

# GOVERNMENT RELATIONS POLICY POSITION PAPER

## Data Security and Privacy

### The Issue

Data breaches, which have increased in size and severity, continued to break records in 2019. Despite increased risk and frequency, congressional efforts to pass meaningful legislation have stalled. Members introduce a number of bills during each session, but long-standing issues of jurisdictional overlap, policy disputes between the financial, retail, and tech sectors, and concerns over federal preemption<sup>1</sup> continue to derail legislative efforts. In the absence of federal action, a patchwork framework of data security and privacy laws has emerged at the state level. LPL Financial believes that a comprehensive federal bill that preempts state law would provide clarity, uniformity, and regulatory relief from conflicting state requirements.

### Current Status

The pandemic has spawned new discussions among federal lawmakers regarding the collection and use of consumers' health and geolocation data. In 2021, while there is still a push for a federal privacy standard, Congress has shifted its immediate focus to the issues of misinformation and disinformation, cybersecurity, and anticompetitive behavior. Nonetheless, LPL, along with several industry groups, continue to advocate for a federal privacy standard that upholds individual consumer rights and while maintaining an ease of doing business.

So far, this year has brought forth only one privacy proposal; however, both Chambers will continue to update and reintroduce proposals from the last Congress in the coming months.

#### 117<sup>th</sup> Congress (January 3, 2021 – January 3, 2023)

- Representative DelBene's (D-WA) introduced the *Information Transparency and Personal Data Control Act*, which marks Congress' initial foray into privacy legislation during the 117<sup>th</sup> Congress.

Rep. DelBene's privacy bill is underpinned by a focus on protecting sensitive personal information, particularly related to personal finance, health, genetics, geolocation, sexual orientation, immigration status, social security numbers, and religious beliefs. Further, the proposal would require companies to issue "plain English" privacy policies, provide opt-in, submit to privacy audits every two years from a neutral third party, and increase transparency via disclosures. In terms of enforcement, the authority of the Federal Trade Commission (FTC) and state Attorneys General (AGs) would be enhanced to ensure rulemaking entities can fine bad actors on the first offense. The bill also prioritizes federal preemption and provides protections for children under 13 years of age. Note, the latter was a recurring theme during the recent House Energy and Commerce hearing with the CEOs of Facebook, Twitter, and Google.

Other House efforts are expected this year from Rep. Schakowsky (D-IL), Chair of the House Energy and Commerce Subcommittee on Consumer Protection and Commerce. She has shared her plans to introduce a privacy bill which "holds companies to account for bad behavior, rather than one that rubber stamps the worst industry practices." Rep. Bilirakis (R-FL), Ranking Member of the Subcommittee on Consumer Protection and Commerce, has expressed a willingness to work with Chair Schakowsky in order to take the best provisions from state laws and enact a bipartisan federal privacy standard.

The Senate has yet to introduce any privacy legislation in 2021.

---

<sup>1</sup> Federal preemption occurs when federal law limits or supersedes state law.

## 116<sup>th</sup> Congress (January 3, 2019 - January 3, 2021)

- Senator Maria Cantwell (D-WA) and other Democratic senators introduced the *Consumer Online Privacy Rights Act of 2019 (COPRA)*,
- Senator Roger Wicker (R-MS) introduced the Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (SAFE Data Act), which not only updated the staff discussion draft of the *United States Consumer Data Privacy Act of 2019 (CDPA)*, but also drew upon two prior bipartisan proposals – the *Filter Bubble Transparency Act* and the *Deceptive Experiences to Online Users Reduction Act (DETOUR Act)*;
- The House Energy and Commerce Committee, staff released a bill for discussion. Notable similarities of the three bills included definitions of covered data, broad applicability to entities subject to Federal Trade Commission regulation, creation of basic consumer privacy rights, and provisions that would have required businesses to maintain reasonable data security practices.

Despite the similarities of the federal privacy proposals, key differences highlighted the challenges ahead. State preemption will be critical to a federal privacy proposal. Federal preemption of state law would halt the proliferation of differing state standards and provide clarity to consumers and businesses. The House Energy and Commerce bill did not take any position on this issue, Senator Wicker's bill would have preempted state laws regarding data privacy or security, but did not preempt state data breach laws. Senator Cantwell's bill would have only preempted directly conflicting state laws and would have allowed states to pass stricter standards.

In addition to state preemption, disagreements over whether to allow consumers to sue companies for violating their privacy, known as a private right of action, persist. CDPA does not include a private right of action, the House bill has a placeholder for a potential private right of action, and COPRA would have allowed individual lawsuits in state and federal court.

According to Commerce Committee Ranking Member Roger Wicker (R-MS), data collection amid the pandemic underscores the need for a national privacy law. Furthermore, new state laws will continue to pressure the federal government to act. The three existing proposals represent a watershed in the privacy debate and will help to inform future legislation.

With the absence of a federal law, California passed the *California Consumer Privacy Act* in June 2018 to introduce strict privacy rules. The legislation went into effect on January 1, 2020. Several states have followed in filing legislation to increase protections surrounding data security and more are expected to follow. While LPL is in compliance with CCPA, we remain concerned about the patchwork of rules emerging from different states.

### **LPL Position**

LPL believes that any company that collects and stores personal information must implement and maintain reasonable security practices to protect the information and notify consumers in the event that their personal information has been unlawfully accessed. We also believe that appropriate federal and state regulators should enforce a national standard. Individual lawsuits by citizens have the potential to be abused and would not adequately address privacy issues.

In this vein, LPL will continue to advocate for thoughtful data security and breach notification legislation. Moreover, LPL will continue to advocate for a federal preemptive standard.

This material was prepared by LPL Financial.

**Securities and advisory services offered through LPL Financial (LPL), a registered investment advisor and broker-dealer (member FINRA/SIPC).** Insurance products are offered through LPL or its licensed affiliates. To the extent you are receiving investment advice from a separately registered independent investment advisor that is not an LPL Financial affiliate, please note LPL Financial makes no representation with respect to such entity.

If your financial professional is located at a bank or credit union, please note that the bank/credit union **is not** registered as a broker-dealer or investment advisor. Registered representatives of LPL may also be employees of the bank/credit union. These products and services are being offered through LPL or its affiliates, which are separate entities from, and not affiliates of, the bank/credit union. Securities and insurance offered through LPL or its affiliates are:

**Not Insured by FDIC/NCUA or Any Other Government Agency | Not Bank/Credit Union Guaranteed | Not Bank/Credit Union Deposits or Obligations | May Lose Value**

For Public Use | Tracking #1-05172842