I. Issues that Have Increased Interest in Federal Privacy Legislation

March 2018, Cambridge Analytica access to Facebook data
May 2018, European Union General Data Protection Regulation becomes effective and data transfer formalities continue to be vulnerable due to EU perception that US privacy law is inadequate
June 2018, California Consumer Privacy Protection Act signed into law with effective date of January 2020 creating new consumer options for control over data about themselves

All against a backdrop of:

- Years of data breaches, including large ones involving Equifax in 2017 and Marriott in 2018;
- States passing data breach notification laws that vary and make multi-state compliance complicated;
- States continue creating new privacy laws (e.g. Illinois’ Biometric Information Privacy Act, http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004 ) and applying state consumer protection laws (unfair or deceptive trade practices) to privacy, some with options for private rights of action...all creating complexity for multi-state compliance and potentially frustrating companies’ ambitions for data-driven developments;
- Fragmented landscape of privacy law that includes sectoral legislation and regulation arguably passed in response to a technology environment that changing more rapidly than the law;
- Federal standing jurisprudence that limits ability of plaintiffs to bring actions for violations of privacy laws;
- Concerns about artificial intelligence and the possibilities for bias and discrimination from automated data processing.

II. Drafts and Other Proposals relating to New Federal Privacy Legislation

A. Intel: Innovative and Ethical Data Use Act, https://usprivacybill.intel.com (detailed draft bill with enforcement by FTC that is given increased support and rulemaking authority; use and accountability method instead of a focus on consent; risk-of harm to individuals or society assessments are required by businesses; FTC regulates risk-assessment; avoids conflict with existing sectoral statutes like HIPAA but does wrap in ISPs; preemption of state law, no private right of action) https://blogs.intel.com/policy/2018/11/05/intel-solicits-feedback-on-u-s-privacy-law-proposal/#gs.SamFQ1D6

Includes a right of Data Portability along with traditional rights like access and correction. Codifies existing FTC Section 5 precedent. Preempts state laws. Has a larger list of “presumptively unfair” data uses such as processing of biometric information and precise location information.


D. Senator Brian Schatz (D-Hawaii): [Data Care Act of 2018](https://www.congress.gov/bill/115th-congress/senate-bill/3744/) (addresses online service providers’ duties of care, loyalty, and confidentiality; focuses on FTC and state AGs for enforcement; does not “modify, limit, or supersede the operation of any privacy or security provision in any other Federal or State statute or regulation.”)

E. Senator Ron Wyden (D-Oregon): Discussion Draft for [Consumer Data Protection Act](https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20Discussion%20Draft%20Nov%201.pdf) (extensive draft; expands FTC authority to promulgate regulations for privacy and data security and allows FTC to fine for violations potentially fines based on 4% of gross revenue; would require annual data protection reports to the FTC; false certification by corporate officers would carry criminal penalties and intentional false certification would result in personal fines based on compensation; FTC would implement Do-Not-Track website for consumer opt-out from data collection and use; anticipates business benefits if it provides consumers an option for fees rather than data collection; preempts private contracts, so no waiving of these terms; violations are unfair or deceptive trade practices; creates Bureau of Technology within the FTC to be led by Chief Technologist appointed by Chair of the Commission; adds 100 personnel in a Division of Privacy and Identity Protection and 25 in the Division of Enforcement and authorizes funds; provides exceptions for journalism).

F. Senator Marco Rubio (R-Florida) [American Data Dissemination Act of 2019](https://www.congress.gov/bill/116th-congress/senate-bill/142/) (based on Privacy act of 1974 emphasizes transparency and accountability but accommodates small businesses; calls for the FTC to develop proposals for Congress to enact, or failing enactment after 2 years, proposals would become effective regulations)

G. National Telecommunications and Information Administration; Dept. of Commerce; in October 2018 sought and in December 2018 published comments on 7 privacy and data security outcomes: transparency, consumer control, reasonable data minimization, security safeguards, consumer ability to access and correct personal data, risk-management for disclosure or harmful uses, and accountability. Federal law to preempt state law was a common goal among responders: [https://www.ntia.doc.gov/other-publication/2018/comments-developing-administration-s-approach-consumer-privacy](https://www.ntia.doc.gov/other-publication/2018/comments-developing-administration-s-approach-consumer-privacy)

H. U.S. Chamber of Commerce: [https://www.uschamber.com/issue-brief/us-chamber-privacy-principles](https://www.uschamber.com/issue-brief/us-chamber-privacy-principles) (advocates federal legislation that preempts state law to create certainty and consistency; risk-of-harm and benefits of data use should guide regulation; businesses should be transparent about data use; federal law should be industry neutral; concludes consumers benefit from responsibility use of data)
I. Internet Association (including Amazon, Facebook, Google, Twitter, etc.)
(advocating federal legislation to streamline compliance, with technology and sector neutrality; FTC and state AG enforcement; standards rather than prescriptive solutions that can become outdated; risk-of-harm based; preemption of state consumer privacy and data breach laws)


K. Charter Communications - https://policy.charter.com/blog/charter-urges-congress-pass-legislation-protecting-privacy-everywhere-internet/ A call for federal preemptive privacy legislation without many details other than a call for transparency and an opt-in for third party data sharing

L. Information Technology and Innovation Foundation – http://www2.itif.org/2019-grand-bargain-privacy.pdf?_ga=2.249272448.665337977.1549330775-2130593196.1549330775 A lengthy report detailing principles for a preemptive privacy law that would supersede existing state and federal privacy laws. Would provide more resources to the FTC and codify basic notice, consent, access and choice obligations, but would otherwise not provide obligations on companies to adopt accountability mechanisms.

III. Frameworks and Features

   a. Collection limitation
   b. Data quality
   c. Use Limitation
   d. Security safeguards
   e. Openness
   f. Individual participation
   g. Accountability

B. Defining FIPPs-related terms
   a. Personal information/Data
   b. Sensitive information
   c. Covered Entity Definition
      i. Corner nail salon
      ii. Information intermediaries (journalists? Libraries?)
   d. Notice
   e. Consent
   f. Transparency
   g. Reasonable data security
   h. Consumer access to held information
i. Third Party
j. Harm, injury, risk
k. Accountability obligations (How much is too little, and how much is too much?)

C. Beyond the FIPPs
   a. Corporate reports on data privacy to be signed by executives
   b. Criminal penalties for executives signing false statements regarding privacy practices
   c. Non-waivable limitations on personal information deemed sensitive
   d. Registries for some actors such as data brokers
   e. Non-waivable restrictions on some sensitive information

D. Remedies and enforcement
   a. Federal Trade Commission questions of expertise, sufficient number of staff, regulatory authority, ability to fine
   b. State AGs (Concurrent with or supplementary authority in relation with FTC?)
   c. Private rights of action? Can federal law preempt negligence claims?
   d. Should safe harbors be designed?

E. Preemption of state law

F. Impact on existing federal law

G. Third party transfer restrictions and obligations (the data broker problem)

H. Right to be Forgotten/Obscurity

I. First Amendment

J. Federal Standing if Private Right of Action

IV. Likelihood of New Legislation Passing in 2019

???

APPENDIX

INTEL SOLICITS FEEDBACK ON U.S. PRIVACY LAW PROPOSAL

Written by David Hoffman | November 5, 2018


By: David A. Hoffman, Associate General Counsel and Global Privacy Officer
Intel is experimenting with a new approach to participatory democracy. We have created a website on which we have posted our recommended draft for a comprehensive U.S. privacy law. The website has a portion where privacy law experts are providing feedback on the draft, and for the public to provide comments. We are going to keep the discussion going for two weeks and then will revise our draft. We encourage everyone to visit the website and participate. Here is some background on the effort and a description of our draft.

**Why Pass a US Federal Privacy Law?**
Effective privacy regulation is critical to allow technologies like artificial intelligence to help solve the world’s greatest challenges. The combination of advances in computing power, memory and analytics create the possibility that technology can make tremendous strides in precision medicine, disease detection, driving assistance, increased productivity, workplace safety, education and more. At Intel we are developing many of these technologies and are focused on integrating artificial intelligence capability across the global digital infrastructure. At the same time, we recognize the need for a legal structure to prevent harmful uses of the technology and to preserve personal privacy so that all individuals embrace new, data-driven technologies. At Intel we know that privacy is a fundamental human right and robust privacy protection is critical to allow individuals to trust technology and participate in society.
What the US needs is a privacy law that parallels the country’s ethos of freedom, innovation and entrepreneurship. That law needs to protect individuals and enable for the ethical use of data. As noted above, the use of data by new technologies such as artificial intelligence will help us solve some of the most vexing global problems while spurring economic growth. That ethical use of data will be critical as we use the data to train artificial intelligence algorithms to detect bias and enhance cyber security. In short, it takes data to protect data. The US needs a law that promotes ethical data stewardship, not one that just attempts to minimize harm. A non-harmonized patchwork of state legislation will cause companies to default to restrictive requirements and the result will decrease the likelihood of realizing technology’s great potential to improve lives.

**How is the proposal structured?**

The law uses the Fair Information Practice Principles (FIPPs) from the Organization for Economic Cooperation and Development’s (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. The OECD FIPPs are “the Global Common Language of Privacy” and many of the privacy laws around the world are based on them. For the past few years, Intel has worked on a “Rethinking Privacy” initiative to take the OECD FIPPs and show how they can be implemented in law differently to promote the innovative and ethical use of data.

**How will the law be enforced?**

Robust, harmonized and predictable enforcement is necessary. The US Federal Trade Commission has decades of experience protecting privacy. What the Commission needs are: 1. More resources, 2. Authority to oversee all industry sectors, 3. A clear mandate to develop guidance and regulations to communicate to organizations how they should implement the FIPPs, and 4. The ability to enforce meaningful but fair sanctions. Our proposal provides all four of those elements, while also preserving a role for State Attorneys General to apply sanctions in situations where the Commission declines to start an enforcement action. The law uses those sanctions as a way to further encourage organizations to demonstrate their accountability, by allowing those entities that adopt robust privacy programs to have a safe harbor from civil penalties.