Cooley

March 5, 2015

On February 27, 2015, President Obama released a draft of a proposed Consumer Privacy Bill of Rights Act (Proposal). The Proposal aims to protect the privacy of individual consumers on the Internet by (a) establishing baseline expectations for companies that collect and use consumer data on the Internet and (b) encouraging businesses to voluntarily adopt public codes of conduct for how they handle consumer data. These protections would ultimately be enforced by the Federal Trade Commission (FTC) or State Attorneys General.

Who and what is covered?

The Proposal would cover any entity that "collects, creates, processes, retains, uses, or discloses personal data in or affecting interstate commerce."[1] It would exempt Federal and state governments, and certain small entities from coverage. The Proposal defines "Personal Data" as any data that can be linked to a specific individual or device which is not publicly available.[2] Data that is de-identified, deleted, or used to investigate or respond to a cybersecurity threat would be specifically exempted from Personal Data.

These definitions of Personal Data and Covered Entities are broad; they would likely cover most businesses that use the Internet to provide goods or services or connect with customers, and most personal data that a business requests or collects from customers. The Personal Data definition includes, for example, data that can be linked to a specific device, not just a specific individual.[3]

The Proposal also includes several exceptions that protect businesses from inadvertent violations. For instance, the Proposal excludes de-identified data, or data that has been altered so that it cannot be linked "as a practical matter" to an individual person or device, from coverage.[4] This would allow a business to use information it collects to improve and analyze its services or even offer third parties general data about its user base as long as that data is stripped of information that could be tied to an individual user. The Proposal also exempts deleted data, employee business information, and information used or disclosed to respond to cybersecurity threats or incidents.

Several entities would be exempt from the Proposal. Businesses that have fewer than 5 employees or that process Personal Data from fewer than 10,000 individuals or devices each year would not be covered. As a further protection, businesses cannot face liability for the first 18 months they create or process Personal Data.

Title I: Privacy Bill of Rights

The Proposal would require covered entities to use reasonable data collection and storage practices measured under 7 different considerations. In particular, covered entities would have to:

- Give consumers reasonable notice about the type, source, and uses of the Personal Data it collects; policies about disclosure, de-identification or destruction; and how individuals may access or change their Personal Data. (*Transparency*)
- Offer consumers a reasonable way to control how their data is collected and used. (*Individual Control*)
- Process Personal Data in a way that is reasonable for the context. This could include performing a privacy risk analysis or submitting their data processing activities for approval by an FTC-approved Privacy Review Board. (*Respect for Context*)
- Limit its collection and use of Personal Data to reasonable practices. This would include deleting, destroying, or de-identifying data after a reasonable amount of time. (*Focused Collection and Responsible Use*)
- Identify risks to the privacy and security of Personal Data, implement reasonable safeguards against unauthorized disclosure, and frequently evaluate their security procedures to make sure their practices are adequate. Entities would have to consider sensitivity of data, foreseeability of threats, industry practices, and cost of implementing safeguards to determine if their security is reasonable. (*Security*)
- Allow individuals reasonable access to Personal Data and maintain a procedure to correct or delete inaccurate data. (*Access and Accuracy*)

- Maintain adequate processes, training, evaluations of privacy procedures, design processes, and confidentiality contracts with third parties to protect the privacy of Personal Data. (*Accountability*)

The Proposal would require businesses to pay specific attention to the context under which personal data is processed. In this regard, the Proposal identifies 11 explicit factors businesses must analyze when establishing the context of their data practices.[5] A business could collect more data, analyze it "in a manner that is not reasonable in light of context," or use it differently than a consumer would expect under the circumstances if the business provides greater transparency or individual control to the consumer.[6] This could include specific "opt-in" procedures for the unusual collection or use of data, and it may require offering users more extensive and customizable privacy settings.

A business would also be allowed to submit its use of Personal Data to a Privacy Review Board instead of offering greater transparency or more extensive individual controls when the analysis of personal data is not reasonable under the given context. The Privacy Review Board would allow the practice if allowing heightened transparency or control is impractical, the practice provides substantial benefits to someone other than the covered entity, the business has taken steps to mitigate privacy concerns, and the overall benefits of the practice outweigh its risks.

Title II: Enforcement

The Proposal would be enforced by the FTC or by the Attorney General of any State through statutory civil penalties or injunctions. The FTC would have the power to enforce Title I violations as an unfair or deceptive act under Section 5 of the FTC Act and only the FTC could seek civil penalties. Daily civil penalties up to $35,000 per day could be issued for knowing violations of the Proposal. If the FTC gave the entity notice before taking action, it could issue penalties of up to $5,000 per aggrieved consumer. The entity could avoid a per-consumer penalty by filing an objection within 45 days of receiving notice. The total civil penalty would be statutorily limited to $25 million, and the FTC could not bring an enforcement action for the first 18 months a covered entity processes Personal Data.

This means that businesses would only be fined up to $35,000 per day if they committed a knowing violation of the Proposal. The penalties would become much more severe if the business continues its violations after the FTC notified the business that it is violating the Proposal. The FTC may impose a fine of up to $5,000 per consumer after this notice is given. Penalties would be capped at $25 million.

States attorneys general could bring an enforcement action in an appropriate federal district court for injunctive relief only. A State Attorney General would have to give the FTC notice 30 days before bringing such an action. The FTC would have the power to intervene or it could allow the State Attorney General to proceed without it.

The Proposal explicitly rejects creating any new private rights of action. This means that consumers could not sue businesses for violating the Proposal. Only the FTC or Attorney General of a State may enforce the provisions of the Proposal. The Proposal would not preempt other claims under state law, such as violations of consumer protection laws or tort laws, unless the state law specifically regulated personal data processing. The Proposal also would not preempt other federal laws that regulate privacy.

Title III: Codes of conduct and safe harbors

The FTC would have to issue regulations to develop codes of conduct for FTC approval. Any approved code of conduct must provide equal or greater consumer protection than Title I and include a process for reviewing the code to ensure continued effectiveness. The process for approving codes of conduct would include a public comment period on the code.

Any person could apply for certification to administer and enforce codes of conduct by the FTC. This administrator could monitor compliance with and enforce violations of FTC approved codes of conduct.

If a covered entity complied with an approved code of conduct, it would have a complete defense against any alleged violation of Title I or any action brought under Title II.

This Title would offer businesses an opportunity to work with other actors in their industry to craft guidelines that address their specific needs and still comply with the Proposal. The industry could certify an expert to monitor individual businesses' activities and approve their personal data processing behavior. If a business complied with an approved code of conduct, it would have a complete defense against any violations of the Proposal.

Why this proposal matters

The Obama Administration has identified Internet privacy as an important issue for the United States economy. This discussion draft of a Consumer Privacy Bill of Rights represents one of the Administration's most concrete effort to date for creating a comprehensive legal framework regulating online privacy. It aims to fill in the gaps left by prior, more targeted executive orders and laws that discuss the issue and create a consistent, nationwide policy governing privacy issues.

The Proposal would require businesses to adopt "reasonable" privacy practices which are evaluated according to seven key factors. The Proposal would encourage businesses to participate in a multi-stakeholder process that may tailor targeted codes of conduct for specific industries. If enacted, many businesses may want to contribute to the development of these codes of conduct so the business can reduce the amount of disruption the law's requirements would create. If a business follows an approved code of conduct, it will not be liable for violating the Proposal. Finally, while the Proposal does not permit private lawsuits, the FTC would have the power to impose significant fines for companies that violate the Proposal.

Presently, there is no congressional sponsor for the measure and its legislative path forward is uncertain. Several industry representatives and privacy advocates issued negative initial reactions to the Proposal. Moreover, the FTC signaled that they oppose the plan as currently drafted. Further complicating matters is the fact Congress is more focused on legislation around discrete privacy issues such as data breach notification and members may be resistant to adding this significant proposal to those efforts.

Notwithstanding the chances of the Proposal becoming law, it does signal the Administration's position on commercial data use and collection. Therefore, it will be important for businesses to engage in any discussion leading to revisions of the draft Proposal and understand its requirements. Businesses may also want to incorporate the basic principles articulated in this Proposal into their current privacy practices since the Administration may try to implement some of these requirements through other government agencies despite the current gridlock in Congress.

NOTES

1. Section 4(b)
2. Section 4(a)
3. Section 4(a)(1)
4. Section 4(a)(2)(A)
5. Section 4(k)
6. Section 103

Key Contacts

Matthew D. Brown **San Francisco**	**brownmd@cooley.com** **+1 415 693 2188**
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090
Vince Sampson Washington, DC	vsampson@cooley.com +1 202 728 7140