Vermont Senate Committee on Institutions
Testimony of Cody Venzke, Senior Policy Counsel, ACLU
On S.71, the Vermont Data Privacy and Online Surveillance Act

Chair Harrison and members of the Committee:

Thank you for holding this hearing and inviting me to offer testimony on S.71, the Vermont Data Privacy and Online Surveillance Act. I am Cody Venzke, a Senior Policy Counsel with the American Civil Liberties Union. I am testifying on behalf of the ACLU and the ACLU of Vermont. For more than 100 years, the ACLU and its 54 state affiliates have been among the nation's premier defenders of civil rights and civil liberties, including longstanding commitments to reproductive autonomy and privacy rights.

Data Abuses Harm Our Most Fundamental Rights

Although doubtlessly a "data privacy" bill, S.71 is an essential step forward to protect myriad rights underlying our constitutional system. S.71 is a step toward a modern bulwark to ensure that the Fourth Amendment retains meaning in the digital age, that Vermonters' rights to reproductive and gender-affirming are protected, and that undocumented people seeking refuge are not denied their right to seek asylum.

These harms are not hypothetical. Instead, we are increasingly seeing the ways that our data may be used to undermine our fundamental rights:

- **Attacking Healthcare, Reproductive Rights, and Gender-Affirming Care.** Last year, the Federal Trade Commission brought enforcement actions against a half dozen data brokers for not only selling location data, but marketing it as revealing visits to hospitals, oncology centers, and other medical centers.[1] Our data can similarly reveal access to abortion or gender-affirming care. For example, reporting by 404 Media detailed how one data set shows a phone beginning a day in mid-June at a residence in Alabama, crossing state lines, and visiting an abortion clinic for approximately two hours.[2] Similarly, data collected by period trackers, fitness apps, or even brick-and-mortar retailers may reveal or provide a means of predicting

[1] Fed. Trade Comm'n, *FTC Takes Action Against Mobilewalla for Collecting and Selling Sensitive Location Data*, Press Release (Dec. 3, 2024), here.
[2] Joseph Cox, *Inside the U.S. Government-Bought Tool That Can Track Phones at Abortion Clinics*, 404 Media (Oct. 23, 2024), here; Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, VICE (May 3, 2022), here (data broker SafeGraph marketing "Planned Parenthood" as a "brand" that can be tracked).

someone's pregnancy status.[3] Such data has been weaponized by anti-LGBTQ[4] or anti-abortion groups[5] to target specific individuals revealed in the data.

- **Tracking Undocumented People.** The federal government's deportation machine depends not only on invasive governmental technology, but private data brokers as well. For example, over the past four years, the data analytics company Palantir has received more than $1 billion from immigration enforcement agencies.[6] Venntel, a provider of location data, had seven contracts with ICE totaling at least $330,000 between 2018 and 2022.[7] ICE and other agencies have similarly utilized databases from LexisNexis and Equifax to conduct millions of searches,[8] including for information as seemingly benign as utility bills to identify and track undocumented people.[9] All this data is the foundation for President Trump's deportation agenda.

- **Undermining the Fourth Amendment.** In addition to the purchases by immigration agencies, other arms of the government have purchased our data from data brokers — all without a warrant or judicial oversight. For years now, federal agencies, including the Internal Revenue Service[10] and the Department of Defense,[11] have been buying their way around the Fourth Amendment by purchasing Americans' sensitive information from data

---

[3] Jiaxun Cao et al., *"I Deleted It After the Overturn of Roe v. Wade": Understanding Women's Privacy Concerns Toward Period-Tracking Apps in the Post Roe v. Wade Era*, Proceedings of the CHI Conference on Human Factors in Computing Systems (2024), here; Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary*, 50 Univ. Baltimore L. Rev. 1 (2020), here.

[4] *Senior US Catholic Resigns Over Grindr Allegations*, BBC (July 21, 2021), here (describing Pillar's acquisition of "commercially available" location data and app usage data showing visits to gay bars); Liam Stack, *Catholic Officials on Edge After Reports of Priests Using Grindr*, N.Y. Times (Aug. 20, 2021), here.

[5] Alfred Ng, *A Company Tracked Visits to 600 Planned Parenthood Locations for Anti-Abortion Ads, Senator Says*, Politico (Feb. 13, 2024), here (describing Veritas Society's use of data brokers to target individuals in Wisconsin, Arkansas, New Jersey, California and Colorado).

[6] Adam Satariano, *The Tech Arsenal That Could Power Trump's Immigration Crackdown*, N.Y. Times (Jan. 25. 2025), here.

[7] *Id.*; *accord* Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall St. J. (Feb. 7, 2020), here.

[8] Sam Biddle, *ICE Searched LexisNexis Database Over 1 Million Times in Just Seven Months*, The Intercept (June 9, 2022), here.

[9] Drew Harwell, *Equifax Will No Longer Sell Utility Data ICE Used to Track The Public*, Wash. Post (Dec. 8, 2021), here.

[10] Byron Tau, *IRS Used Cellphone Location Data to Try to Find Suspects*, Wall St. J. (June 19, 2020), here.

[11] Joseph Cox, *How the U.S. Military Busy Location Data from Ordinary Apps*, VICE (Nov. 16, 2020), here.

brokers. These companies often obtain this information through common applications, like The Weather Channel[12] or Tinder,[13] without users realizing it, and then the government uses it to track people's location without a warrant or probable cause — or even suspicion that anyone in the dataset had done anything wrong.

- **Empowering the DOGE Agenda.** Since President Trump's inauguration, the so-called Department of Governmental Efficiency has sought to stymie programs that provide crucial — sometimes life-saving — support to Americans. At the core of DOGE's strategy has been access to our data at the Internal Revenue Service, the Centers for Medicare and Medicaid Services, the Social Security Administration, and more. Ongoing litigation may ultimately end DOGE's access to federal data, but that may not be enough: just as DHS and other agencies have ready access to the data broker market, DOGE too may be able to satisfy its hunger with the privately held data that is just clicks away.

Use and abuse of our data is about more than wonky, technocratic debates over privacy policies and data practices — it is about real harms for real people.

S.71 Provides Key Guardrails Against Data Abuses

S.71 will provide real, meaningful protections against these incursions. Several features of this bill mean it will not be "business as usual" for Big Tech, data brokers, and those who profit off their surveillance:

- **Universal opt-out.** Nearly all state privacy bills purport to provide individuals with the ability to "opt-out" of three data uses: sale of data, targeted advertising, and profiling. However, as the Federal Trade Commission has emphasized, those opt-out rights are all too often "illusory."[14] In many cases, opt-out "rights" require navigating layers of settings, which can be divided among multiple tabs, with unclear and sometimes conflict interactions among the options.[15] This bill would not only prohibit such "dark patterns," but given users a new tool in their toolbox: universal opt-out mechanisms, which are browser extensions or other

[12] Suzanne Smalley, *Exploring the Surveillance Partnership Between the Government and Data Brokers*, The Record (Mar. 21, 2024), here.
[13] Natasha Singer & Aaron Krolik, *Grindr and OkCupid Spread Personal Details, Study Says*, N.Y. Times (Jan. 13, 2020), here.
[14] Federal Trade Commission Staff, A Look At What ISPs Know About You at 27 (2021), here.
[15] *Id.* at 28–29.

technologies that automatically exercise opt-out rights determined by the individual.

- **Robust data minimization**. Data minimization means limiting the collection and use of our data to what is needed to provide the services we request. If you permit a mapping application to access your geolocation to provide directions, it will be prohibited from using that data to secretly identify what health clinics you have visited. If you provide bodily statistics to a fitness tracker, it will not sell those to a data broker.

  This provision is so essential because although many data harms stem from data brokers, that data must come from somewhere — and in reality, it comes from the apps we use every day — apps for weather, dating, shopping, games, and even levels and flashlights.[16] Under this bill, Vermonters can be confident that the data they provide for important services is used only for those services.

- **Shoring up existing anti-discrimination laws.** Algorithms are increasingly used to help make decisions about us in areas that have long been protected by civil rights laws like housing, employment, credit, governmental benefits, healthcare, education, insurance, and the criminal legal system. Algorithmic systems can cause discriminatory outcomes, propelled by data reflecting existing biases and disparities, misuse by users, deployment within discriminatory or otherwise flawed structures, or a poor fit between what an algorithm measures and its intended purpose. For example, tenant-screening algorithms are prone to errors and incorrectly include criminal or eviction records tied to people with similar names.[17] Similarly, algorithmic resume scanners favor male candidates, are inaccessible to applicants with disabilities, and may discriminate against first-generation college graduates.[18]

---

[16] Federal Trade Commission Staff, A Look Behind the Screens at 27 (2024), here ("The three types of entities the [social media and streaming] Companies most often reported sharing Personal Information with were: service providers and vendors, developers, and law enforcement. ") Joseph Cox, *How the U.S. Military Busy Location Data from Ordinary Apps*, VICE (Nov. 16, 2020), here.
[17] Kaveh Waddell, *How Tenant Screening Reports Make It Hard for People to Bounce Back From Tough Times*, Consumer Reports (Mar. 11, 2021), here; Lauren Kirchner, *Can Algorithms Violate Fair Housing Laws?*, The Markup (Sept. 24, 2020), here.
[18] Charlotte Lytton, *AI Hiring Tools May Be Filtering Out The Best Job Applicants*, BBC (Feb. 16, 2024), here; Olga Akselrod & Cody Venzke, *How Artificial Intelligence Might Prevent You From Getting Hired,* ACLU (Aug. 23, 2024); Lydia X.Z. Brown et al., Center for Democracy & Tech., Algorithm-Driven Hiring Tools (2020), here; Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women*, Reuters (Oct. 10, 2018), here.

These fundamental protections are accompanied in S.71 by important data rights, protections for sensitive data, and guardrails for health data.

S.71 Would Finally Hold Big Tech Accountable

In many ways, S.71 builds off efforts in other states and the lessons learned there. S.71's universal opt-out rights closely follow mechanisms recognized in California, Colorado, Connecticut, Minnesota, Montana, and Maryland. Similarly, the data minimization provisions in the bill iterate on requirements passed in California and Maryland, and the anti-discrimination measures draw heavily from Maryland and Minnesota.

Crucially, however, S.71 reflects the hardest lesson learned about other states' efforts: they simply do not work. Many states have replicated Virginia's approach to privacy: lean heavily on consumers to do the work, provide few guardrails, and enforce sparingly. Virginia's model perpetuates the fiction that we "consent" to data practices buried in dense, impenetrable privacy policies. Those laws leave us to individually police Big Tech and data brokers, filing data rights requests one-by-one with the hundreds of companies that use — and abuse — our data. Meanwhile, tech companies can do what they like, as long as their practices are "disclosed" to us.

This is perhaps one of the few cases when sunlight is *not* the best disinfectant. Virginia-style laws have passed in (give or take) 17 states, and they have not reduced data abuses at all. The threats to healthcare, undocumented people, and our Fourth Amendment rights still abound. What we need are guardrails, not empty promises — and S.71's universal opt-out, data minimization, and anti-discrimination provisions provide those safeguards.

S.71 Is a Thoughtful Compromise

Despite its many, many strengths, S.71 is not the perfect bill from the perspective of ACLU or ACLU of Vermont. We would continue to refine the provisions regarding "heightened risk of harm" to avoid potential First Amendment implications or abuse by enforcers. Similarly, we would expand the private right of action and the scope of the bill's coverage. That said, the bill's sponsors have clearly engaged with a wide range of stakeholders across advocacy and business. They have carefully crafted a bill that would make Vermont a leader in addressing harms while still enabling innovation and the services we depend on to speak, learn, run businesses, and connect.

Thank you.