Policy Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Senior California Democrats Stake Out Privacy Position with Draft Federal Framework

June 27, 2019

Background

As the privacy debate heats up on Capitol Hill, Rep. Anna Eshoo (D-CA), a senior member of the House Energy and Commerce Committee, and Rep. Zoe Lofgren (D-CA), a senior member of the House Judiciary Committee—both of Silicon Valley—have teamed up to draft privacy legislation, the Online Privacy Act of 2019 (Act). The pair recently shared their draft framework for the Act with stakeholders. They have solicited feedback, which is due by July 12, 2019.

Akin Gump is working with clients to address issues raised by the framework. Please reach out to one of the attorneys listed below if you are interested in joining this effort or obtaining additional information.

The Eshoo-Lofgren framework does not include a provision to preempt state laws like the expansive California Consumer Privacy Act (CCPA), which takes effect on January 1, 2020. As California Democrats, Reps. Eshoo and Lofgren were not expected to support preemption at this early stage, particularly in light of Speaker Nancy Pelosi's (D-CA) public comments expressing skepticism about federal legislation that preempts protections provided by the CCPA.

The Eshoo-Lofgren draft is representative of the high standards California Democrats will demand if they are asked to support legislation that includes federal preemption of the CCPA. Additional federal privacy legislation is still expected from the Senate's Gang of Six (Sens. Wicker (R-MS), Moran (R-KS), Thune (R-SD), Cantwell (D-WA), Schatz (D-HI) and Blumenthal (D-CT)) and with the Energy & Commerce Committee in the House.

Highlights

- Does not preempt state privacy laws or outline the bill's impact on other federal data laws, such as the Gramm-Leach-Bliley Act (GLBA) or the Health Insurance Portability and Accountability Act (HIPAA).
- Creates a new "U.S. Digital Privacy Agency" modeled after the Consumer Financial Protection Bureau.

Contact Information
If you have any questions concerning this alert, please contact:

Ed Pagano
Partner
epagano@akingump.com
Washington, D.C.
+1 202.887.4255

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Ryan Thompson
Senior Advisor
thompsonr@akingump.com
Houston
+1 202.887.4138

James Romney Tucker Jr.
Partner
jtucker@akingump.com
Washington, D.C.
+1 202.887.4279

Chris A. Treanor
Counsel
ctreanor@akingump.com
Washington, D.C.
+1 202.887.4551

Diana E. Schaffner
Counsel
dschaffner@akingump.com
San Francisco
+1 415.765.9507

-
- Gives individuals the right, if technologically feasible, to opt out of personalized targeting, and covered entities must provide nonpersonalized versions of services.
- Includes a private, right of action, by which individuals can seek injunctive relief for any violation of the Act, and a more expansive form of collective action whereby non-profits can bring cases on behalf of individuals, or at the request of states, and seek a range of recourses (including monetary damages and fees) for any violation of the Act.
- Permits enforcement by state attorneys general (AGs), who may bring cases themselves or assign rights to bring cases to non-profits.
- Grants individuals new rights, including the (1) right of access, (2) right of correction, (3) right of deletion, (4) right of portability (limited), (5) right to human review of automated decisions, (6) right to opt out of personalized content and (7) right to be informed.

Definitions

The draft framework's definitions section will attract significant attention from industry stakeholders and privacy advocates. The "covered entity" definition is broad. It includes all entities that both process personal information and transmit information over "an electronic network." The definition excludes service providers (e.g. ISPs), which are entities that do not control the selection or transformation of personal information and do not differentiate between personal information and other types of information. Service providers are not required to comply with the section of the Act concerning individuals' rights.

The draft framework defines "personal information" to include any information that is linked or reasonably linkable to a specific individual. Excluded from this definition is information an individual makes public, information derived from personal information that cannot be linked back to an individual and information "that has been obfuscated" in a manner the covered entity cannot reverse. These exclusions appear to cover deidentified and aggregate information.

Certain provisions of the draft framework would not apply to "small businesses," defined as entities that do not earn revenue from the sale of personal information, earn less than half of their annual revenue from targeted advertising, have fewer than 500,000 users, have less than 200 employees or have less than $10 million in revenue. The exemption for small businesses is limited to certain provisions of the Act only. Certain rights, like the right to be informed or the limited right to human review of automated decisions, would apply to any covered entity.

Title I: User Rights

The draft framework centers on core user rights, including rights to access, correction, deletion and portability. Some of these rights are limited to situations that create, or increase, "privacy harms," which is broadly defined to include a range of, among others, monetary, psychological or reputational harms. The draft framework grants users the right to access all of their personal information and requires covered entities to inform users how their information has been disclosed (i.e., to which third parties) and why the information was collected or shared.

Dario Frommer
Partner
dfrommer@akingump.com
Los Angeles
+1 213.254.1270

Galen Roehl
Senior Policy Advisor
groehl@akingump.com
Washignton, D.C.
+1 202.887.4224

Taylor Daly
Public Policy Specialist
tdaly@akingump.com
Washington, D.C.
+1 202.416.5541

Users also have a right to correct or dispute inaccuracies in their personal information. This mirrors a right granted to data subjects under the European Union's General Data Protection Regulation (GDPR).

The draft framework's right to deletion potentially goes beyond that in the CCPA to the extent that it explicitly requires covered entities to delete personal information the entity collected or received, including from third parties.

Only covered entities that meet certain requirements are obligated to abide by the right to portability. The draft framework proposes to establish an oversight Agency that would provide additional details on this issue.

Reflective of many privacy advocates' concerns, the draft framework would allow users to request human review for any privacy-related action carried out through an automated process. This right would be limited to situations where the decision at issue creates or increases significant privacy harms to the requesting user.

The draft framework also establishes the rights for consumers to opt-out of data collection used for targeted material. It requires platforms to allow users the option to use a version of the service without personalized content.

There are several exemptions to user rights. The draft framework's user rights do not apply to personal information used for safeguarding against malicious activity, law enforcement purposes, legal obligations, public safety, preventing service abuses and uncovering cybersecurity events.

Covered entities are also free to deny user requests under Title I that if they cannot confirm a user's identity, they are prohibited, by law, from complying or denying the requests necessary to protect a right or privilege, the request would limit free expression or pose a safety risk or if the information is necessary for a transaction or contract and was collected solely for that purpose.

Finally, Title I does not apply to deidentified data that cannot be reidentified using data stored by the covered entity.

Title II: Privacy and Security Requirements

The draft framework contains a provision on data minimization, which establishes that the collection, processing or storage of personal information must be conducted for a legitimate business purpose and account for possible privacy harms. It further proscribes notice requirements for collecting information that is concise, clear and meets metrics to be established by the new Agency. Covered entities must obtain consent from users for each category of a third party which they intend to send user data to.

Title II of the draft framework establishes several prohibitions on the disclosure of personal information, including disclosing user information to entities outside of the jurisdiction of the U.S., selling user information without obtaining consent for each transaction (this does not apply to lead generating and aggregation services requested by user) or including personal information in advertisement disclosures allowing for its connection to past or future disclosures.

Consent is not required for deidentified personal information if the data has been deidentified using best practices, and where disclosure is limited to the narrowest possible scope for the intended benefits.

The draft framework includes information security provisions that require reasonable security, mandate a range of precautionary measures (e.g., adopt an incident response plan) and obligate covered entities to provide quicker and more wide-ranging notice following data breaches. Covered entities experiencing a data breach would have to disclose to the data protection agency and the other entities affected within 72 hours. Entities would be required to notify individual consumers of a breach within 14 days. The event must be disclosed to users within 72 hours if it would be likely to lead to additional privacy harms.

The draft framework's focus on information security, as well as privacy, may mark a new drive to handle these issues in a single piece of legislation. Information security has not been a primary focus of Senate efforts to draft privacy legislation, with some lawmakers discussing the need to tackle data security in a separate bill. Rep. Schakowsky (D-IL) has also discussed the possibility of bundling competition and data protection provisions together in a bill.

Title III: Digital Privacy Agency

The draft framework notably proposes that a new agency be created to enforce a federal privacy standard. This perspective deviates from recent calls for increased enforcement authority and resources for the Federal Trade Commission (FTC) to penalize companies for privacy violations.

The proposed U.S. Digital Privacy Agency (Agency) would be comparable to the Consumer Financial Protection Bureau (CFPB) and would be authorized for $200 million with around 1,600 staff members. The staff allotted in the draft framework is significantly higher than current staff devoted to working on similar issues at the FTC, which has consistently received criticism for its lack of full-time staff devoted to privacy and data security.

The Agency would be led by a presidentially appointed Director, who would serve a term of five years. A Deputy Director would also be appointed, and the Agency would contain a principal office, along with several field offices. Congressional oversight of the Agency would be conducted by the House Energy and Commerce Committee and the Senate Commerce, Science, and Transportation Committee.

Title IV: Enforcement

The draft framework grants the new Agency the authority to conduct investigations, hold hearings and adjudication proceedings, and impose civil monetary penalties for violations of the law. It also allows the Agency to grant other forms of relief, including notification of the violation to the public, payment of damages, restitution, reformation of contracts, and disgorgement.

Enforcement would be shared with state AGs, who could bring cases or assign non-profits to bring cases on behalf of their citizens. The Agency would be able to take over any case from a state AG.

Finally, the draft framework contemplates civil enforcement by both individuals and non-profits to seek recourse for any violation of the Act. The CCPA's private right of

action, in contrast, is currently limited to the data breach context. Individuals would only be able to seek declaratory or injunctive relief. Non-profits acting on behalf of individuals, however, may be able to seek additional recourse, including damages and fees.

The issue of whether and the extent to which to include a private right of action in federal privacy legislation recently prompted a clash between lawmakers in the Senate Gang Six's privacy working group. We expect this issue to continue to be hotly contested.

akingump.com