Neil Richards
Koch Distinguished Professor of Law
Director, Cordell Institute for Policy in Medicine & Law
Washington University in St. Louis
February 4, 2026

Members of the Vermont General Assembly, my name is Neil Richards, and I am delighted to have the opportunity to talk to you this morning about privacy law and privacy reform, topics that I have studied extensively for the past 25 years. I am the Koch Distinguished Professor of Law at Washington University, where I co-direct the Cordell Institute for Policy in Medicine & Law, a center focused on the issues of health and human information policy that I understand to be on the legislative agenda in the great state of Vermont this session. I am the author of dozens of articles and two books on privacy, including my 2022 book *Why Privacy Matters*.[1] I have also testified about these issues before Congress or otherwise offered my expertise in many high-profile privacy cases,[2] including serving this summer as the court-appointed Consumer Privacy Ombudsman in the closely-watched 23andMe genetic data bankruptcy,[3] to articulate the public interest in data protection.[4]

I am not a lobbyist. I am not being paid to be here today, and the views I express are my own and not those of my university or of the center I direct. I am

[1] NEIL RICHARDS, WHY PRIVACY MATTERS (Oxford Press 2022).
[2] *AI at a Crossroads: A Nationwide Strategy or Californication?*: Hearing Before the Subcomm. on Courts, Intell. Prop., Artificial Intelligence, and the Internet of the H. Comm. on the Judiciary, 119th Cong. (2025) (written testimony of Prof. Neil Richards) [hereinafter *AI at a Crossroads* Hearing]; Neil M. Richards, Woodrow Hartzog & Jordan Francis, Comment on Trade Regulation Rule on Commercial Surveillance and Data Security, FTC Docket No. FTC-2022-0053-1071 (Nov. 21, 2022), https://www.regulations.gov/comment/FTC-2022-0053-1071 [hereinafter Cordell Institute FTC Comment].
[3] Cassandre Coyer, *23andMe's Genetic Data Trove Rests on Professor as Protector*, Bloomberg L. (May 22, 2025), https://news.bloomberglaw.com/privacy-and-data-security/23andmes-genetic-data-trove-rests-on-professor-as-protector.
[4] Report of Consumer Privacy Ombudsman, at 44, *In re 23andMe Holding Co.*, No. 25-40976-357 (Bankr. E.D. Mo. June 11, 2025) (report of Neil M. Richards), ECF No. 718, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5476672.

here to share what I have learned studying privacy in the decades since the early days of the Internet, and from deep study of the interdisciplinary academic literature on privacy, a field I helped to create.

My views are also shaped by the fact that my 19-year-old son Declan is a Vermonter. He's a sophomore at Middlebury, and he plans to remain in Vermont and teach English after graduation. I love this state, and I want to help you make good decisions to protect the privacy of your constituents in ways that also build the consumer trust your businesses need to thrive in the long term.[5]

These are hard and important questions, and I am grateful that this body is interested in exploring them, in doing something meaningful about them, and in doing the *right* thing, not necessarily the easy thing, which would be doing nothing or following the herd of other states that are largely passing ineffective and under-protective "comprehensive" privacy laws. So I want to try to help this morning by offering some high-level observations about privacy, privacy law, and privacy reform. I understand that my colleagues – and you have a world-class group of thoughtful scholars and other experts speaking to you today – will be going into greater detail. But I want to offer three points to kick us off:

- First, I will explain why privacy matters.
- Second, I will explain why the research suggests that we need better privacy laws.
- Third, I will offer what I think are the two essential elements of any privacy law that is likely to protect consumers. These elements are (1) *substantive consumer protections* and (2) *meaningful remedies*.

First, **why privacy matters**. As I explain at length in my book, privacy matters because information is power and information about people confers power over those people.[6] We need privacy over our personal information to develop our identities, to participate as free citizens in a democratic society, and to be able to

[5] Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. (2016).
[6] RICHARDS, *supra* note 1.

participate as consumers in a digital economy free from manipulation, exploitation, and exposure.

Now some people will tell you that human data is necessary for our economy, for "innovation," or to train AI models. That might be true to some degree, but the people of Vermont do not deserve to have their lives as open books to marketers and data scientists, AI developers, police, masked federal immigration agents, or other entities who seek information about them. A right to privacy is a fundamental right necessary for any decent democratic society,[7] and that right should be extended to protect ordinary people from corporate uses of human data as well as from government uses.

The burden of constant privacy vigilance should not be put solely on ordinary people to protect their privacy from all the entities that are seeking their data for whatever purposes. Moreover, as I have explored in a series of articles with Prof. Hartzog, whom you'll hear from next, good privacy rules are necessary to build the trust businesses need to thrive.[8] Just as with doctors and lawyers, if we have real trust in the entities we share our data with, we will share more data, and everyone is better off. But *real privacy protections are necessary* if this is to happen. And that's why privacy matters.

The second thing I want to talk about this morning is **why we need better laws to protect our privacy**. I was in law school when the Internet came into ordinary people's lives, so I have been with the questions of law, policy, and the digital revolution from the beginning. During the dot-com era, the basic regulatory idea was that people might have varying privacy preferences, so companies could write down their privacy practices in a privacy policy, people could read that policy, and they could make privacy choices as a result. This has been the default approach

[7] RICHARDS, *supra* note 1; Neil Richards & Woodrow Hartzog*, Privacy's Trust Gap*, 126 YALE L.J. 1180 (2017).

[8] Richards & Hartzog, *Taking Trust Seriously*, *supra* note 5.

to privacy regulation in the US, and both common sense and the overwhelming weight of scholarly evidence reveal that it has been a *colossal failure*.[9]

People don't read privacy policies because they simply can't.[10] There are too many of them from too many companies they encounter – comprising hundreds and hundreds of pages of complicated text that is both dense and vague at the same time. Ask yourself – have you read the privacy policy for your ISP, your email provider, your search engine, your cloud provider, your AI assistant, your car's operating system, your bank, your grocery store loyalty program, your child's learning management system, or any of the other dozens of businesses that hold your data? Do you know who they share with? There are more of these than any consumer can read, much less understand.[11] And if you do read one of these policies, you'll find it to be simultaneously dense, vague and unhelpful.

People struggle to remember their passwords – how can we expect them to remember dozens of sets of terms of service and what their answers are to their constantly-changing settings? The answer is that we cannot, and this form of self-regulation that we call *notice and choice* has been a catastrophic failure, offering the fiction of protection that masks a practical reality in which companies have the ability to run roughshod over the privacy of every Vermonter.[12] This is an unreasonable and unacceptable burden to place on already harried consumers who are just trying to live their lives and not work out a fiendish puzzle of corporate legal and technical obfuscation.

Other states have passed so-called "comprehensive" privacy laws, but most of the ones to date make the problem worse by merely rubber-stamping industry practice and keeping the burden of privacy protection on already confused and over-burdened consumers to read, understand, and then take affirmative steps to protect

[9] Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461 (2019); Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32 (2011); Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013).

[10] Richards & Hartzog, *Pathologies, supra* note 9.

[11] *Id.*

[12] *Id.*; *see also* Cordell Institute FTC Comment, *supra* note 2.

their privacy.[13] The obligation to protect privacy by design and by default should instead be placed on the powerful companies who collect, process, and often sell vast amounts of personal data, rather than on the harried individual consumers who are just trying get on with their busy days.

Vermont can do better. In fact, Vermont can be a leader in this area. What we need is privacy law that sets reasonable rules of the road for businesses using our data. We don't have that yet in the United States, which is shameful. And let me be clear: If the past twenty-five years of one privacy and security scandal after another have taught us anything, it is that companies cannot be trusted to safeguard our data without rules of the road.[14] Just as we don't trust motorists to drive cars safely without speed limits and traffic signs; we don't trust lawyers with unregulated access to our secrets; we don't trust doctors with unregulated access to our medical data; and we don't trust banks with unregulated access to our money.

Good regulation and innovation are not inconsistent. While we can certainly debate how much regulation (and what kind) is appropriate, having no new regulations at a time of rapid change would be a disaster. Additionally, if innovation is as magical as industry says it is, it can still do good things while respecting the policy choices of the people's elected representatives. In this way, the *necessity* required by reasonable regulation has been and should continue to be the *mother of invention*. Good regulations take dangerous or disloyal business practices off the table, and they give companies incentives to compete fairly by serving their customers better, rather than competing on who can make the most money exploiting them and their data.[15]

This brings me to my third and final point: **What are the essential elements of a good privacy bill**? I'm not here to endorse any one bill over

[13] See, *e.g.*, Electronic Privacy Information Center & U.S. PIRG Education Fund, *The State of Privacy: How U.S. State "Privacy" Laws Fail to Protect Privacy and How We Can Do Better* (Jan. 2025), available at https://epic.org/wp-content/uploads/2025/04/EPIC-PIRG-State-of-Privacy-2025.pdf.

[14] *See* Richards, *supra* note 1; Cordell Institute FTC Comment, *supra* note 3.

[15] Woodrow Hartzog & Neil Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 356 (2022).

another, but it should be clear by now that my view, as well as the view of the large community of privacy scholars, is that a bill that just doubles down on notice and choice is not enough.[16] Any bill that relies on having people read dozens and dozens of privacy policies and then makes them take affirmative steps with dozens and dozens of companies is not remotely enough to empower consumers, much less to protect them and their families. No bill would be better than a bill of this kind that would offer only the illusion of protection, while having the effect of rubber-stamping dangerous corporate data practices.

I think that instead there are two elements that a good privacy bill should have – they are ***substantive restrictions on dangerous data practices*** and ***meaningful enforcement by both the government and private citizens***. First, a good privacy bill needs *substantive restrictions* on what companies can do with personal data rather than acting as merely a recipe for extracting permission from confused consumers. One essential *substantive restriction* is what we privacy lawyers (in the academy, in practice, and among regulators) call *data minimization*. Data minimization means you only collect the information you need to provide a service, and you delete unnecessary data when you're done with it. Data that isn't needed shouldn't be collected, because then the data that isn't collected can't be misused, taken by law enforcement, or leaked in an inevitable data breach.

Another different kind of substantive restriction is a duty of data loyalty. This requires that, while human data can be used to provide a service, it cannot be used to betray or act contrary to the best interests of the consumer.[17] These are the kinds of obligations that our law has placed on doctors, lawyers, corporate officers, agents, trustees, and other powerful entities for literally centuries, and they would work wonders if we wanted to be serious about protecting people from the powerful companies that process their data and increasingly come to shape their very lives.[18]

[16] *See, e.g.*, Richards & Hartzog, *Pathologies*, *supra* note 10; Nissenbaum, *supra* note 11; Solove, *supra* note 12; Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 Stan. Tech. L. Rev. 74, 131 n.4 (2018) (noting that "the critiques of Notice and Choice are too voluminous to list").

[17] Hartzog & Richards, *Legislating Data Loyalty*, *supra* note 15.

[18] *Id.*

Substantive restrictions like data minimization and data loyalty are essential because they take dangerous data practices off the table, and they require companies to use consumer data for good purposes like serving their customers rather than exploiting them or betraying them.

Besides substantive restrictions, the second essential feature of a good privacy bill is *meaningful enforcement*. This has two elements. The first of these is enforcement by the government, such as the Vermont AG's Office, which has a long and proud history of consumer protection, and which should be allowed to continue to protect the privacy and security of Vermonters with appropriate resources. But the second of these is a private right of action that lets people (in this case Vermonters) whose rights have been violated sue to enforce those rights.

Tech companies hate private rights of action, and they devote millions of dollars to pay lobbyists who will tell you how awful they are. But by opposing private rights of action, the companies are essentially saying that they should be able to break the law and harm people, and that those harmed people will have no recourse other than to complain to the government. What this really means is that tech companies want to be able to break the law and have no consequences for doing so. It's the opposite of regulation—it's an invitation to misbehave, and one that this body should not permit.

If you want to make a law ineffective, just make it unenforceable. That's when it will be ignored, and that's the gospel that the tech lobbyists are preaching. But that's a recipe for lawlessness – the same kind of under-regulated Wild West of data exploitation that has gotten us into this mess and diminished the trust that people have in the companies that use their data. Such a world is bad for everyone – including well-meaning companies – in the long run.

By contrast, a law that creates protections (in this case for privacy) needs to have some mechanism that makes sure that those protections are respected. This is what private rights of action do, and what they have done in our law for centuries. Indeed, the foundation of American law itself—*Marbury v. Madison*—famously restated the ancient legal principle that for every right there should be a remedy.[19] That's all private rights of action are, and they are only controversial in privacy reform because rights of action are what makes law work. A privacy law without a private right of action is likely to be a toothless law, as state attorney general offices are already small and overworked.

Let me conclude by thanking you for your time, and offering one final observation. When it comes to privacy, the worst thing that this body could do would actually not be doing nothinging. Doing nothing is only the second-worst thing you could do. The first-worst thing you could do would be to pass a weak privacy bill – one that lacks substantive protections or lacks meaningful enforcement like a private right of action. Such a law would create the illusion that privacy had been protected, but it would merely rubber-stamp the kinds of exploitative and unfair trade in personal data that the privacy law purported to fix. It would place an unreasonable burden on ordinary Vermonters to protect their privacy in an impossible game that is rigged against them. It would create the illusion that privacy reform had happened, and that the legislature could move on, even though the problem hadn't been fixed. And this is particularly a problem in the tech sector, because privacy is today's legislative problem, but tomorrow's will be AI.

A good privacy law will help solve the problems that AI presents, but a bad privacy law will only make things worse. A bad privacy law will mean that the problem doesn't get fixed. It will be bad for the legislature because it failed to fix the problem. It will be bad for your constituents, because they won't be properly protected. And it will be bad for business, because exposed consumers are afraid to give those businesses the trust they need to thrive. That's why privacy matters, and it's why a privacy bill with substantive protections and meaningful enforcement is essential.

[19] *Marbury v. Madison*, 5 U.S. (1 Cranch) 137, 163 (1803) ("The very essence of civil liberty certainly consists in the right of every individual to claim the protection of the laws, whenever he receives an injury.").

Thank you for considering my thoughts on these questions. I remain ready to help with any further assistance I might provide.