for their profits, we believe that we should take a step back and shift our focus back towards autonomy in a broader sense.

Privacy is often justified as an instrumental value that enables us to make choices in daily life—choices over who we are, what we read, how we worship, who we love, what products and services we use, and more. This is a broad autonomy-based articulation of the goals of privacy law, at some distance from the thin, crabbed, muddled and ultimately disempowering autonomy thicket approach. The normative consequence of disentangling privacy's autonomy thicket, we believe, should be a shift towards maximizing these meaningful kinds of choices within the context of relationships—the liberal conception of private choice in the broad sense as opposed to only choices over our data. Put another way, we should ask whether people are actually given desirable choices in their information relationships rather than over-worked and ground down to resignation

---

[105] *See supra* Part II.A.

by the impossible challenge of being "in control" of their data.[106]

Separating choice from consent and control allows lawmakers to focus on the many different choices people make in their data-heavy relationships with other people and organizations.[107] We make decisions constantly. A simple trip to the grocery store involves choice of store, route, whether to use a navigation service such as GPS, app-enabled parking payments, which products to buy, whether or not to participate in a loyalty program, and so forth. We form information relationships with companies providing turn-by-turn directions, states collecting tolls with the assistance of license plate readers, the operating system of our "smart car," the interface (like Apple Car Play) between our phone and the car, our credit card company, our grocery store's "loyalty program," and more.[108] Each of these relationships has a purpose, and usually needs some modicum of data to effectuate that purpose. While privacy might be salient in some aspects of these relationships, such as opt-in involvement in a loyalty program, it isn't something that occurs to most of us as we make most of our choices each day, even for the most privacy-conscious people. (Did you read all of the privacy policies for each of these services carefully? No one does, because it is a practical impossibility. And these are just the services you use when you drive to the shops.)

This decisional complexity affects choices outside the consumer privacy context as well. Consider employment. For a wide swath of people, an employer's privacy policies are unlikely to be a deciding factor in the decision to accept, or remain in, a job. Employment decisions are a complex function of an individual's skills, aptitude, inclination and interests, educational background, prior work experience, pay demands, existing resources, personal criteria such as location, work-life balance and flexibility, benefits, and so much more. There is a power imbalance between employer and employee that complicates employment decisions as well. Losing an employee is often a lesser pain to an employer than switching jobs is for an employee. Switching jobs, let alone leaving a job without an alternative lined up, is fraught with peril and financial risk. Against that backdrop of inequality, it feels theatrical to individuals to consent to data practices or somehow exercise controls to limit their employer's surveillance. And this analysis can be extended to many other contexts as well, such as the learning management system at schools, the privacy practices of a new range of "smart" appliances from ovens to boilers to wi-fi-enabled BBQ smokers, and many, many others. As more and more commercial and government services become app-enabled, the problem of privacy which once was restricted to the now-quaint world of "cyberspace" is now a problem in virtually every important relationship in our lives.

If we really want privacy law to help people, it should relieve them of the burden of fretting over what happens with their data and leave them to the business of making choices that further their goals for data-intensive relationships. This would further individual autonomy goals while

---

[106] Solove, *supra* note 38, at 1893.
[107] *Id.* at 1896–97.
[108] Thorin Klosowski, *Big Companies Harvest Our Data. This is Who They Think I Am*, N.Y. TIMES (May 28, 2020), https://www.nytimes.com/wirecutter/blog/data-harvesting-by-companies [https://perma.cc/7M6M-48ZT].

also allowing lawmakers to focus on privacy rules that target design, infrastructure, mental health, discrimination, and other factors that advance social and collective virtues.

B. Providing Meaningful Choice Requires Substantive Duties and Rules Prohibiting Privacy-Invasive Practices

Insofar as promoting autonomy is the goal of privacy law—to support the intellectual freedom, identity formation, and individualism necessary for human flourishing in a democratic society—policymakers should prioritize ensuring that people have meaningful choice over control or consent. Broadly, this requires lawmakers taking Julie Cohen's advice to "turn privacy inside out" by "focusing on the conditions that are needed to produce sufficiently private and privacy-valuing subjects."[109] For Cohen, this means a regulatory focus "on the design, production, and operational practices best suited to instantiate and preserve those conditions."[110] In order to create the sort of environment where people can make meaningful life choices unburdened by unreasonable privacy risks, lawmakers should embrace substantive interventions, such as reforms to corporate governance, imposition of strong duties of care and loyalty, regulation of unfair, deceptive, and abusive design practices, and bright-line prohibitions on inherently harmful or unreasonably risky acts or practices.

Michael Birnhack recognizes as much in his defense of PaC. For example, in arguing that control is more than just consent and the initial meeting point between data subject and controller, he praises many existing substantive requirements of the GDPR that "supplement and strengthen control," such as requirements concerning lawful bases, data minimization requirements, purpose limitation, onward transfer restrictions, and privacy-by-design.[111] Imposing duties on controllers that require no action or input by the data subject is not strengthening control; it is recognizing control's limits and prioritizing meaningful choice.[112] Going further, Birnhack advocates for "prohibiting commercial practices that are meant to induce people to provide data about others without sufficient justification."[113] These interventions go beyond control, and thinking about how they affect our autonomy and freedom of choice independent of requests for consent and specific controls could help clarify when such interventions are appropriate.

Prioritizing meaningful choice also means lawmakers should embrace Anita Allen's argument that in some circumstances, privacy should be mandated because "[p]rivacy is too important to be left entirely to chance and taste."[114] Allen argued that while lawmakers should pass laws that help ensure that others leave us alone, it might be equally important to "create and preserve forms of privacy to which we may be unwisely indifferent that are nonetheless important

---

[109] Cohen, *supra* note 101.
[110] *Id.* at 3.
[111] Birnhack, *supra* note 1, at 20–21.
[112] *See* Solove & Hartzog, *Kafka*, *supra* note 2, at 1029 (identifying elements of GDPR that align more with the Societal Structure Model than informational self-determination).
[113] Birnhack, *supra* note 1, at 36.
[114] ANITA ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 197 (2011).

to lives of opportunity promised by a free and democratic society."[115] According to Allen, there are all sorts of understandable reasons we might be unwisely indifferent to our own privacy, and it's natural to fear a paternalistic government response.[116] But according to Allen, the sort of modest paternalism she is suggesting "is consistent with—and indeed required by—a robust liberalism, appreciative of the respects in which unchecked losses of privacy can leave one, in the words of an historic judicial opinion, slave to merciless masters."[117] And even when privacy is not strictly mandated, requirements that defaults for information collection be set in privacy-protective ways are a good place to start. Such rules are by no means foreign to U.S. law; in fact, they are the foundation of health privacy under the HIPAA Privacy Rule. Under that regime, health information collected as part of a medical treatment underwritten by health insurance is allowed to flow for purposes of the treatment of patients, the payment of bills, and the operation of hospitals and health systems, but anything else requires informed consent in the form of a written, gold-standard consent known as a HIPAA authorization.[118] Beyond the narrow context of treatment (for which consent is presumed), the defaults have been set in a privacy-protective direction for decades, with undeniable benefits to the trust and effectiveness of our health care system.

Disentangling privacy's autonomy thicket provides new tools for evaluating the effectiveness of novel legal requirements in promoting individual autonomy. Take, for example, the recent shift in U.S. state privacy legislation from procedural to substantive data minimization.[119] Of the nineteen U.S. state to enact "comprehensive" consumer privacy laws, fourteen have procedural data minimization rules that require companies to limit their collection of personal data to what is "adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer."[120] Advocates and scholars have long argued that such rules entrench notice-and-choice and have called for stronger rules that place meaningful, substantive limits on data aggregation rather than requiring firms to merely go through the procedural motions of notice-and-choice. In recent years, state lawmakers have taken heed.[121] A handful of recently-enacted laws, such as Washington's My Health My Data Act, the New York Child Data Protection Act, and the Maryland Online Data Privacy Act, include substantive data minimization rules that, subject to some variation and exceptions across these laws, go further and

---

[115] *Id.*

[116] *Id*. ("We may be unwisely indifferent to our own privacy because we are young, or because we are busy, or because we are unfamiliar with the risks of data collection, sharing, and storage that come with the mysterious technology we enjoy.").

[117] *Id*. (citing Pavesich v. New England Life Ins. Co. 50 S.E. 68 (Ga. 1905)).

[118] *See* Kirk Nahra, *HIPAA Privacy and Security for Beginners*, WILEY REIN LLP (July 2024), https://www.wiley.law/newsletter-5029 [https://perma.cc/MEC9-PHJS].

[119] *See generally* JORDAN FRANCIS, DATA MINIMIZATION'S SUBSTANTIVE TURN: KEY QUESTIONS & OPERATIONAL CHALLENGES POSED BY NEW STATE PRIVACY LEGISLATION (FUTURE OF PRIVACY FORUM, 2025), https://fpf.org/wp-content/uploads/2025/06/FPF_Data-Minimization.pdf [https://perma.cc/EX7V-VCDM].

[120] DEL. CODE ANN. tit. 6 § 12D-106 (a)(1) (2025); *accord* COLO. REV. STAT. § 6-1-1308(3) (2025); CONN. GEN. STAT. § 42-520(a) (2024); IND. CODE § 24-15-4-1(1) (2024); KY. REV. STAT. ANN. § 367.3617(1) (West 2025); MINN. STAT. § 325M.16, subd. (2) (2025); MONT. CODE ANN. § 30-14-2812(1) (2025); NEB. REV. STAT. § 87-1112(1) (2025); N.H. REV. STAT. ANN. § 507-H:6(I) (2025); N.J. STAT. ANN. § 56:8-166.12(a) (West 2025); OR. REV. STAT. § 646A.578 (2025); TENN. CODE ANN. § 47-18-3305(a) (2025); TEX. BUS. & COM. CODE ANN. § 541.101(a) (West 2025); VA. CODE ANN. § 59.1-578(A) (2025).

[121] Jordan Francis, *Unpacking the Shift Toward Substantive Data Minimization Rules in Proposed Legislation*, IAPP (May 22, 2024), https://iapp.org/news/a/unpacking-the-shift-towards-substantive-data-minimization-rules-in-proposed-legislation [https://perma.cc/4SD7-BL55]; FRANCIS, *supra* note 119.

limit the collection and processing of personal data to what is reasonably or strictly necessary to provide or maintain a requested product or service.[122]

Conceptually, these substantive data minimization rules that advocates and scholars have called for are not all that different from notice-and-choice. Under both frameworks, individuals engage in the market and, by virtue of selecting specific products of services, implicitly consent to the collection, use, and disclosure of their personal data for certain purposes. Under notice-and-choice, those permissible purposes are determined solely by the business based on the terms it buries in its privacy policy. Under a substantive data minimization rule approach, however, the permissible purposes are tied to the functionality of the product or service, which limits companies' ability to engage in exploitative and unnecessary data practices. Simply hiding a vague term in a privacy policy that few read or understand would no longer be enough. Substantive data minimization requirements therefore aim to align data practices with consumers' reasonable expectations, in the same legal tradition as the now-venerable HIPAA Privacy Rule. In contrast to notice-and-choice, which fails to protect individuals from the structural power imbalances that businesses have, substantive data minimization rules are designed to be autonomy-preserving by allowing consumers to safely interact in markets without powerlessly or accidentally submitting to undue privacy risks or one-sided data extraction simply as a cost of participation in modern life.

It remains to be seen whether substantive data minimization requirements are a temporary experiment or if they will take root more broadly in American privacy laws. There are also many issues to resolve, such as the scope of what data is necessary to provide a requested product or service and the difference between reasonably and strictly necessary uses.[123] But in combination with other substantive reforms, such rules could promote people's meaningful choice by reducing the unreasonable expectations of privacy-self-management.

C. Disentangling Privacy's Autonomy Thicket is Necessary for Navigating a World Increasingly Reliant on Artificial Intelligence

The last few years have seen the rapid development, dissemination, and deployment of artificial intelligence seemingly across all walks of life.[124] This technological tide has made untangling privacy's autonomy thicket more urgent than ever, if we want people to be able to preserve their autonomy and be empowered to navigate an AI-mediated world on their own terms. Just as in traditional privacy contexts, consent and control are inadequate to promote true accountability and choice for individuals when dealing with AI.[125] Similarly, procedural approaches to data minimization will pose but a trivial obstacle to the rhetorical imperative to

---

[122] Md. Online Data Privacy Act, 2024 Md. Laws 454; N.Y. Child Data Protection Act, 2024 N.Y. Laws 121; 2023 Wash. Legis. Serv. Ch. 191.
[123] FRANCIS, *supra* note 119.
[124] *See* Anisha Sircar, *3 Years After ChatGPT's Launch, The AI Rush Has Only Just Begun*, FORBES (Dec. 2, 2025, 7:21 AM), https://www.forbes.com/sites/anishasircar/2025/12/01/three-years-after-chatgpts-launch-the-ai-rush-has-only-just-begun [https://perma.cc/ZG9L-PYQU].
[125] *See* Lina M. Khan et al., *After Notice and Choice: Reinvigorating "Unfairness" to Rein In Data Abuses*, 77 STAN. L. REV. 1375 (2025) (discussing on consent and control in traditional privacy contexts).

collect all personal data in order to better train AI models.[126] These facts are true regardless of which of the many distinct technologies we might mean when we use the vague umbrella term of "AI"—whether we mean is consumer facing generative-AI products such as chatbots and text-to-video generators, deepfake tools, automated decision-making systems that facilitate consequential decisions, use of agentic AI, or private or government surveillance by facial recognition.[127] AI systems are infamously opaque and difficult to explain, factors which compound many of the pathologies that plague consent.[128] And as we have noted, their data-hungry nature creates the incentive to bury "we will train AI" permissions in privacy policies—a phenomenon that has already started to happen in practice.[129] Control, too, is inadequate to deal with AI's challenges to privacy law. As with other digital products and services that have come before, these tools are often foisted upon individuals and give them little say over whether and how they are deployed. As authors, we had no control over whether our prior work (copyrighted or otherwise) was used to train AI models, and as consumers, we have little control over whether our use of (for example) generative AI will be used to train and refine those models. AI's powerful ability to generate inferences further erodes the effectiveness of an individual control model.[130]

Preserving individuals' autonomy in the age of AI therefore requires promoting choice through a variety of substantive legal interventions.[131] Requiring that agentic AI systems serve the best interests of their users, subject to safeguards for public safety, could be vital in preventing self-dealing and exploitation by developers. Confidentiality requirements as a default for AI chatbots could prevent inadvertent data leakage or intentional disclosure to law enforcement.[132] Outright prohibitions on harmful deepfakes, one-to-many facial recognition systems, and surveillance pricing may also be necessary to protect our collective autonomy.[133] Automated

---

[126] *See* Thomas Lambert, *Data Minimization Strategies: A Comprehensive Guide*, PDTN (Aug. 27, 2025), https://pdtn.org/data-minimization-strategies [https://perma.cc/5CKB-RRW2] (providing information on implementing data minimization).

[127] *See* ARVIND NARAYANAN & SAYASH KAPOOR, AI SNAKE OIL: WHAT AI CAN DO, WHAT IT CAN'T, AND HOW TO TELL THE DIFFERENCE (Princeton Univ. Press 2024) (providing examples and discussion of different applications of AI).

[128] *See* Lou Blouin, *AI's Mysterious 'Black Box' Problem, Explained*, UNIV. OF MICH. DEARBORN (Mar. 6, 2023), https://umdearborn.edu/news/ais-mysterious-black-box-problem-explained [https://perma.cc/CY5E-BZTC] (explaining the "black box" problem, referring to the difficulty in understanding how AI systems operate).

[129] *See, e.g.*, *Privacy Policy*, LINKEDIN (Nov. 3, 2025), https://www.linkedin.com/legal/privacy-policy [https://perma.cc/6LU6-H66C] ("We may use your personal data to improve, develop, and provide products and Services, develop and train artificial intelligence (AI) models, develop, provide, and personalize our Services, and gain insights with the help of AI, automated systems, and inferences, so that our Services can be more relevant and useful to you and others."); *see also* Brandon Vigliarolo, *You Have One Week to Opt Out or Become Fodder for LinkedIn AI Training*, REGISTER (Oct. 27, 2025), https://www.theregister.com/2025/10/27/linkedin_ai_profile_scraping (covering the broader global rollout of default settings enabling personal data to be used for AI training unless an individual opts-out).

[130] Solow-Niederman, *supra* note 24.

[131] *See* Solove & Hartzog, *Kafka*, *supra* note 2.

[132] *See* Nils Gilman, *If You Tell ChatGPT Your Secrets, Will They Be Kept Safe?*, N.Y. TIMES (Nov. 10, 2025), https://www.nytimes.com/2025/11/10/opinion/chatbot-conversations-legal-protection.html [https://perma.cc/Z5UD-VAL9] (advocating for "A.I. interaction privilege," subject to the conditions that (1) "communications with the A.I. for the purpose of seeking counsel or emotional processing should be protected from forced disclosure in court;" (2) the privilege "must incorporate the so-called duty to warn principle;" and (3) "there must be an exception for crime and fraud"); *but see* Alicia Solow-Niederman, *AI and Doctrinal Collapse*, 78 STAN. L. REV., at *50 (forthcoming 2026) (noting how doctrinal collapse between information privacy law and copyright law enables AI companies to strategically invoke user privacy to evade discovery in copyright litigation).

[133] *See* Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOYOLA L. REV. 101 (2019); Mayu Tobin-Miyaji, *Kroger's Surveillance Pricing Harms Consumers and Raises Prices, With or Without Facial Recognition*, ELEC. PRIV. INFO. CTR. (Feb. 14, 2025), https://epic.org/krogers-surveillance-pricing-harms-consumers-and-raises-prices-with-or-without-facial-recognition [https://perma.cc/2A3T-SBXE].

decision-making systems must be deployed only alongside technological due process rights that ensure appropriate transparency, governance, and rights such as correction, opt-outs, or appeals.[134]

CONCLUSION

Calls for substantive reforms to American privacy law, such as the imposition of fiduciary duties and strong default protections for humans and their data will struggle to advance as long as proponents of control and consent frameworks can frame substantive proposals as being "anti-choice" and then offer only weak procedural rules and the failing notice-and-choice regime in return. Privacy's autonomy thicket—the conflation and imprecise use of choice, consent, and control in policy debates—frustrates meaningful, substantive privacy reform that places the human rights of individuals over the business interests of companies. Most pointedly, it clouds our understanding of how it is really notice-and-choice that frustrates our ability as consumers to make meaningful choices about the ways our data is processed and how that affects our lives.

Americans rightly value their autonomy and freedom of choice, but current privacy law typically offers only a weak caricature of these goals in practice. To the extent that informational privacy facilitates autonomy, it is by granting meaningful choice over our actions in informational relationships. This comes not through privacy-as-control—which is overwhelming and illusory—nor consent—which is impossible and insufficient in constructed environments with unequal power dynamics. Instead, it comes via the kinds of substantive reforms that leave humans protected regardless of the choices they make and that limit companies from engaging in unnecessary and exploitative collection, use, and disclosure of our personal information. That, and not notice-and-choice or the illusion of privacy-as-control, is the best path to something approaching real autonomy for digital consumers and citizens.

---

[134] Danielle Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1305–13 (2008).