FUTURE OF PRIVACY FORUM

1400 Eye Street NW, Suite 450 | Washington, DC 20005 | 202-642-9142 | fpf.org
published by IAPP, January 13, 2020

Federal privacy preemption and informed consideration of existing and future state laws

By Peter Swire and Polly Sanderson

There are signs that U.S. Congress is getting closer to a bipartisan approach to federal privacy legislation. In the Senate Committee on Commerce, Science, and Transportation, draft bills by Sens. Chairman Roger Wicker, R-Miss., and Ranking Member Maria Cantwell, D-Wash., contain important similarities on a wide range of issues. As Cameron Kerry of the Brookings Institution has explained, the two bills "adopt the same general framework: a set of individual rights combined with boundaries on how businesses collect, use, and share information, all of which would be enforced through the Federal Trade Commission."

The two bills differ, notably, on two topics. The first, and the topic of our proposal here, is the extent to which the federal law will "preempt" state data privacy and security laws — in what circumstances would the federal law mean that state laws no longer apply? The second concerns how the laws will be enforced. The two bills are similar in empowering enforcement by the FTC and state attorneys general, but the Cantwell bill would also enable individuals to bring private rights of action.

The two draft bills currently show large differences on preemption. Wicker's draft would replace state laws: "No State or political subdivision of a State may adopt, maintain, enforce, or continue in effect any law, regulation, rule, requirement, or standard related to the data privacy or security and associated activities of covered entities." By contrast, Cantwell's draft would generally retain current state protections that afford "a greater level of protection to individuals" covered by the law. Cantwell's bill also specifies eight categories of state laws that would continue in effect as currently written, even if they afford a greater level of protection to individuals. These laws include, for instance, current state contract, tort and criminal law provisions, as well as student and employee privacy. The two bills are similar on one topic: allowing state laws to continue for the notification of consumers in the event of a data breach.

As was discussed in two previous articles for the IAPP, "preemption is a technically complex subject, as well as being politically controversial." The political controversy is well known: Industry emphasizes the need for a uniform national law, while privacy advocates emphasize the role that states play in providing new protections for consumers. One major political question will be whether the federal law will preempt new and comprehensive state laws, such as the California Consumer Privacy Act or the similar Nevada legislation.

In our work, we are not seeking to resolve this political debate. We instead seek to provide technical assistance, to assist those from all perspectives to narrow the areas of disagreement. Our proposal seeks a way out of the current zero-sum debate in which one side "wins" and the other "loses" depending on how much preemption occurs in a federal privacy law. Our proposal seeks to define areas of consensus concerning state data privacy and security laws. After developing areas of consensus, there likely will remain important disagreements. Those disagreements, however, will concern a more manageable subset of issues. If the negotiators get to a small subset of issues, then an overall deal becomes more likely.

Here is the proposal. The late Robert Ellis Smith published a "Compilation of State and Federal Privacy Laws," most recently updated in 2018. We propose that the members and legislative staff working on privacy legislation simply read through the existing laws. Our hypothesis is there will be consensus for some categories of current laws that should be retained. For instance, we doubt the drafters are seeking to repeal attorney-client privilege or state cybercrime laws that prohibit hacking. Where there is consensus, have congressional experts in legislative drafting create language to implement the consensus.

Here are chapters in the Smith compilation that address the commercial use of personal information covered by the proposed bills:

1. Arrest records, including rules about sale of arrest records for background checks.
2. Bank and financial records, including rules limiting disclosure of account information.
3. Cable television, including records of video watched.
4. Computer crime, including what constitutes illegal entry into a computer system.
5. Credit reporting and investigations, including limits on fraudulent "credit repair."
6. Electronic surveillance, including states that require all parties to consent to recording a conversation.
7. Numerous state laws regulating privacy in employment, from limits on video surveillance in the workplace to prohibitions on requiring employees to provide social media passwords. The Smith book contains an additional chapter on urinalysis, genetic and blood tests.
8. Identity theft, including criminal and civil penalties for identity fraud.
9. Insurance records, including use of genetic information.
10. Library records, including prohibitions on commercial sale of such records.
11. Mailing lists, including individual rights to opt out of lists.
12. Medical records, including HIV testing and many other state laws that have continued in effect after the Health Insurance Portability and Accountability Act.
13. Miscellaneous, including breastfeeding and non-electronic visual surveillance.
14. Polygraphing in employment.
15. Privacy statutes/state constitutions, including the tort right to publicity.
16. Privileged communications, including protection of attorney/client, doctor/patient and spousal privileges.
17. Social Security numbers, including laws prohibiting display or required provision of SSNs.
18. Student information, including laws passed in recent years limiting commercial use of student information in school software.
19. Tax records, including prohibitions on requiring tax records except in specified situations.
20. Telephone services, including Caller ID and Do-Not-Call state laws.
21. Tracking technologies, including drone surveillance and location tracking.

This list is not complete: It omits, for instance, important state cybersecurity laws outside of data breach, including New York's Department of Financial Services Cybersecurity Regulation. In addition, states have recently added other laws, concerning topics such as data brokers and internet-of-things cybersecurity. To help build consensus around this complex question and supplement the Smith compilation, the Future of Privacy Forum has begun to list and categorize existing and potential future privacy laws that might be impacted by a federal law. Readers who are aware of other state data privacy or security laws are welcome to contact FPF.

Our goal in this description of state laws is not to persuade Congress about what should be preempted. Instead, the goal is to provide an accurate resource about state laws. That can assist those negotiating on preemption to draft a bill that accurately implements what they wish to accomplish.

For those interested in precedent, the proposed examination of state laws resembles the process Congress used in drafting the Foreign Intelligence Surveillance Act of 1978. For national security reasons, the government did not wish to publicly release details of its actual surveillance practices at the time. Instead, those negotiating the bill crafted a series of hypotheticals, similar in this respect to the actual state laws discussed here. Those negotiating FISA then reached consensus by discussing the hypotheticals, and the bill became law. For preemption, similarly addressing specific existing state laws can assist the negotiators to discover important areas of agreement.

We add two additional topics for comment. First, data privacy and security laws operate against the background of general tort, contract, property and criminal law. Since Louis Brandeis and Samuel Warren published the "Right to Privacy" in 1890, state tort law has protected individuals against harms such as public disclosure of private facts. Privacy protection takes place under state contract law, such as the innumerable business associate and other contracts in which one company relies on a written contract to ensure the other company follows good security and privacy practices. Similarly, criminal law applies to serious violations such as hacking and identity theft. We encourage legislators to be cautious about disrupting these general legal protections.

The second topic concerns how the federal law will approach emerging issues of data privacy and security. Information technology keeps evolving, leading to new privacy and security issues in information management. For instance, in the absence of federal privacy legislation, we may see states considering topics such as virtual and augmented reality, smart-cities regulation, automated decision-making and artificial intelligence, and laws about confidentiality and data sharing if a new epidemic occurs, similar to the HIV laws from the 1980s.

To the extent Congress decides to implement preemption, it may wish to consider whether to include any escape valves, to address new technologies or in some other way. Creative use of a sunset provision is one way to prompt Congress to reexamine issues that merit reconsideration over time.

We are suggesting that the seemingly intractable issue of preemption can become more manageable by studying existing state data privacy and security laws. The positive goal is to discover areas of consensus and draft legislation accordingly.

On the other hand, failure to do this state law analysis would risk at least two major problems. First, the federal legislation could have unintended negative consequences, such as making current privacy-protecting contracts unenforceable. Second, the repeal of desirable state laws could become a persuasive basis for opposing an otherwise-desirable federal privacy law.

In short, informed consideration of existing state and future laws is important to completing the drafting of federal privacy legislation.