September 24, 2018

The Honorable John Thune
Chairman
Committee on Commerce, Science, & Transportation
512 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Bill Nelson
Ranking Member
Committee on Commerce, Science, & Transportation
512 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Thune and Ranking Member Nelson:

The Electronic Frontier Foundation (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. With over 38,000 dues-paying members and well over 1 million followers on social networks, we focus on promoting policies that benefit both creators and users of technology. Furthermore, we work to ensure that the rights and freedoms of individuals are retained and enhanced as their use of technology grows.

EFF submits this letter to the Senate Commerce Committee to detail the dangers to individual user privacy posed by industry suggestions that Congress should wipe the slate clean of state privacy laws through preemption. Many states have already created strong statutory and other protections of user privacy. If Congress enacts data privacy legislation that is weaker than the existing state data privacy laws, and simultaneously preempts the stronger state data privacy laws, the result will be a massive step backwards for user privacy. We urge the Committee to recognize the scope of what is being asked before acting on federal legislation, as the lives of technology users and their currently existing rights increasingly overlap with their Internet usage, and as data brokers grow increasingly sophisticated at mining and monetizing information about our off-line activity.

In essence, a federal law that sweeps broadly in its preemption could reduce or outright eliminate privacy protections that Congress has no intent to eliminate, such as laws that protect social security numbers,[1] prohibit deceptive trade practices,[2] and protect the confidentiality of library

[1] CONGRESSIONAL RESEARCH SERVICE, *The Social Security Number: Legal Developments Affecting Its Collection, Disclosure, and Confidentiality* (Feb. 4, 2014), available at https://digital.library.unt.edu/ark:/67531/metadc282348/m1/1/high_res_d/RL30318_2014Feb04.pdf.

[2] NATIONAL CONSUMER LAW CENTER, State by State Summaries of State UDAP Statutes (Jan. 10, 2009), available at https://www.nclc.org/images/pdf/udap/analysis-state-summaries.pdf (the overlap between state Unfair and Deceptive Acts and preemption of state privacy laws is when the deceptive or unfair conduct involves the collection, use, or disclosure of personal information. Congress has already witnessed this unforeseen consequence when it passed the Homeowners Protection Act to address homeowner challenges with private mortgage insurance and granting them rights to terminate insurance with disclosure obligations. The wide reaching preemptive language within the federal law was seen by the courts as a bar on states prosecuting deceptive conduct by mortgage service

records.[3] Also, every state which is represented by the Senate Commerce Committee has various common law privacy rights that courts have recognized,[4] and that some state legislatures have codified.[5]

To better understand the harmful consequences of the preemption being proposed by certain industry groups, it is valuable to take a closer look at three of the state privacy laws that would be preempted. California's recent Consumer Privacy Act protects all manner of personal information and applies to all manner of businesses. Vermont's recent Data Broker Act focuses on third-party data mining, where the business collecting the information has no direct relationship with the consumer. It is the first state law directed at the data broker industry since the Equifax breach that harmed 145 million Americans. Lastly, the decade-old Illinois Biometric Information Privacy Act requires businesses to get a person's opt-in consent before they gather and monetize their biometrics. The people of these and other states would suffer if Congress enacts a weak consumer privacy law that preempts these stronger consumer privacy laws.

## California's Consumer's Privacy Act

Earlier this year, California enacted a far-reaching consumer privacy statute called the Consumer Privacy Act (A.B. 375).[6] The following are among its key protections:

---

companies, effectively eliminating state protections against deceptive conduct for that industry). *See* Fellows v. CitiMortgage, Inc., 710 F. Supp. 2d 385.

[3] AMERICAN LIBRARY ASSOCIATION, *State Privacy Laws Regarding Library Records*, available at http://www.ala.org/advocacy/privacy/statelaws (Nearly every state has laws assigning confidential status to library records with the exception of Hawaii and Kentucky. However in those two states the state AG has issued opinions outlining protection around library user privacy).

[4] The following states represented by the committee have judicially recognized common law privacy rights: Alaska (Greywolf v. Carroll, 151 P.3d 1234, 1244–45 (Alaska 2007)), Colorado (Doe v. High-Tech Inst., Inc., 972 P.2d 1060, 1066–67 (Colo. App. 1998)), Connecticut (Carney v. Amendola, No. CV106003738, 2014 WL 2853836, at *17 (Conn. Super. Ct. May 14, 2014)), Florida (Allstate Ins. Co. v. Ginsberg, 863 So. 2d 156, 162 (Fla. 2003)), Hawaii (Mehau v. Reed, 869 P.2d 1320, 1330 (Haw. 1994)), Illinois (Lawlor v. N. Am. Corp. of Ill., 983 N.E.2d 414, 424–25 (Ill. 2012)), Indiana (Cullison v. Medley, 570 N.E.2d 27, 31 (Ind. 1991)), Kansas (Werner v. Kliewer, 710 P.2d 1250, 1255 (Kan. 1985)), Michigan (Tobin v. Mich. Civil Serv. Comm'n, 331 N.W.2d 184, 189 (Mich. 1982)), Minnesota (Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 233–35 (Minn. 1998)), Mississippi (Plaxico v. Michael, 735 So. 2d 1036, 1039 (Miss. 1999)), Missouri (Sofka v. Thal, 662 S.W.2d 502, 510–11 (Mo. 1983)), Montana (Rucinsky v. Hentchel, 881 P.2d 616, 618 (Mont. 1994)), Nevada (City of Las Vegas Downtown Redevelopment Agency v. Hecht, 940 P.2d 127 (Nev. 1997)), New Hampshire (Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1008 (N.H. 2003)), New Mexico (Moore v. Sun Publ'g Corp., 881 P.2d 735, 742–43 (N.M. Ct. App. 1994)), Oklahoma (Munley v. ISC Fin. House, Inc., 584 P.2d 1336, 1339–40 (Okla. 1978)), South Dakota (Kjerstad v. Ravellette Publ'ns, Inc., 517 N.W.2d 419, 424 (S.D. 1994)), Texas (Valenzuela v. Aquino, 853 S.W.2d 512, 513 (Tex. 1993)), Utah (Cox v. Hatch, 761 P.2d 556, 563–64 (Utah 1988)), Washington (Mark v. Seattle Times, 635 P.2d 1081, 1094 (Wash. 1981) (en banc)), and West Virginia (Crump v. Beckley Newspapers, Inc., 320 S.E.2d 70, 85 (W. Va. 1984)).

[5] The following states have codified the common law right to privacy: Massachusetts (MASS. ANN. LAWS ch. 214, § 1B (LexisNexis 2011)), Nebraska (NEB. REV. STAT. ANN. § 20-203), and Wisconsin (WIS. STAT. ANN. § 995.50(2)(a) (West 2007)).

[6] California Consumer Privacy Act of 2018, (signed into law Jun. 28, 2018), available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

- Consumers have a "right to know" what personal information a business has collected about them, and where (by category) that personal information came from or was sent. *See* Sections 100, 110, 115.

- Consumers have a right to delete information that a business collected from them, with exceptions, including for the First Amendment. *See* Section 105.

- Consumers have a right to opt-out of the sale of personal information about them. *See* Section 120.

- Consumers have a right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act, though with significant exceptions. *See* Section 125.

The Act defines "consumer" as any natural person who resides in California. *See* Section 140(g). In order to exempt small businesses, it defines a "business" as a for-profit entity with $25 million in revenue, with personal information from 50,000 consumers, or with half of its revenue from sale of personal information. *See* Section 140(c).

The California Attorney General will be responsible for enforcing the Act, and for promulgating regulations about it. *See* Sections 155, 185. The Act creates a limited private cause of action for consumers against businesses for data breaches, based on California's existing data breach notification law. *See* Section 150.

**Illinois' Biometric Information Privacy Act**

A decade ago, Illinois enacted our nation's strongest statutory protection of biometric privacy: the Illinois Biometric Information Privacy Act, 740 ILCS 14.[7] At its core, the Illinois law forbids private entities from acquiring or disclosing a person's biometric information, absent their informed, opt-in consent. *See* Section 15(b) & (d). This empowers people to autonomously decide for themselves whether it is in their best interests to share their biometric information with others.

The Illinois statute also limits the time that a private entity may store a person's biometric information, *see* Section 15(a); bars the sale of biometric information, *see* Section 15(c); and requires entities that hold biometric to securely store it, *see* Section 15(e).

The Illinois law empowers persons aggrieved by violations of the Act to bring a private cause of action against the offending parties. *See* Section 20.

[7] 740 ILCS 14 (Biometric Information Privacy Act), available at http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

## Vermont's Data Broker Act

Earlier this year, Vermont enacted its Data Broker Act (H. 764).[8] The following are its key protections of consumers from data brokers:

- Data brokers must annually register with the state. When they do so, they must disclose information of value to consumers, including: whether there is a way for consumers to opt-out of data collection, retention, or sale, and if so, how they may do so; whether the data broker has a process to credential its purchasers; and whether it has had any data breaches. *See* Section 2446.

- Data brokers must securely store the personal information they acquire. *See* Section 2447.

- Data brokers may not collect personal information by fraudulent means, or for the purpose of harassment or discrimination. *See* Section 2433.

- Credit reporting agencies must provide consumers a free "credit freeze" as a protection against data thieves who attempt to commit credit fraud against breach victims. Many creditors will not extend credit absent a report from a credit agency. If the consumer has previously obtained a "credit freeze," the credit agency will not issue the report, and the creditor in turn will not extend credit to the fraudster. Vermonters now can freeze their credit at no cost, and when they actually want credit, they can unfreeze their credit at no cost. *See* Section 2480b & Section 2480h.

Vermont's Attorney General is empowered to enforce these rules. Individual Vermont residents may bring a private cause of action to enforce the data security mandate and the ban on fraudulent acquisition.

## EFF Urges Caution Before Acting

This letter is by no means an exhaustive list of the potential privacy harms that could be done by preemption, but it is meant to convey the gravity of what is being asked of Congress. Many of the companies that are intentionally seeking to monetize information about everything we do online and elsewhere do not intend to ask for laws that actually restrain their business plans. The Committee should understand that the only reason many of these companies seek congressional intervention now, after years of opposing privacy legislation both federally and at the states, is because state legislatures and attorney generals have acted more aggressively to protect the privacy interest of their states' residents, in many cases over their objections. Indeed, 91 percent of Americans believe they have lost control over how their personal information is collected and

[8] 9 V.S.A. Ch. 62 as amended by the 2018 Acts 171 available at https://legislature.vermont.gov/assets/Documents/2018/Docs/ACTS/ACT171/ACT171%20As%20Enacted.pdf.

used[9] with many Americans choosing to avoid using the Internet for various activities due to privacy concerns.[10]

The latest series of national data privacy scandals (many of which have been investigated by this Committee and others) has forced the industry to recognize that state legislators want to protect the privacy of their constituents, and grant them legal rights, including a right to be made whole after an egregious breach of their personal information through a private right of action.

If Congress wishes to enact legislation that genuinely improves the data privacy of Americans, EFF urges Congress to include the following as part of the baseline:

- Opt-in consent to the collection, use, and disclosure of personal information by online services.
- A "right to know" what personal information companies have gathered about us, where they got it, and with whom they shared it.
- "Data portability," meaning the power of users to take their data, in a usable form, from a company and bring it elsewhere. This will ensure users can vote with their feet should they find a particular practice unacceptable and will promote competitive forces to address privacy concerns.
- A right to equal service, without change in price or quality, for users who exercise these rights.
- A private right of action for users to bring to court companies that violate these rights.

There is much that Congress might do to help protect data privacy. But weak federal legislation that preempts stronger state legislation would be far worse than doing nothing.

Sincerely,

Electronic Frontier Foundation

CC: Members of the Senate Commerce Committee

[9] PEW RESEARCH CENTER, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, available at http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns.
[10] Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NTIA (May 13, 2016), available at https://www.ntia.doc.gov/print/blog/2016/lack-trust-internet-privacy-andsecurity-may-deter-economic-and-other-online-activities.