R Street

Free markets. Real solutions.

R SHEET ON

# NATIONAL DATA PRIVACY AND DATA SECURITY LEGISLATION

April 2021

## BACKGROUND

As technology has become increasingly intertwined with every facet of our daily lives, companies hold unprecedented amounts of our personal information. As a result, ensuring data security (keeping this data out of the hands of hackers and other malicious actors) and data privacy (making sure companies do not misuse the data they hold) is more important than ever before.

A number of countries have responded to this need by rolling out or signing onto data security and data privacy laws, such as Europe's General Data Protection Regulation or Japan's Act on the Protection of Personal Information. Until now, the United States has allowed each state to determine their own data security and data privacy laws, resulting in a variety of different standards. This lack of a uniform national standard makes it difficult for both companies and customers to know how they can use data, what data needs to be protected and who is liable in the case of a breach.

## CURRENT DEBATE

While there is a general sense that it is important to have national, standardized laws on data privacy and data security, there are many areas of contention when it comes to the specifics of the law.

### Defining Personal Data

The first issue any law will have to grapple with is how to determine what types of data need to be protected and how. Standardizing these definitions will greatly assist with increasing transparency, as myriad laws currently in place define personal data differently.

Additionally, lawmakers will need to determine how to handle both de-identified and aggregated data, both of which can be useful for research but which run the risk of being abused if not secured properly. Some cases have shown that previously de-identified data can be re-identified.


SUMMARY

- Congress needs to pass a comprehensive, national legal framework for data privacy and data security.
- An effective framework will need to address liability, preemption, private right of action, competition and innovation.


### Preemption of Existing State Law

Also pressing is the question of whether a national law should preempt state privacy legislation. Privacy advocates argue that state privacy laws may be stricter and therefore overriding them may lead to data becoming less secure. They also argue that state legislation often serves as a marketplace for ideas, where new legal frameworks can be tested and tried as the need arises. Meanwhile members of industry claim uniformity is needed for the sake of harmonization and compliance, as complying with 50+ different data privacy standards is expensive for companies and confusing for customers.

### Private Right of Action and Liability

Also contentious, when it comes to comprehensive privacy and security legislation, is the issue of private right of action. Private right of action allows private parties, as opposed to the state, to stand to sue for injuries in a court of law.

Advocates of private right of action argue that private lawsuits are important for ensuring individuals who have their privacy rights violated have a way to seek redress. Adversaries, including most companies, worry that allowing class action lawsuits will lead to an overwhelming number

of nuisance lawsuits that will clog the judicial system and hamper companies as they live in constant fear of being sued. A national data law will also have to decide who is responsible for protecting the data in question: internet service providers, data holders or other parties.

### Competition and Innovation

A comprehensive data privacy and data security law will also need consensus regarding what types of data are covered and which uses of that data are permissible for companies. At the same time they consider which data should be protected, policymakers must also consider that overly strict limitations on the uses of data can limit innovation in emerging technologies, such as artificial intelligence, that require access to large datasets. Complying with privacy legislation can also be costly for small- and medium-sized enterprises, which could negatively impact economic growth and competition.

## ACTION ITEMS

Individuals need to know that their data is secure. To achieve this, there must be transparency regarding the security practices of companies holding their data.

In order to protect Americans' data and provide the regulatory transparency necessary for American companies to act confidently and securely, Congress needs to pass a national data privacy and data security law. Effective legislation will need to clarify a number of concerns including by defining what counts as personal data; determining how to deal with aggregated data; deciding what minimum standards should determine how and whether personal data can be collected, stored, analyzed or shared with a third-party; and how companies should handle requests for deletion or correction of data. The Federal Trade Commission should be equipped with the necessary authorities to be the primary enforcement body.

## CONTACT US

For more information on this subject, contact the R Street Institute, 1212 New York Ave. NW, Washington, D.C. 20005, 202-525-5717.

Tatyana Bolton
Policy Director, Cybersecurity and Emerging Threats
R Street Institute
tbolton@rstreet.org

Kathryn Waldron
Fellow, Cybersecurity and Emerging Threats
R Street Institute
kwaldron@rstreet.org