June 29, 2026

Massachusetts House–Senate Committee of Conference
on the Massachusetts Consumer Data Privacy Act (H.5479 / S.2619)

The Honorable Karen Spilka, Senate President
The Honorable Ronald Mariano, Speaker of the House
The Honorable Cynthia Stone Creem, Senate Majority Leader
The Honorable Barry R. Finegold, State Senator
The Honorable Patrick M. O'Connor, State Senator
The Honorable Michael J. Moran, House Majority Leader
The Honorable Tricia Farley-Bouvier, State Representative
The Honorable David T. Vieira, State Representative

Re: Letter Urging the Committee of Conference to Retain the Private Right of Action in the Massachusetts Consumer Data Privacy Act

Thank you for your important work to reconcile the House and Senate versions of the Massachusetts Consumer Data Privacy Act. We write in our individual capacities as scholars of privacy, technology, artificial intelligence, and civil liberties law.[1] Among us are those who now live and teach in Massachusetts (or who used to), and those who grew up and who studied in the Commonwealth. Our concern is straightforward. The House bill, H.5479, contains a vital private right of action; the Senate bill, S.2619, does not. That single difference will go a long way toward determining whether the final statute actually protects the people of the Commonwealth or merely offers the illusion of protection while leaving Bay Staters exposed. Simply put, a right to privacy that people cannot enforce is no right at all. A private right of action is an essential feature of any effective consumer privacy bill. We therefore respectfully urge the Committee to retain the private right of action that the House adopted unanimously and, wherever the two bills diverge, to choose the stronger protection.

We have researched and written about information privacy law since its maturation as a field, collectively publishing dozens of books and hundreds of articles over many, many years. Our research regularly analyzes the features that separate effective privacy laws from ineffective ones. Drawing on our combined decades of study, we believe three features make any data privacy law meaningful: (1**) substantive limits on data collection** through data minimization; (2) **bright-line prohibitions** on the most dangerous categories of data processing; and (3) most importantly, **a private right of action** that consumers themselves can use to enforce their rights. The first two features shape what companies may do with our personal information. The third, a private right of action, decides whether those protections will be meaningfully enforced at all. Our letter focuses

[1] The opinions of the signatories are those of the individual scholars in their personal capacities as experts rather than those of their universities and research centers. The institutional affiliations are thus provided for identification purposes only.

on this third feature and why it is essential, why the objections to it do not hold, and how the Committee can preserve and strengthen it in the final bill.

Companies collect as much of our personal information as they can because that data is profitable. If left unchecked, they will gobble up all of our data, and with it, all of our privacy. Data minimization and other substantive rules push back against that incentive to collect everything. They limit collection to what a product actually needs, instead of whatever a company can get away with in the fine print. But these rules only work if they can be enforced. While the Massachusetts Attorney General does truly excellent work, no single taxpayer-supported office can watch over every large firm that collects and sells data on Massachusetts residents. To hold the largest technology companies accountable, public enforcement must be paired with a private cause of action. A right that no one can enforce is an empty promise. Without meaningful accountability, the dangerous data practices that concern us most will simply continue unchecked.

Fortunately, Massachusetts is well-positioned to fix this problem. Following their well-worn playbook for spreading last-minute fear, uncertainty, and doubt, industry lobbyists will soon descend upon your offices and claim that a private right of action is too burdensome, arguing that it will bury small businesses in litigation and "stifle innovation." Neither claim withstands scrutiny. A private right of action is not an all-or-nothing proposition. It can be calibrated in any number of ways to balance protection for consumers against ample room for businesses to operate. The House bill has already struck that balance elegantly. H.5479 confines private suits to "large data holders," which are entities that, in the prior year, collected, processed, or sold the personal data of more than two million consumers or the sensitive data of more than 200,000.[2] The Commonwealth's small and mid-sized businesses fall well outside that threshold. The provision reaches only the largest collectors of personal information, and it does so through the familiar mechanism of Massachusetts's established consumer-protection statute, Chapter 93A. This is a measured step instead of a radical one.

Massachusetts is not the first state to face this choice. Some states—like Illinois, Washington, and California—have passed strong privacy rules with a private right of action that meaningfully protect their state residents while industry continues to thrive.[3] Vermont faced that same question this spring, and got it wrong after lobbyists spread misinformation and fear. Across two legislative sessions, Vermont lawmakers led by Representative Monique Priestley fought to enact a

[2]An Act establishing the Massachusetts consumer data privacy act, H.5479, 194th Gen. Court (2026), https://malegislature.gov/Bills/194/H5479 (defining a "large data holder" as a controller or processor that, in the most recent calendar year, collected, processed, or sold the personal data of more than two million consumers or the sensitive data of more than 200,000 consumers, and authorizing private suits against such entities under Chapter 93A).

[3]See, e.g., Biometric Information Privacy Act, 740 ILCS 14/20 (Ill.) (private right of action); California Confidentiality of Medical Information Act, Cal. Civ. Code § 56.35 (private right of action); California Consumer Privacy Act, Cal. Civ. Code § 1798.150 (private right of action for certain data breaches); My Health My Data Act, Wash. Rev. Code ch. 19.373 (enforced as a violation of the Washington Consumer Protection Act, Wash. Rev. Code § 19.86.090).

comprehensive privacy law with a private right of action. Each time, the technology industry and its allies claimed that private enforcement would flood the courts, burden small businesses, and make Vermont a regional outlier. Under that pressure, and facing the threat of a gubernatorial veto, the legislature stripped the private right of action from the bill. In June 2026, Vermont enacted a privacy law enforced by the Attorney General alone.[4] The bill that survived was so weakened—no private right of action and diluted data-minimization and sensitive-data rules—that privacy advocates called it an industry-approved law offering Vermonters the illusion of protection without any substance.[5] Its own author, Representative Priestley, voted against the final version, unwilling to put her name to a bill that surrendered the very protections she set out to create. The same campaign of misinformation and fear that hollowed out Vermont's bill is now underway here. This Committee must not repeat Vermont's mistake.

Two witnesses in Vermont's own hearings answered these arguments directly and are worth your careful attention. Melanie Ensign spent fifteen years doing public relations for large technology companies, and she laid out the playbook that industry runs every time a meaningful privacy bill gains support in a legislature. If they haven't reached you already, industry lobbyists are going to come to your offices and tell you that exploiting our data isn't harmful and that data collection is too complicated to regulate. These claims will be made despite the fact that other states (including the ones where their headquarters are) and many other countries in the world have privacy laws with private rights of action and stronger privacy rules than the ones you are considering here. The lobbyists will also tell you that "more study is needed" despite two decades of clear evidence that unrestricted data collection leaves us worse off and paying more. Meanwhile, our local businesses suffer and are put at a significant disadvantage without a strong privacy law because they can never compete with the likes of Big Tech for a competitive advantage. In short, they will ask you to sell out Massachusetts small businesses in favor of Big Tech for no benefit to the Commonwealth.

As two of us wrote in an op-ed for WBUR, "[B]ig tech companies have spent a lot of time and money trying to convince the American public that we don't deserve strong privacy rules because they would hurt small businesses. Don't fall for it. Most of the noise coming from 'small businesses' is really big tech in disguise. This includes downplaying their role in scorched-earth lobbying against any strong privacy rule by bankrolling and leveraging 'small business collectives'

[4]Vermont Data Privacy and Online Surveillance Act, S.71 (Vt. 2026) (enacted June 16, 2026) (enforcement by the Attorney General; no private right of action); see also H.121 (Vt. 2024) (vetoed by Governor Scott over its private right of action).

[5]S.71 as enacted removed both the private right of action and the strong data-minimization requirements of earlier drafts, prompting privacy advocates to condemn it. See Press Release, Consumer Reports, Statement on Passage of Vermont's Comprehensive Privacy Bill (May 29, 2026); Vermont Legislature Passes Connecticut-Like Consumer Privacy Law, Privacy Daily (May 29, 2026) (quoting EPIC Deputy Director Caitriona Fitzgerald that the law gives "the illusion of privacy without any meaningful protection," and reporting that Representative Monique Priestley, the bill's author, voted against the final version).

to give the appearance of some kind of grassroots movement. Fake grass-roots movements are what are known in the trade as astroturfing, and they are a trick."[6]

These are the same claims this Committee is no doubt hearing now. As Ms. Ensign testified in Vermont, the industry is not worried about the cost of compliance. These are the most powerful and profitable companies ever to exist. They are heavily regulated in many other ways and regularly subject to private rights of action in other states, where they are doing just fine. Rather, Big Tech is worried about accountability interfering with their profits.[7]

Daniel Solove, who joins us on this letter, testified in that same Vermont debate on why enforcement by a government agency alone is not enough. Public enforcers are stretched thin, subject to political pressure, struggle to act quickly, and are frequently unable to put money back in the hands of the people who were harmed.[8] A private right of action does not replace public enforcement. Instead, it supplements it by filling the gaps that public enforcement cannot address. The Senate bill relies on the Attorney General alone. That model will fall short, while the House bill adds the private right of action that we regard as essential. Preserving a private right of action is what separates a privacy law that works from the toothless version that Vermont just passed.

Industry's other claim, that accountability slows innovation, also does not hold up. Reasonable substantive limits on data practices set the kind of sensible rules of the road on which fair and profitable competition can flourish, because good privacy practices build consumer trust, and consumer trust is good for business. A private right of action pushes companies to earn that trust rather than exploit it. Massachusetts is consistently ranked among the most innovative states in the country, second only to the District of Columbia in a widely cited 2026 ranking.[9] Fellow innovation leaders such as California and Washington pair that success with some of the nation's strongest consumer privacy laws and private rights of action, while many of the least innovative

---

[6] Woodrow Hartzog and Neil Richards, *Big tech is hungry for consumer data. Mass. needs privacy legislation now*, WBUR COGNOSCENTI, https://www.wbur.org/cognoscenti/2026/03/04/big-tech-data-ai-consumer-privacy-law-woodrow-hartzog-neil-richards ("[Research shows that] when consumers buy through targeted ads, they risk spending more and getting a worse product or product experience than if they had purchased through search results. There's also strong research tending to show that targeted advertising only brings in marginally higher revenues for companies. So who benefits? Big tech platforms make huge profits from sending us tailored ads for banned or scam items. In 2024, for instance, Facebook's internal projections predicted the company would make 10% of its annual revenue from these types of fraudulent ads. Besides, any marginal gains small businesses achieve using behavioral ads stand to be wiped out by the massive advantage that big tech companies gain in order to target (and thus siphon off) those same consumers elsewhere online. Small businesses will never have more data (or a greater ability to target consumers) than large tech companies, and if data is what determines the fight for our attention and money, then Silicon Valley will win every time. In other words, when it comes to behavioral advertising, Silicon Valley gets the meal and gives small businesses the table scraps.").

[7] Melanie Ensign, Written Testimony in Support of S.71, Vermont Data Privacy and Online Surveillance Act (Apr. 29, 2026).

[8] Daniel J. Solove, Enforcing Privacy Law: Why Private Litigation Is Essential, Testimony for the Vermont Data Privacy Hearing (Feb. 4, 2026), https://ssrn.com/abstract=6083968.

[9] Most & Least Innovative States, WalletHub (2026), https://wallethub.com/edu/most-innovative-states/31890 (ranking Massachusetts second among all jurisdictions, behind only the District of Columbia).

states have weak privacy protections or none at all.[10] Strong privacy protections with a private right of action and a thriving innovation economy can plainly coexist.

A private right of action also conserves public resources. An Attorney General's office can realistically pursue only a fraction of potential violations, and it must choose its cases carefully. Without private enforcement, accountability for even the largest data holders would depend entirely on whether the Attorney General, with finite staff and budget, has the capacity to bring a given case. Big Tech has nearly limitless resources to defend its unprecedented profits in court, and it can and does swamp state enforcers by driving up the costs of litigation, by contesting every point, and by "flooding the zone." A private right of action levels the playing field, letting consumers enforce their own rights while the Attorney General focuses resources where they are needed most. Such private enforcement also reinforces the accountability on which trust between Massachusetts businesses and their customers depends.

Both bills correctly ground their protections in substantive data minimization rather than in "notice and choice," which substitutes unreadable disclosures and a click of "I agree" for real limits on what companies collect. The overwhelming consensus in privacy law scholarship shows what every consumer knows intuitively: that notice and choice has been a failure. Transparency is necessary, but reforms built on consumer consent alone tend to entrench the very practices they purport to regulate.[11]

The reasons notice and choice fails are not abstract. The "control" companies promise is largely an illusion. People can only choose among the options a designer elects to present, and firms have every incentive to engineer interfaces that nudge us toward pushing the big blue buttons that say "accept all." The model also does not scale. A single mobile app can request hundreds of permissions, and the average app requests several.[12] Multiplied across the dozens of services on a typical phone, the task of reading every policy and adjusting every setting is a burden no person can actually carry. Our attention and willpower are finite, and these systems are designed to deplete, degrade, and overwhelm them.[13] Lawmakers who place individual consent and control at

---

[10] See generally, Caitriona Fitzgerald et al., The State of Privacy: How "privacy" laws fail to protect privacy and what they can do better, EPIC (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/. Although Washington has not enacted a comprehensive consumer privacy statute, its My Health My Data Act provides strong protections for a broad category of health-related data, making it one of the most protective regimes in the country. By contrast, several of the least innovative states in the WalletHub ranking, supra note 9—including Mississippi, West Virginia, and North Dakota—have not enacted a comprehensive consumer privacy law, and Iowa's law is widely regarded as among the weakest in the nation.

[11] See, e.g., Neil Richards & Woodrow Hartzog, The Pathologies of Digital Consent, 96 Wash. U. L. Rev. 1461 (2019); Daniel J. Solove, Murky Consent: An Approach to the Fictions of Consent in Privacy Law, 104 B.U. L. Rev. 593 (2024); Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880 (2013); Ignacio Cofone, The Privacy Fallacy: Harm and Power in the Information Economy (2023).

[12] Kenneth Olmstead & Michelle Atkinson, Apps Permissions in the Google Play Store, Pew Research Center (Nov. 10, 2015), http://www.pewinternet.org/2015/11/10/apps-permissions-in-the-google-play-store/.

[13] Aileen Nielsen, *Tech Has An Attention Problem*, UC Berkeley Center for Long-Term Cybersecurity (2021), at 6.

the center of a privacy regime risk overlooking how unevenly information and power are distributed. The wiser course is to protect people regardless of which boxes they happen to click. That is why the Committee should preserve the robust data-minimization limits both bills share, ensuring companies collect only what a requested product or service actually requires.

Finally, we applaud the bright-line prohibitions on the sale of sensitive data and trust that the Committee will preserve them. Some practices are so dangerous and offer such marginal benefits to ordinary consumers that they should be off-limits altogether. Precise location data is the clearest example. It threatens not only privacy but also physical safety, and it can expose a person's health, beliefs, and daily movements. The Federal Trade Commission has had to act repeatedly against a data broker that profiled consumers through their location[14] and against another that sold data trails tracking people to medical clinics, places of worship, and domestic-violence shelters.[15] Both bills rightly ban the sale of precise geolocation data and extend that protection to anyone present in the Commonwealth, not merely its residents. That safeguard matters acutely today, when people who travel to Massachusetts to seek or provide reproductive and gender-affirming care face rising threats against the constitutional rights of the people of Massachusetts. We urge the Committee to keep this bright-line rule for location data and, consistent with the Senate bill, to extend it into a full ban on the sale of all sensitive data.

In sum, we respectfully urge the Committee of Conference to take three steps.

- First, and most importantly, the Committee should retain the private right of action in H.5479 and reject any effort to weaken it, including the reintroduction of a right to cure, which the House eliminated and which would blunt enforcement even against egregious violations.

- Second, the Committee should also make clear that a violation of the Act constitutes an injury under Chapter 93A. Without that clarification, existing 93A case law may require private plaintiffs to prove a separate, concrete harm to recover for a violation of their rights. The hidden nature of modern data flows often makes this kind of proof practically impossible, and without this clarification the private right of action could be rendered largely ineffective.

- Finally, the Committee should preserve the substantive data minimization and bright-line prohibitions in the bills, adopting the Senate's broader prohibition on the sale of sensitive

[14] Fed. Trade Comm'n, FTC Order Will Ban InMarket from Selling Precise Consumer Location Data (Jan. 18, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-inmarket-selling-precise-consumer-location-data; Complaint at 3, In re InMarket Media, LLC, No. 202-3088 (FTC 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Complaint-InMarketMediaLLC.pdf.

[15] Fed. Trade Comm'n, FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data (Jan. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.

data and retaining the bright-line ban on the sale of precise location data, covering residents and visitors alike.

Of these, preserving the private right of action matters most. Without it, the law's other protections may never be enforced.

Massachusetts has the opportunity to enact the most protective consumer privacy law in the country, one built on substantive obligations rather than empty procedure, on bright-line limits for the most dangerous practices, and on enforcement that consumers themselves can invoke. Such a law would be good for the Commonwealth, good for its citizens, and (though the lobbyists will tell you otherwise) good for business because it will safeguard the trust our digital economy needs to thrive. The House took a unanimous step in that direction. We urge the Committee to bring that effort to completion and give the people of the Commonwealth the privacy law they can be proud of, the privacy law that gives them enforceable rights, and the privacy law that they deserve.

Sincerely,

Woodrow Hartzog
Andrew R. Randall Professor of Law, Boston University School of Law
Fellow, Cordell Institute for Policy in Medicine & Law, Washington University in St. Louis

Neil Richards
Koch Distinguished Professor in Law, Washington University in St. Louis School of Law
Co-Director, Cordell Institute

Daniel J. Solove
Eugene L. and Barbara A. Bernard Professor of Intellectual Property and Technology Law, George Washington University Law School

Anita L. Allen
Henry R. Silverman Professor of Law and Professor of Philosophy, Emeritus, University of Pennsylvania Carey Law School

Elettra Bietti
Assistant Professor of Law and Computer Science, Northeastern University School of Law

Ryan Calo
Virginia and Prentice Bloedel Professor, University of Washington School of Law

Bernard Chao
Professor of Law and Maxine Kurtz Research Scholar, University of Denver Sturm College of Law

Ignacio Cofone
Professor of Law and Regulation of AI, University of Oxford

Thomas Kadri
Professor of Law, University of Miami School of Law

Paul Ohm
Professor of Law, Georgetown University Law Center

Ngozi Okidegbe
Professor of Law and Assistant Professor of Computing & Data Sciences, Boston University

Lauren Scholz
McConnaughhay and Rissman Professor of Law, Florida State University College of Law

Chinmayi Sharma
Associate Professor of Law, Fordham University School of Law

Jessica Silbey
Professor of Law and Honorable Frank R. Kenison Distinguished Scholar in Law, Boston University School of Law

Alicia Solow-Niederman
Associate Professor of Law, George Washington University Law School

Olivier Sylvain
Professor of Law, Fordham University School of Law

Jeffrey L. Vagle
Associate Professor of Law, Georgia State University College of Law

Ari Ezra Waldman
Professor of Law and Professor of Sociology, University of California, Irvine School of Law

Enforcing Privacy Law: Why Private Litigation Is Essential

Testimony for the Vermont Data Privacy Hearing
February 4, 2026

Professor Daniel J. Solove

Thank you for inviting me to testify about the effective enforcement of privacy laws. My name is Daniel J. Solove, and I'm the Bernard Professor of Intellectual Property and Technology Law at the George Washington University Law School. I am Faculty Co-Director, GW Center for Law & Technology and Faculty Director, Privacy & Technology Law Program.

My remarks will summarize a recent paper I wrote called ***Enforcing Privacy Law: Why Private Litigation Is Essential***. The paper is available to download for free at https://ssrn.com/abstract=6083968. The paper provides citations and support for the statements in my testimony, and it elaborates on many of the arguments made below.

Enforcement is an essential dimension for effective privacy and data protection laws—and it is probably the most important one. No matter how many privacy laws are enacted and how strong the laws are, if enforcement falls short, the laws will fail to achieve their goals.

Unfortunately, the enforcement of privacy laws is often weak and inadequate, a plague that renders them infirm. Privacy enforcement has long been condemned as weak and ineffective. Countless studies show that compliance with privacy laws is poor, with many companies not complying at all. For companies that comply, the percentage of the budget devoted to privacy is paltry.

Government enforcers lack the resources, size, budget, and speed to keep up with their enforcement duties. They face political pressures that greatly constrain them from exercising the full extent of their powers.

New privacy laws often dump enforcement into the hands of existing enforcers without any additional budget or personnel. Enforcement becomes an unfunded mandate for agencies already overwhelmed with work and strapped for resources. These problems, along with weak penalties and structural impediments compel enforcers to adopt strategies and make tradeoffs that undermine effective enforcement.

I will make four primary arguments.

1. First, the effectiveness of privacy laws depends upon enforcement, and poor enforcement can neuter even a strong law. The enforcement of privacy laws is currently quite weak.

2. Second, government enforcement has many substantial shortcomings that undermine its effectiveness. Government enforcement requires far more resources, insulation from political interference, consistency, and potency. Even with considerable improvement, there ultimately will be a ceiling. In most cases, government enforcement will never be nearly enough.

3. Third, enforcement is about incentives. Far too often, the incentives are poorly aligned for organizations to follow the law. Government enforcement is rarely sufficiently dissuasive. The risk equation comes out heavily in favor of non-compliance or poor compliance because penalties are not severe or frequent enough to outweigh the benefits of noncompliance.

4. Fourth, enforcement from multiple enforcers and enforcement mechanisms works best, and private litigation is an essential part of the enforcement equation, adding dimensions to enforcement that

government enforcement lacks.

THE SHORTCOMINGS OF GOVERNMENT ENFORCEMENT

Government enforcement has many shortcomings that limit its effectiveness.

Political Constraints

Government enforcement is constrained by political limitations. There are strong political realities that restrict how aggressively government enforcers can enforce—and often, these realities result in their pulling their punches or leaving many of their powers untapped.

Like nearly all U.S. government agencies, the FTC is subject to significant political pressure from both the legislative and executive branches. Congress must confirm FTC commissioners, and it can curtail the FTC's powers dramatically. This happened with KidVid in the 1970s. Congress sternly punished the FTC for its attempt at a rulemaking attempt to limit advertising to children. Congress cut funding and took away the most efficient way for the FTC to promulgate rules. As a result, the FTC's enforcement actions have been too conservative. The FTC has left a large amount of its power unused, likely due to the necessity of strategically navigating a political landscape riddled with landmines.

Lack of Resources

Most government enforcers are woefully under-resourced in both funding and personnel. Data protection agencies are generally poorly funded and staffed.

In the U.S., state attorneys general have limited time and staff to enforce. U.S. federal enforcement agencies also suffer from a similar lack of resources. For example, the FTC enforces about eighty statutes, most of which aren't related to privacy. The FTC's budget in 2025 was $425.7 million. Professor William Kovacic, former chair and general counsel of the FTC stated that an adequate budget for the FTC should be more than $1 billion. In 2020, the FTC had only 61 staff devoted to privacy protection. Compare this to the EU, where in 2023, Ireland's Data Protection Commissioner had 150 employees and Germany's Data Protection Agency had 745.

But even these numbers are far from sufficient. Most EU data protection authorities have begged for larger budgets and more personnel, but their pleas haven't been answered. EU regulators have stated they're overwhelmed by the workload. Most have said their funding is inadequate and they are understaffed.

When flooded with complaints, enforcers are spread thin and unable to give most cases the time and attention they deserve. Companies know that enforcement agencies are in a position of weakness and can bargain harder for a gentler settlement. They can call an agency's bluff knowing the agency will be reluctant to litigate.

Weak Penalties

Government enforcement can be ineffective when penalties are too weak. Many fines are low. Government enforcers often settle for fines that are far lower than the maximum fines allowable under the law. Many enforcement penalties are merely warnings to sin no more or orders to start following the law.

Failure to Compensate Harmed Individuals

Many privacy laws lack a means of compensating harmed individuals. A consumer gets harmed, but the money goes to the state coffers.

Slow Resolution of Cases

The process of investigating and resolving cases is often slow. In many circumstances, cases can take 2 years to more than 5 years to resolve. Technology moves at the speed of light, but enforcers must lumber carefully at the speed of a tortoise. For example, by the time enforcers resolve issues with an AI model, companies might be using models several generations newer.

Insufficient Quantity of Enforcement

Due to insufficient resources, enforcers must often enforce sporadically. For the decade between 2009 and 2019, the FTC brought only 101 internet privacy enforcement actions, an average of only ten per year.

The FTC and other enforcers find it much easier and cost-effective to settle cases or issue warnings than to risk litigation, which will drain massive resources. This incentivizes enforcers to choose clear egregious violations and to work out a resolution that the violators find acceptable.

Generally, there just aren't enough resources to enforce most violations, so a few unlucky violators must be singled out and made examples of to try to achieve general deterrence.

The Difficulties of Qualitative Enforcement

Government enforcers often enforce simple clear-cut violations rather than ones that involve more qualitative judgments. Many laws are enforced only when duties are completely ignored or done in a woefully inadequate manner. Companies can comply in a generally poor way and get away with it. The incentives to enforcement agencies are stacked against enforcing more qualitatively.

Inconsistent Enforcement

Enforcement is often inconsistent. Enforcement by state attorneys general varies considerably; some state attorneys general are aggressive whereas others have not brought any enforcement actions. Enforcers just don't have the time or resources to enforce consistently.

Failure to Incentivize Complaints

Unfortunately, most laws create poor incentives for people to file complaints with regulators. People receive no benefit or redress for their complaint, so filing a complaint is akin to performing an act of charity. Filing a complaint thus is a thankless chore.

Because many people who are aware of a violation have little incentive to file a complaint, complaint statistics are skewed. If there is no incentive for individuals to file complaints, many people will not do so.

THE IMPORTANCE OF INCENTIVES

Enforcement ultimately boils down to incentives. If the risk equation is not dissuasive enough, then the law is not sufficient. The incentive must account for the entire risk equation, which is the severity of the penalty and the likelihood of getting caught. To be effective, penalties must be dissuasive, but they often aren't.

The most clear-eyed approach to evaluating enforcement is to analyze it from the perspective of an amoral actor making a risk calculation. Enforcement must change the calculation. Violations must make violators significantly worse off than if they had never committed the violation. Why not take a gamble when there's a lot to gain, nothing to lose except the winnings, and a low probability of giving up the winnings?

Companies also know the maxim: *Better to ask for forgiveness than for permission.* Companies know the likelihood of being enforced against is low. They know that if they're caught, they can plead for mercy and get off with a light penalty. Companies know they can get away with many infractions because there are other companies with worse violations. Unfortunately, the law makes it economically advantageous to violate the law.

SHORTCOMINGS CAN BE IMPROVED BUT NOT OVERCOME

Government enforcement can certainly be improved, but several debilitating shortcomings can't be entirely eliminated. Enforcement will likely never be frequent enough quantitatively or bold enough qualitatively. Even with a dramatic increase of many times their current budget and personnel, government enforcement agencies will likely always lack sufficient resources. The political realities will also likely not disappear. Ultimately, although government enforcement can improve significantly, these realities, like gravity, will restrain it from rising to the level where it will be truly effective.

THE ESSENTIAL ROLE OF PRIVATE LITIGATION

Another way to enforce against privacy law violations is through private litigation. Private rights of action have become one of the most debated enforcement mechanisms in privacy laws—and one of the most inconsistently included.

The GDPR and many comprehensive privacy laws around the world have private rights of action. In the U.S., the laws are mixed. Many federal privacy laws include private rights of action, such as:

- the Telephone Consumer Protection Act (TCPA)
- the Electronic Communications Privacy Act (ECPA)
- the Video Privacy Protection Act (VPPA)
- the Driver's Privacy Protection Act (DPPA)
- the Privacy Act, the Fair Credit Reporting Act (FCRA)
- the Cable Communications Policy Act (CCPA)

But other federal privacy laws vest enforcement solely with government entities, such as:

- the Children's Online Privacy Protection Act (COPPA)
- the Family Educational Rights and Privacy Act (FERPA)
- the Health Insurance Portability and Accountability Act (HIPAA)
- the FTC Act, and the Gramm-Leach-Bliley Act (GLBA)

State privacy laws are also mixed. Some subject-specific state privacy laws have private rights of action,

the most notable example being the Illinois Biometric Privacy Act (BIPA). There are also private rights of action in state consumer protection laws, such as the unfair and deceptive acts and practices (UDAP) laws of many states.

But nearly all state general consumer privacy laws passed since 2018 lack a private right of action. The main exception is the California Consumer Privacy Act which has a private right of action that is limited only to data security breaches. The lack of a private right of action in state consumer privacy laws is a fatal flaw, in my view. These laws aren't effective without one.

THE VIRTUES OF PRIVATE LITIGATION

Private litigation avoids many of the problems that beset government agencies. Judges and juries are generally more insulated from industry pressure than the personnel at government enforcement agencies.

In many contexts, private litigation has succeeded in addressing societal problems that government policymakers have failed to tackle because of lobbying, corruption, and other political impediments.

Private rights of action can escape from the vagaries of politics. When a different president or governor or state attorney general comes into power and shifts enforcement priorities, private rights of action can maintain enforcement consistency.

Private litigation can supplement government enforcement, helping to overcome problems with limited funding and staff. Success in litigation is rewarded by a payoff. In contrast, the budgets for government enforcers rarely grow with success.

Private rights of action have sometimes been understood as a way to deputize private parties into serving as "private attorneys general." The great thing about these private attorneys general is that they don't cost the state a salary or benefits or office expenses. As Stephen Burbank contends: "Allowing and encouraging private litigation can bring vastly more resources to bear on enforcement, potentially mobilizing private litigants and plaintiffs' attorneys in numbers that dwarf agency capacity."

Government enforcement of most privacy laws isn't sufficient because government agencies lack the resources to pursue most violators.

Government enforcers shouldn't have the exclusive ability to determine what cases are most important. Otherwise, they will ignore victims when cases are small or lacking in media attention on a violation.

The threat of private litigation has significant deterrent and incentive effects. Damages in class action lawsuits can add up to a large enough amount to gain the attention of upper management and corporate boardrooms.

Unlike much government enforcement, private litigation can provide plaintiffs with compensation for harm. Private enforcement through collective litigation makes it economically feasible to pursue enforcement against violations that cause many people a small amount of harm.

Private litigation enables individuals to become involved in the enforcement process. According to Professor Alexandra Lahav, litigation is essential to democracy and individual participation. Litigation "enables people to promote the rule of law and affirms our citizen-centered political system."

Litigation can also expose important information about privacy practices and compliance. Civil discovery in litigation is a powerful information-gathering tool; it functions to provide transparency.

It is immensely empowering for individuals who are victims of privacy violations to have a mechanism to stand up for themselves. Private rights of action allow victims to punch back, demand accountability, and make a powerful statement that their injuries matter and that they shouldn't be ignored or exploited in a company's quest for power and profit. Private rights of action allow victims to vindicate their rights when government enforcers forsake them.

ADDRESSING THE PROBLEMS WITH PRIVATE LITIGATION

Critics of private litigation argue that it serves mainly to enrich lawyers and generate costs to organizations without offering much financial benefits to victims.

Abusive Frivolous Litigation

The portrait of out-of-control litigation with immensely high damages and vexatious litigants is overblown and not supported by the actual evidence. Ultimately, given the tremendous underenforcement of privacy laws, it is far from clear that more private rights of action will shift the needle to the side of overenforcement.

Excessive Liability

A related critique of private litigation is that it can yield excessive damages for small harms.

Instead of being excessive, high damages might be driving a more appropriate level of compliance. It is far from clear that the damages and costs from mass litigation outweigh the total harm that violations create. In the event damages are excessive, courts also have tools such as remittitur where they can lower damage awards.

Loss of Innovation

The loss of innovation argument is often trotted out against nearly any form of regulation or accountability.

Companies already have powerful incentives to innovate—enormous sources of venture capital and investment, corporate limited liability, and the potential for gigantic profits if technologies are successful.

Where incentives are lacking is in being responsible and focusing on internalizing harm to individuals and society. For too often, innovation is worshipped blindly and for its own sake, even if what is being innovated is dangerous or harmful.

No company or industry wants to internalize cost. Externalizing costs is far more lucrative. Forcing the internalization of cost leads to safer and more responsible behavior and has not spelled the end of innovation.

THE CASE FOR MULTIPLE MECHANISMS OF ENFORCEMENT

As a general matter, given the challenges of enforcement, it is far better to have multiple enforcers and tools. Private rights of action and government enforcement each achieve different enforcement goals and have a different mix of strengths and weaknesses. They complement each other well. In most circumstances, neither government enforcement nor private litigation alone are sufficient to enforce most privacy laws.

State privacy laws with private rights of action allow for state courts to serve as alternative enforcement

zones that escape the barrier of standing, which mainly applies to federal cases. State courts can free themselves from the U.S. Supreme Court's antipathy toward privacy harm. For example, Illinois courts have interpreted the Illinois Biometric Information Privacy Act (BIPA) with a more robust conception of harm.

Companies are immensely powerful and can readily neutralize or weaken enforcement efforts, so enforcement often fares better when it is more diverse and multifarious.

CONCLUSION

Enforcement is essential to the effectiveness of privacy laws, but unfortunately, it is often woefully inadequate. There is a big difference between the text of privacy laws and the way they work in practice. Laws are hollow without rigorous enforcement.

Because the vast majority of enforcement authorities are under-resourced, overstretched, and politically-constrained, they are unable to enforce frequently and consistently enough; and they must adopt strategies that weaken their effectiveness and leave their full powers unused.

The best most resilient enforcement involves multiple enforcers using different enforcement tools. Private litigation is an essential dimension of enforcement, as it complements government enforcement by filling in where it is weak.

Enforcement should be strong, consistent and not arbitrary, rewarding of reasonable efforts and good faith, practical and strategic, qualitative, and sufficiently frequent so as not to appear as a remote risk. To be effective, privacy laws must have meaningful enforcement. Otherwise, they are empty vessels.

Written Testimony in Support of S.71

Vermont Data Privacy and Online Surveillance Act

Submitted by Melanie Ensign, Founder & CEO, Discernible

April 29, 2026

Introduction

My name is Melanie Ensign. I'm the founder of Discernible, a cybersecurity and privacy communications advisory, and a small business owner. I hold a master's degree in corporate public relations and spent fifteen years working in PR for some of the largest technology companies in the world. I am submitting this written testimony in support of S.71, the Vermont Data Privacy and Online Surveillance Act.

I am not a lawyer or a political expert, but I know exactly how the companies lobbying against this bill communicate with legislators, because I have been in the rooms where those strategies are developed. The purpose of this testimony is to name those tactics plainly, so that policymakers can recognize them for what they are.

The five tactics described below are documented, studied, and named in the academic literature on public relations and crisis communication. They are also, in my direct professional experience, actively in use today.

Tactic 1: Harm Denial

When a company claims there is no evidence its products cause harm, that claim frequently reflects a deliberate choice not to measure harm, or to structure operations in a way that makes harm difficult to trace. The absence of evidence is not evidence of absence.

This industry has deliberately chosen complexity over accountability and uses that complexity as a shield. That choice is a business strategy and S.71 directly addresses this by requiring data protection assessments for high-risk processing activities, including targeted advertising, processing of sensitive data, and profiling that affects decisions about housing, credit, employment, and health care. These assessments create a record of decision-making that is essential for future accountability and enforcement.

The relevant bill section is §2415g (Data Protection Assessments).

Tactic 2: Consumer Blame

Legislators will hear some version of the argument that consumers choose to share their data, that they agreed to terms of service, and that they have sufficient tools to protect themselves. This framing is deliberate and well-documented in public relations scholarship and literature as a strategy for shifting responsibility away from powerful institutions and onto individuals.

S.71 explicitly names and rejects this argument. The bill's definition of consent (§2415a(7)) excludes agreement obtained through dark patterns and acceptance of broad terms of service that bundle privacy language with unrelated content. This reflects a substantive judgment that meaningful consent requires genuine choice rather than a manufactured illusion of it.

When a child's school requires a platform account, consent is not voluntary. When an employer uses behavioral tracking software, opting out is not a realistic option. The consumer blame argument describes a world that does not exist for most people.

Tactic 3: Manufactured Complexity

Privacy and data infrastructure can be technically complex, but that complexity is a choice. Companies knowingly take on technical debt and accumulate data in pursuit of growth and monetization. So, the complexity isn't incidental — it's what happens when you prioritize data collection over responsible design, and then use the resulting mess as a reason you can't be held accountable.

S.71 is specific. The definition of sensitive data (§2415a(53)) covers Social Security numbers, financial account credentials, immigration status, pregnancy status, gender identity, sexual orientation, biometric data, precise geolocation, neural data, and keystrokes. These are categories of information that, when collected and sold without meaningful consent, expose people to demonstrable harm. The bill's prohibition on selling sensitive data (§2415e(a)(8)) is a clear line. Complexity is not a compelling argument against that line — on the contrary, it’s an argument for the kind of clear, enforceable standards this bill provides.

On the small business argument, legislators are also told that this bill would hurt small businesses. Big Tech and data brokers use small businesses as a human shield while simultaneously misleading them about how indispensable their platforms are. Data brokers in particular have no direct relationship with consumers at all — they collect, package, and sell personal information about people who have never heard of them and never agreed to anything. Small businesses are not partners in this data economy. They are, in large part, data collection points that generate value for the platforms and brokers, not for themselves.

This argument also does not hold up against legal precedent. A small medical clinic is not exempt from HIPAA because compliance is burdensome. Nor is a community bank

exempt from anti-fraud regulations because it is not a large institution. The risk to consumers isn't based on the size of the business handling sensitive information; the risk travels with the data whereve it goes.

Tactic 4: Delay by Design

Calls for more studies, working groups, pilot programs, and stakeholder input are sometimes legitimate. In the context of data privacy legislation, they more often function as strategies for postponement. This industry has had decades to self-regulate and their record on voluntary compliance is not good.

Moreover, S.71 has already made significant concessions to industry. Enforcement runs through the Attorney General rather than through a private right of action (§2415j). This means individual Vermonters who are harmed by violations can't sue and the entire enforcement burden falls on a unit of two attorneys and one investigator appropriated only $650,000. The industry has received substantial accommodations in this bill's current form. Further delay or weakening is beyond a negotiation — it's capitulation.

Tactic 5: Science Manipulation

This tactic has a longer and better-documented history than most people realize, and understanding that history is useful context for evaluating the research industry lobbyists will present to legislators.

Edward Bernays, described in his 1995 New York Times obituary as the 'father of public relations' and a nephew of Sigmund Freud, used his uncle's insights on human psychology to advise corporate clients on how to move public opinion. One of his best-documented campaigns was a 1929 effort staging women smoking publicly at the New York City Easter parade, framing cigarettes as 'torches of freedom' on behalf of the American Tobacco Company.

The tobacco industry later retained the PR firm Hill & Knowlton to run a coordinated campaign manufacturing doubt about the scientific link between smoking and cancer. Beginning in 1953, the industry created the Tobacco Industry Research Committee to challenge mounting evidence of harm, funded alternative research designed to produce the appearance of scientific controversy, and distributed materials to doctors, media, and policymakers insisting there was no cause for alarm — all while internal industry documents showed executives privately acknowledged the evidence against them.

The same pattern has appeared in the technology sector and data brokers. In 2021, internal Facebook documents leaked by whistleblower Frances Haugen revealed that the company had conducted its own research into Instagram's negative effects on teen mental health, was aware of possible solutions, and had not acted on that research publicly. Six months before the leak, CEO Mark Zuckerberg testified before Congress that 'the research is not conclusive' on the connection between social media and teen mental health.

When industry presents legislators with research about the economic value of data sharing or the impracticality of data minimization, the appropriate questions are: Who funded this research? What research is not being presented (and why)? What do the companies' own internal studies actually show?

Conclusion

S.71 establishes that Vermonters have the right to know what data is being collected about them, to correct it, delete it, and opt out of having it sold or used to target them. It prohibits the sale of the most sensitive categories of personal information — the kind that can get someone fired, deported, denied housing, or physically harmed. Far from radical propositions, they are baseline conditions for any business, regardless of size or industry, to operate honestly, ethically, and with respect to human dignity.

I have spent my career helping security and privacy professionals communicate more clearly with the public. That work is necessary because the default in this industry is obfuscation and deflection. The protections consumers deserve do not happen voluntarily. They have to be required.

This bill is not perfect. No bill is. But the industry lobbying against it is not worried about compliance costs. They are worried about accountability. This bill should pass without further weakening.

Key Sources Referenced

S.71 Draft (April 24, 2026): Vermont Legislature

Edward Bernays, Wikipedia: en.wikipedia.org/wiki/Edward_Bernays

"A Frank Statement" and Hill & Knowlton tobacco campaign, Wikipedia: en.wikipedia.org/wiki/A_Frank_Statement

Inventing Conflicts of Interest: A History of Tobacco Industry Tactics, PMC/NCBI: pmc.ncbi.nlm.nih.gov/articles/PMC3490543

Facebook's Internal Documents on Teen Mental Health, The Conversation: theconversation.com

Whistleblower Frances Haugen Senate Testimony, NPR: npr.org

HIPAA Overview, HHS: hhs.gov/hipaa