1212 New York Ave. NW
Suite 900
Washington D.C. 20005
202-525-5717

Free Markets. Real Solutions.
rstreet.org

February 26, 2023

Representative Gus Bilirakis, Chairman
Innovation, Data, and Commerce Subcommittee
House Energy and Commerce Committee

Re: Comments for the Record - "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy" Hearing on March 1, 2023

Dear Chairman Bilirakis,

I would like to thank you again for the opportunity to testify at the Feb. 1, 2023, hearing "Economic Danger Zone: How America Competes to Win the Future Versus China." I am thrilled to see that the March 1, 2023, hearing "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy" will focus on a comprehensive data privacy and security law. Such a law is needed now more than ever. Data privacy and security is a central part of the R Street Institute's Cybersecurity and Emerging Threats team's work. I respectfully submit a series of resources as "comments for the record" to aid the subcommittee as it considers a federal data privacy and security law.

For background, we published a report last year in conjunction with the Harvard Kennedy School's Belfer Center to provide recommendations to address some of the most challenging aspects of a federal data privacy and security law, including preemption, a private right of action and the role of the Federal Trade Commission. Our research included consultations with over 125 entities of varying ideologies, and we also held multiple events and Hill briefings. We were thrilled to see many of the recommendations make it into the bipartisan, bicameral American Data Privacy and Protection Act (ADPPA) last congress. We believe that a federal data privacy and security law will require consensus and compromise to become a reality.

One key aspect of our ongoing work is the intersection of privacy and security, including how national security and data security should be key drivers in passing a federal law. That was the subject of my Feb. 1 testimony.[1] However, consumers and industry would also directly benefit from a federal law. Notably, some proposals are only targeted toward protecting children's privacy. While protecting children is a laudable goal, we believe that a comprehensive law that protects all Americans regardless of age is critical.

[1] Brandon Pugh and Steven Ward, "House Subcommittee on Innovation, Data, and Commerce Hearing," Feb. 1, 2023. https://www.rstreet.org/commentary/house-subcommittee-on-innovation-data-and-commerce-hearing-overview-featuring-r-streets-brandon-pugh.

Thank you for your consideration of these materials. Please do not hesitate to let me know if I can be a resource to you or any member of the subcommittee.

Respectfully,

Brandon J. Pugh

Brandon Pugh
Policy Director & Senior Fellow
Cybersecurity & Emerging Threats Team
bpugh@rstreet.org

Material Overview:

1. Brandon Pugh, "If the president is genuine on data privacy and security, specifics would help," February 2023.
2. Steven Ward, "Data Privacy and Security Lessons from the Latest Law Enforcement Data Exposure," January 2023.
3. Brandon Pugh, "Readout from a Congressional Data Privacy and Security Briefing," September 2022.
4. Tatyana Bolton et al., "The Path to Reaching Consensus for Federal Data Security and Privacy Legislation," May 2022. – Intro article with three components:
    - 4a. Intro Article
    - 4b. Preemption in Federal Data Security and Privacy Legislation
    - 4c. The Role of the Federal Trade Commission in Federal Data Security and Privacy Legislation
    - 4d. Limiting a Private Right of Action in Federal Data Security and Privacy Legislation

REAL SOLUTIONS

If the president is genuine on data privacy and security, specifics would help.

BY BRANDON PUGH

FEB 8, 2023

ISSUES: CYBERSECURITY POLICY, DATA SECURITY AND DATA PRIVACY

The 2023 State of the Union address brought about mixed results for data privacy followers and for all Americans. On one hand, privacy and data collection got shout-outs, but it was not more than we have already heard from the White House. If the president is genuine about acting on data privacy and security, he must move beyond generic calls for action and offer a concrete position. The president called for bipartisan legislation to stop Big Tech from collecting personal data on kids, a ban on targeted ads to kids and stricter limits on personal data collection. There was no mention of the historic bipartisan privacy legislation introduced last Congress, the American Data Privacy and Protection Act (ADPPA), nothing concrete on how to move forward, and no mention of the data privacy and security risk holistically.

It is helpful to review what the president said in the 2022 State of the Union address to get a fuller picture of his stance. Last year, President Joe Biden essentially called for the same as this year: strengthening privacy protections, banning targeted ads to kids and demanding tech companies to stop collecting personal data on kids. While strengthening privacy protections was mentioned, it was in a section dedicated to kids. There was no call for federal legislation and no direct connection to privacy concerns facing all Americans. The only real difference in the 2023 address was that bipartisan privacy legislation was flagged and all Americans were considered.

Against the 2022 stance, the president's op-ed in the Wall Street Journal, "Republicans and Democrats, Unite Against Big Tech Abuses," became one of the first and loudest statements from the administration on data privacy and security. This shifted the view to risks posed for "ordinary Americans" and highlighted potential issues with data misuse. The direct call for "serious federal protections for Americans' privacy" was a good step, although combining it with a slew of anti-Big-Tech rhetoric and broader controversial tech measures reduced the effectiveness of this call and overshined the privacy focus.

A hopeful sign that the 2023 address might have contained a strong privacy stance was the White House's "Fact Sheet" released before the speech. In that, the president expanded in the greatest detail yet on his desire to "protect kids online" and "strengthen data privacy and platform accountability for all Americans." Specifically, he flagged the data collection risk and the need for strict limits on collection, use and transfer of data.

How, then, do we move forward in 2023?

First, the president should more closely work with Congress to find a solution. In an ideal world, he would support moving the ADPPA forward and help break down challenges experienced in the 117th Congress. For example, we did not see consensus between key leaders in the Senate and House and a California versus the United States trend developed over whether a federal law should override state privacy laws. The support from members of Congress is there, evidenced recently by member comments in a House Energy and Commerce subcommittee hearing and applause for privacy in the State of the Union.

Second, we need to remember that action is not just a matter of helping consumers. While that is important, there are broader benefits. This includes helping industry like small- and medium-sized businesses, advancing America's competitive stance on the global stage and strengthening national security.

Third, we need to move away from the notion that data privacy and security risks are caused solely by Big Tech. Data privacy and security risks do not depend on company size. There are countless examples of small and medium-sized companies, and even large non-tech companies, employing terrible data privacy and security practices involving highly sensitive data. Relatedly, we should keep action on privacy focused on privacy. Adding in other controversial measures, like antitrust, content moderation and Section 230, are sure ways to stall progress. This means acting on legislation that protects the data privacy and security of all Americans, not just kids.

While it is always great to hear data privacy get mentioned by the president, hopefully it appears next year as a bipartisan accomplishment.

Image credit: suebsiri

REAL SOLUTIONS

Data Privacy and Security Lessons from the Latest Law Enforcement Data Exposure

BY STEVEN WARD

JAN 26, 2023

ISSUES: CYBERSECURITY POLICY, DATA SECURITY AND DATA PRIVACY, FEDERAL GOVERNMENT AFFAIRS

When agencies decide to use third-party vendors, they must be aware of any and all potential issues that could arise from the convenience of the service. Recently, a security flaw discovered in SweepWizard, an app developed by ODIN Intelligence to assist law enforcement agencies in managing multi-agency raids, illustrated a prime example of the risks associated with third-party vendors. SweepWizard permitted unauthorized access to sensitive data, including over 1,000 suspects' social security numbers; law enforcement officers' names, phone numbers and email addresses; pre-raid briefing locations; and raid locations. Law enforcement agencies were using a free trial of SweepWizard, which claimed to be Criminal Justice Information Services (CJIS) compliant. Later, unknown hackers claimed to possess 16 gigabytes of data from ODIN Intelligence.

SweepWizard is a kind of intelligence sharing, which refers to the collection and dispersion of sensitive data with agencies and third-party vendors to prevent and solve crime. When an agency shares data with a third-party vendor, it must assess whether that shared data will be secured from non-authorized users, foreign adversaries or malicious cyber actors, like ransomware hackers plotting to exploit security vulnerabilities. But an assessment is not foolproof.

The privacy implications of SweepWizard's data exposure could devastate officers and suspects. Some states provide special protection to law enforcement officers' personal information because disseminating an officer's personal information can have dire consequences. Further, the suspects' names and locations were exposed, which may put people at risk. The suspects could find themselves an internet search away from employment and housing opportunity denial or in the mob justice and vigilantes' crosshairs, like Richard Jewels and Steven Hatfill.

There are operational implications to consider, too. Raids are most successful when each suspect's residence is raided simultaneously to prevent the raid details from being leaked. If revealed, officer safety and evidence are severely compromised, and the opportunity to secure incriminating evidence for current or future investigations vanishes. Potential investigative leads vanishing could have devastating consequences, and crime victims will bear that cost. In online child sexual exploitation cases, for example, one suspect can help bring down an entire criminal organization dedicated to exploiting children. An investigator can assume a suspect's vetted online identity and infiltrate exclusive groups and organizations, which might otherwise be impossible to access.

The Need for a Comprehensive Data Privacy Law

To safeguard public trust and community safety, agencies must apply data privacy and security protection principles to data collected and shared with other agencies or third-party vendors. Generally, there are law enforcement and/or government exceptions from most comprehensive privacy laws. However, agencies must comply with the Federal Bureau of Investigation's (FBI) CJIS Security Policy if accessing the FBI's CJIS databases, like fingerprint identification data. The CJIS Security Policy guides law enforcement agencies nationwide to secure and protect criminal justice information from unauthorized access, dissemination and transmission. However, CJIS compliance—even when subject to audits—can fail. That is why we need a comprehensive federal data privacy and security law that third-party vendors must adhere to.

A comprehensive federal data privacy and security law, like the American Data Privacy and Protection Act (ADPPA) proposed in the 117th Congress, is one of the best ways that we can secure our data. In 2022, the ADPPA made significant progress, but ultimately stalled out. Many privacy professionals and groups supported the comprehensive bipartisan privacy bill. It would have brought stability to the legal privacy landscape currently hampered by state-by-state privacy patchwork laws. Multiple provisions in the ADPPA could help prevent breaches like the one that SweepWizard experienced. For example, Section 208 of the ADPPA requires non-exempt entities to implement and maintain security measures adequately to protect data against unauthorized access and acquisition. Section 208 also provides specific requirements that certain entities must meet, including security system vulnerabilities, taking preventive and corrective action, evaluating their systems, retention and disposal schedule, training and an organization's incident response.

In addition, a fundamental privacy principle conveyed in ADPPA was data minimization, which limits what data an entity may collect, process or transfer. This helps limit the amount of data collected in the first place. Another ADPPA strength was its inclusion of essential privacy principles, like a data retention and disposal schedule that requires "…. the deletion of covered data when such data is required to be deleted by law or is no longer necessary…." While some privacy frameworks touch on data minimization, the ADPPA expanded data minimization with specific and detailed restrictions.

In the SweepWizard data breach, several police investigations from as far back as 2011 were accessed without authorization. Whether that data needed to be retained is unknown—but it seems unlikely. Decade-old multi-agency raid data holds minimal value and should have been deleted from the SweepWizard's database.

Passing a comprehensive federal privacy and security law and demanding better privacy and security policies from law enforcement agencies will improve community trust and safety. Only then can we work together to secure our data from those who wish to do us harm.

Image credit: Rawpixel.com

ANALYSIS

Readout from a Congressional Data Privacy and Security Briefing

BY BRANDON PUGH

SEPT 26, 2022

ISSUES: CYBERSECURITY, CYBERSECURITY POLICY, DATA SECURITY AND DATA PRIVACY, FEDERAL GOVERNMENT AFFAIRS

On Sept. 21, 2022, R Street's Cyber team, in partnership with Public Knowledge and The Leadership Conference on Civil and Human Rights, hosted a briefing geared toward Hill staffers on data privacy and security legislation. The briefing focused on the American Data Privacy and Protection Act (ADPPA), which was released by the House Energy and Commerce Committee in July by a 53-2 vote. We sought to provide an overview on the legislation, explore specific aspects and highlight the broader need for action.

House Energy and Commerce Chairman Rep. Frank Pallone (D-N.J.), one of the main sponsors of the ADPPA, opened the program with introductory remarks. He emphasized several provisions in the bill, including additional protections for consumers and children. He also highlighted the legislation's bipartisan backing and movement on key areas that have been obstacles in the past.

The briefing featured a panel of diverse experts, including Brandon Pugh of the R Street Institute, Paul Lekas of the Software & Information Industry Association (SIIA), Sara Collins of Public Knowledge and Yosef Getachew of Common Cause. The panel was moderated by Lauren Zabierek of the Harvard Kennedy School's Belfer Center, who helped lead an earlier effort at reaching consensus on privacy legislation.

Highlights are shared below.

Reasons to Support the ADPPA

Each panelist began by sharing reasons their organization supports the ADPPA and highlighting the need for data privacy and security legislation more broadly. While there was some overlap, each speaker raised a different aspect. These reasons included ensuring the United States remains competitive on the global stage; providing rules of the road for how data can be used and shared; increasing protections for marginalized communities; allowing Congress to act on privacy policy questions instead of federal agencies; and increasing national security and data security.

Discussions also touched on the current landscape of privacy legislation, which includes laws in five states, federal laws in different sectors like health and finance, and international frameworks, among others. Some panelists conveyed that this structure supports legislative action itself because it leaves a gap in protections for individuals and leads to a patchwork of laws that impacts businesses.

The Necessity of Compromise for the ADPPA

Panelists shared historical efforts at passing legislation along with traditional points of contention like a private right of action, preemption and the role of the Federal Trade Commission (FTC) in rulemaking and enforcement. Some highlighted the important role of compromise in the ADPPA since some members of Congress and external groups have moved on specific areas in the spirit of passing a federal law. For instance, some traditionally opposed to broad preemption are supportive of a bill with it because other parts were included, like a private right of action, and vice versa. However, support for the bill does not revolve solely around these key areas because the substance and fundamental provisions are still important.

An attendee raised California's concerns with preemption, especially as House Speaker Nancy Pelosi (D-Calif.) said work is needed to address outstanding concerns. Panelists' responses to this included reflecting on the changes to the ADPPA to account for the California Privacy Protection Agency; providing a role in enforcement for states; the ADPPA being stronger in multiple areas like civil rights; and providing rights for all Americans.

Possible Adjustments to the ADPPA

While panelists all expressed support for the progress so far, each shared ways the ADPPA can be fine-tuned, and not all agreed with each change mentioned. Some suggestions included clarifying the distinction between Federal Communications Commission (FCC) and FTC in privacy enforcement; revising the applicability and scope of algorithmic impact assessments; tailoring specific definitions for algorithms and sensitive covered data categories; ensuring the ability to use publicly available information in the public interest; and revisiting the applicability of sections to some entities like nonprofits and small businesses. Even broader changes are possible, but they could impact the delicate attempt at consensus.

Panelists explored a variety of other questions, such as how provisions apply to communities of color and the benefits and challenges with the provisions surrounding children.

Overall, the panel showed how groups with different ideologies and constituencies are coming together in the spirit of compromise to help make data privacy and security legislation a reality given the overarching need for action. The ADPPA still has barriers ahead, like the timing of the election and some outstanding concerns, but it is the most significant step in the U.S. privacy journey thus far.

REAL SOLUTIONS

The Path to Reaching Consensus for Federal Data Security and Privacy Legislation

BY TATYANA BOLTON, BRANDON PUGH, SOFIA LESMES, LAUREN ZABIEREK, CORY SIMPSON

ISSUES: CYBERSECURITY POLICY, DATA SECURITY AND DATA PRIVACY

MAY 26, 2022

This is a joint project between the R Street Institute's Cyber Team, led by Tatyana Bolton, the Belfer Center's Cyber Project, led by Lauren Zabierek, and Cory Simpson, a senior advisor on the Cyberspace Solarium Commission.

Data privacy is one of the nation's most pressing issues. The current lack of federal privacy legislation affects the economy, national security and consumer safety and is—at its most basic level—not a controversial issue for most Americans. Multiple leaders of top-tier tech companies have, in recent weeks, called for privacy legislation. The major bills on the table are mostly aligned. Where they differ, however, and where Congress must find consensus, is on the most contentious issues: preemption, private right of action (PRA) and the role of the Federal Trade Commission (FTC). Our goal in developing this series is to offer recommendations on the best way to find agreement on these key issues.

The United States is one of the industrialized countries that lacks a single, national data privacy law, which affects our global competitiveness. In the vacuum left by the lack of federal government progress, state laws are passing quickly. But this isn't the best path forward. Studies have shown that a patchwork of state privacy laws could cost the United States over $1 trillion in out-of-state costs over 10 years. In addition, this patchy landscape would be difficult for businesses to navigate, especially small and medium companies.

Moreover, many countries want to take our data and weaponize it. For example, China—the most significant of these threats—is working to overtake the United States in the technology sector and is actively using our weak cybersecurity and data privacy protections to gather our data and use it against us. This can have many consequences, from blackmailing U.S.-based critics to identifying intelligence agents. Thus, the United States stands to gain significant competitive and national security advantages if our companies keep data private and secure.

The majority of Americans want data privacy regulation. Without a federal standard, consumers are left with unequal protections, or none at all.

We have drafted three articles, each of which focuses on one of the main areas of federal privacy law debate, identifies a variety of options for consensus and offers initial recommendations for compromise.

Our articles on preemption, PRA and the role of the FTC are intentionally framed differently than standard academic and think tank products. Our goal is to provide key members who are debating privacy legislation with a guide to the most challenging issues national legislation has faced, offering succinct options for bipartisan consensus. Although we present these topics separately, we recognize that these issues overlap, and progress toward consensus on one may mean a tradeoff on another.

Our work, which is the result of over 130 engagements across a full range of stakeholders, including Congress, the private sector, consumer groups and privacy advocates, builds off of the efforts of other experts, such as the Brookings Institution, Privacy for America and Duke University. Varied perspectives—even if conflicting—were crucial to understanding what an effective, passable bill could look like.

A federal data security and privacy law has never been more necessary, and we are closer to realizing that goal than ever before. For the sake of our economy, national security and consumer rights, the United States must act now rather than continue to hold out for the perfect law.

PART 1 – Preemption in Federal Data Security and Privacy Legislation

PART 2 – The Role of the Federal Trade Commission in Federal Data Security and Privacy Legislation

PART 3 – Limiting a Private Right of Action in Federal Data Security and Privacy Legislation

EXPLAINER – Answer to Tough Questions: The Framework of a Federal Data Security and Privacy Law

REAL SOLUTIONS

Preemption in Federal Data Security and Privacy Legislation

BY TATYANA BOLTON, BRANDON PUGH, SOFIA LESMES, LAUREN ZABIEREK, CORY SIMPSON

ISSUES: CYBERSECURITY POLICY, DATA SECURITY AND DATA PRIVACY

MAY 31, 2022

Preemption is the ability of the federal government to overrule or replace state law in favor of federal law. It is rooted in the U.S. Constitution's Supremacy Clause, and it remains a central challenge in passing federal data security and privacy legislation.

Five U.S. states have passed comprehensive data privacy laws. In 2021, at least 25 states introduced comprehensive legislation, along with even more that introduced less-comprehensive legislation to address specific privacy issues. In fact, in the span of time it took us to write this article, the United States went from three to five states with comprehensive data privacy laws. State laws could all be affected by a preemptive federal law, so determining whether and how existing and future state laws should operate with federal law is an essential part of developing federal privacy legislation.

This has fueled a debate on whether federal privacy legislation should allow for stronger state privacy frameworks or whether it should prevent states from having their own frameworks at all. On one side of the debate, a federal law could set minimum requirements and allow states to make new or stricter laws. Proponents of this approach believe that states are best suited to account for their unique needs and to innovate. On the other side, a federal law could displace state frameworks and serve as the uniform standard, with or without carve-outs for state action and existing federal law. Proponents of this strong preemption approach assert that it would end the current patchwork of laws that have led to inconsistent protections for consumers and avoid the industry-related compliance challenges that would come with meeting the requirements of 50+ frameworks.

Fortunately, the preemption debate does not need to be resolved by taking one side or the other. The solution exists along a spectrum, depending on how much Congress wants to allow state laws to complement federal law. A balance can be achieved by having a uniform federal privacy law that can preempt states on substantive provisions covered at the federal level but also preserve existing privacy-related federal frameworks and carve out areas for traditional state authority and emerging areas.

This publication—the first in a series of three main articles—explores the various forms preemption can take and provides recommendations to reach consensus among these options. For more, read our explainer about tough questions and answers here.

CONSIDERATIONS AND OPTIONS

Consideration #1: Preemption and Savings Clauses

Preemption allows federal law to overrule or replace state law in a field or topic, but a savings clause, which is referred to as a carve-out for simplicity, can be added to prevent certain areas of state law from being preempted. Such a clause determines how federal law interplays with state law. Of note, preemption and savings clauses often arise with regard to federal legislation so they are not unique to privacy legislation. In certain situations, preemption is impermissible and considered commandeering (e.g., *Murphy v. NCAA*). Congress should be aware of these limitations as they craft preemption for privacy legislation.

Consideration #2: Carve-Outs for State Action

At least 10 areas could be considered for carve-outs in federal privacy legislation to keep existing state law intact, and statutory language should address how carve-outs involving covered data are handled. Doing so would result in uniform legislation while allowing states to retain control over certain areas. The areas that should be considered for carve-outs broadly fall into two categories: areas of traditional state control and emerging areas/gap-fillers.

Areas of traditional state control to consider include, but are not limited to:

- **Civil Rights Laws**—Establishing carve-outs for these laws helps avoid canceling protections in states with more robust civil rights laws. If a federal data privacy law contains a civil rights clause, it may address some of these restrictions, but states still may provide additional protections.

- **State Statutes Surrounding Unfair and Deceptive Acts and Practices**—Every state has a consumer protection law that prohibits deceptive practices, and many others prohibit unfair or unconscionable practices. The effectiveness, strength and applicability of these laws vary widely across the country.

- **State Constitutional Law**—States may offer their denizens additional rights under their state constitution that are not offered at the federal level.

- **State Laws Relating to Tort, Contract and Property in Statute or Common Law**—These areas have evolved at the state level over time and often reflect a state view.

- **State Criminal Law**—All 50 states have computer crime laws of varying scope, from unauthorized access to targeting specific types of crime.

- **Laws Governing Specific Relationships**—Common examples in state statute include landlord-tenant, employer-employee relationships, library patrons and student privacy.

- **State Laws Pertaining to Government Activities**—States often regulate state government agencies or state government employee actions relating to privacy, including prohibiting or permitting certain actions. For example, a state may regulate the collection and preservation of public records.

Emerging areas and gap-fillers to consider include, but are not limited to:

- **State Cybersecurity Laws**—Some states have laws that require businesses to follow rules related to encryption, data breaches, incident reporting, ransomware and other cybersecurity practices that could go further than the provisions in a federal data privacy bill.

- **State Versions of Federal Laws That Allow for Stronger Provisions**—Multiple federal privacy laws do not preempt stricter privacy protections at the state level like the Health Insurance Portability and Accountability Act (HIPAA) and the Cable Communications Policy Act of 1984, among others. In fact, some federal laws preempt "contrary" state laws but include an exception for state laws providing greater protections.

- **State Laws Governing an Area the Federal Law Does Not Address or Contemplate**—Federal privacy legislation is unlikely to account for certain

privacy concerns unique to certain states, so states should retain the ability to legislate in these areas to avoid gaps, such as anti-paparazzi laws and audio recordings between parties.

- **Biometrics**—This area requires special consideration because aspects such as definitions, collection versus use and enforcement mechanisms are still widely debated. While some bills do contain biometric definitions and provisions already, and one state—Illinois—has passed a law governing this particular data, this hotly debated topic should be considered outside of existing debates on comprehensive data security data privacy legislation.

Consideration #3: Carve-Outs for Existing Federal Laws

Multiple pieces of current, privacy-related federal law could be explicitly carved out so they are not modified by a new law. Statutory language should address how data is treated when it may be subject to a sectoral privacy law and a comprehensive privacy law, including whether compliance with a sectoral law satisfies requirements set by a new comprehensive law. Existing privacy-related federal laws already have regulatory frameworks in place, and any changes should be addressed through different legislation or amendments to the original statute. These broadly fall into six categories, including but not limited to:

- **Student Privacy**—Family Educational Rights and Privacy Act (FERPA)
- **Health Privacy**—HIPAA and Health Information Technology Economic and Clinical Health (HITECH) Act
- **Financial Privacy**—Gramm-Leach-Bliley Act (GLBA), Fair Debt Collection Practices Act (FDCPA) and Fair Credit Reporting Act (FCRA)
- **Children's Privacy**—Children's Online Privacy Protection Act (COPPA)

- **Federal Government Practices**—Privacy Act of 1974 and E-Government Act of 2002

- **Other Laws**—Communications Assistance for Law Enforcement Act (CALEA), Communications Act of 1934, Electronic Communications Privacy Act (ECPA), Driver's Privacy Protection Act of 1994, Controlling Assault of Non-Solicited Pornography and Marketing Act, Restore Online Shoppers' Confidence Act, part C of title XI of the Social Security Act, Telemarketing and Consumer Fraud and Abuse Prevention Act, Telephone Consumer Protection Act, Genetic Information Nondiscrimination Act and Federal Aviation Act of 1958

Consideration #4: Other Aspects: The scope of preemption is important, but there are other aspects to consider when including preemption language. These include:

- Language and definitions need clear meaning—Otherwise, uncertainty can be introduced in the laws and regulations, which could lead to litigation and force courts to decide what is and is not preempted or additional agency action may be required. For example, if new legislation has language targeting laws that "directly conflict," a debate could ensue on what falls under that provision. To ensure that clear language and definitions are established, a federal agency like the FTC could be empowered to review cases of preemption as either an advisory body for federal courts or with decision-making authority. In addition, Congress could leave certain provisions open to states or a federal agency like the FTC to define (e.g., the federal law may not establish a uniform age of consent to define minors and teens).

- Grandfather existing state privacy laws—Specific state laws could be grandfathered in or each one enacted prior to federal legislation to allow them to continue despite a new federal law. For example, California's privacy legislation could be allowed to remain in effect, while others are preempted.

- Enforcement by state governments—State attorneys general or other state agencies could be empowered to assist in enforcing federal legislation, including bringing civil actions on behalf of residents of their state and/or investigating violations. This could be helpful in enforcement against largely local bad actors. They already play a role in enforcing other pieces of federal privacy legislation. Specific considerations would need to include whether notification needs to be made to the FTC first, whether the FTC has a right of first refusal, where actions can be brought, and the role of state-level data protection authorities.

RECOMMENDATIONS

Taking these options into consideration, we offer three main recommendations related to preemption in federal data security and privacy legislation: preemption should not be approached as all-or-nothing, rights and provisions of a federal law should be compared to existing and proposed state laws, and state governments should have a role in enforcement.

Recommendation #1: Preemption should not be approached as all-or-nothing.

A federal privacy law should preempt states on substantive provisions covered by the federal law but should also include carve-outs. It is important to prohibit states from making stricter or additional protections, as failure to restrict this action would inevitably result in returning to the existing patchwork of state restrictions. Federal legislation must also be strong enough to provide adequate privacy and security protections to consumers while taking into account the needs of businesses and groups that will be tasked with complying with it.

This allows for a uniform approach for both consumers and industry while protecting areas of state concern through carve-outs. It will prevent entities from having to follow various state frameworks and any subsequent amendments, which would result in large compliance costs, uncertainty on what is needed to comply and the need to monitor all 50 states regularly. A single standard also produces greater trust and ensures that all individuals enjoy the same protections regardless of where they reside or travel.

Specifically, we suggest that federal privacy legislation include:

- **Clear Statutory Language That Explicitly Preempts States from Making Their Own Privacy Laws, but That Includes Carve-Outs for Certain Areas**—This would prevent states from making distinct, inconsistent frameworks. Select carve-outs are important, however, because they respect and uphold the long history of states having control over unique issues that affect their area, they account for areas that are best addressed by having a local approach instead of a national one and they can help fill gaps not covered by federal law.

We recommend carve-outs for areas of traditional state concern (civil rights laws; state statutes surrounding unfair and deceptive acts and practices; state constitutional law; state laws relating to tort, contract, and property in statute or common law; state criminal law; laws governing specific relationships; and state laws pertaining to government activities) and for emerging areas and gap-fillers (state cybersecurity laws, state versions of federal laws that allow for stronger provisions and state laws governing an area the federal law does not address or contemplate; biometrics require special consideration, as highlighted above).

We also recommend that carve-out implementation be considered in statute in the following ways:

- If an issue area has been addressed by federal statute, the statute should preempt any state level law covering the same topic. For example, if biometric provisions are substantively included in a federal law, states should not be able to make additional or stricter standards.

- If state laws regulate the collection, use, maintenance or other handling of covered data addressed by federal legislation, then those provisions of state law should be preempted, even if that state law encompasses a carve-out enumerated above.

- State laws should not be used to litigate claims related to violations of the federal data security and privacy law.

- Actions by states should be monitored to ensure that additional or new protections are not being created under a carve-out, including under unfair and deceptive acts and practices statutes. For example, a new privacy protection could be created by a state as a tort or an unfair and deceptive practice as a way to expand provisions and get around preemption.

- **A Prohibition of Grandfathering Existing State Frameworks or Laws Outside of Those Covered as Carve-Outs**—One or multiple existing state laws, such as California's, should not be singled out and allowed to stand while preempting others. A basic premise of the U.S. legal system and our constitutional framework is that all states are equal. Selective preemption of some states' laws would undermine that concept. Furthermore, allowing some existing frameworks to persist would result in inconsistencies from the outset.

- **Clear Statutory Language That Explicitly Excludes Select Federal Laws from Being Affected**—Certain existing laws have agreed-upon regulatory frameworks that have existed for years. If these current frameworks were affected by a new law, it would result in burdensome compliance actions and costs for companies and would weaken data security by subjecting unique data to a broader law instead of a sector-specific law. Although this means that some entities would have to follow multiple frameworks, the challenges of making changes to existing laws would outweigh the benefits of a single

framework. Therefore, any changes suggested to these existing frameworks should be considered through separate legislation or amendments to their original statute.

The federal carve-outs we recommend excluding from a federal privacy law are 11 of the statutes previously mentioned. They pertain to student privacy, health privacy, financial privacy, children's privacy and other categories. These include FERPA, HIPAA, HITECH Act, GLBA, FCRA, COPPA, CALEA, ECPA, Communications Act of 1934 (except as noted below), Driver's Privacy Protection Act of 1994, and the Federal Aviation Act of 1958. Specifically, data covered by and used in accordance with these existing federal privacy laws should be excluded, but if a covered entity collects data not subject to the other laws, it should follow the provisions in the comprehensive federal legislation for that other data. This will help avoid dual systems for the same data.

Also, we recommend that a data privacy federal law aims to have entities covered by the statute be regulated by only one agency for data privacy and security, rather than multiple. In the area of data security and privacy, specifically, Congress could consider allowing the FTC to solely regulate the area to avoid confusion and duplication with the Federal Communications Commission. Of note, certain provisions of existing statutes currently prevent the FTC from regulating data security and privacy fully, such as those related to common carriers; therefore, existing statues may need to be amended or superseded to allow for this approach.

Recommendation #2: Rights and provisions of a federal law should be compared to existing and proposed state laws.

The substance of a final privacy bill will reflect how the politics surrounding preemption are addressed. For example, advocates of California's privacy framework may be less likely to oppose broader preemption if the rights and structures currently in place are comparable or stronger in a federal law. On the other hand, if federal law offers fewer protections and still preempts state laws, many are likely to see the federal law as a step backward.

This means that preemption is directly related to other areas of disagreement in the privacy debate like a private right of action (PRA), rulemaking authority and enforcement mechanisms. For example, if the FTC has rulemaking authority, there is an increased likelihood of conflict with state laws and regulations in the absence of broader preemption.

Recommendation #3: State governments should have a role in enforcement.

Permitting state attorneys general, consumer protection officials, or other state officials to share in enforcement will amplify enforcement efforts and make sure local concerns are being addressed. States should be able to conduct investigations into violations affecting their state and bring civil suits in federal court. However, the FTC or a designated federal agency should have the right to be heard in any case brought to help ensure consistency and expertise.

In addition, states should be permitted to maintain state-level data protection authorities, like the California Privacy Protection Agency. However, the agencies should not be permitted to take action that is inconsistent with federal legislation or that is exclusively granted to a federal agency. Sample roles could include serving as a subject-matter expert for implementation, addressing previously mentioned carve-outs, training and raising awareness.

About this series: *This is part of a series considering the major stumbling blocks of federal data security and data privacy efforts. It draws upon existing research and interview data to identify the most salient issues within data security and data privacy and recommend the most appropriate courses of action in an effort to find compromise on federal legislation.*

INTRODUCTION – The Path to Reaching Consensus for Federal Data Security and Privacy Legislation

PART 1 – Preemption in Federal Data Security and Privacy Legislation

PART 2 – The Role of the Federal Trade Commission in Federal Data Security and Privacy Legislation

PART 3 – Limiting a Private Right of Action in Federal Data Security and Privacy Legislation

EXPLAINER – Answer to Tough Questions: The Framework of a Federal Data Security and Privacy Law

(Image credit: “The Era of Oversharing (pt.3)” by is licensed under CC BY 4.0)

REAL SOLUTIONS

The Role of the Federal Trade Commission in Federal Data Security and Privacy Legislation

BY TATYANA BOLTON, BRANDON PUGH, SOFIA LESMES, LAUREN ZABIEREK, EXECUTIVE DIRECTOR, CYBER PROJECT AT HARVARD KENNEDY SCHOOL'S BELFER CENTER, CORY SIMPSON, SENIOR ADVISOR, CYBERSPACE SOLARIUM COMMISSION

ISSUES: CYBERSECURITY POLICY, DATA SECURITY AND DATA PRIVACY

MAY 31, 2022

The Federal Trade Commission (FTC) is the nation's primary consumer protection body, and while some have called for a new data protection agency, most believe the FTC should be the body responsible for data security and privacy. Indeed, the FTC already enforces some privacy legislation and seeks to expand on its role in data privacy. As federal data and privacy bills are considered, it is therefore critical that we understand the role the FTC might play in overseeing and enforcing such legislation as well as the important role that lawmakers will have in setting parameters for the FTC.

The issues related to rulemaking and enforcement authority are especially important and complex. Unchecked or overly prescriptive authority risks unwieldy regulation that could harm innovation and business, but too little authority risks insufficient protection from privacy harms and overly rigid protections that cannot adapt to rapidly changing technology. We must work to avoid both ends of this spectrum and, instead, strike a balance that ensures that the FTC is appropriately resourced to deliver on the agency's promise to protect citizens and their data.

As a result of our engagement with stakeholders, we believe the key to striking the right balance lies in "guided FTC rulemaking" in a federal law, echoed by privacy experts and private sector companies alike. With such an approach, Congress would be tasked with establishing clear guardrails and definitions around the type of rulemaking authority the FTC could use, the targeted areas in which that authority could be applied, and the means by which such efforts could be undertaken. Parameters for assessing penalties would also be key in ensuring that the enforcement of violations is carried out in a way that upholds compliance rather than conveying a perception of unguided fining.

This publication—the second in a series of three main articles—explores these issues and provides recommendations for what we consider to be the most reasonable solutions.

CONSIDERATIONS AND OPTIONS

This section addresses the key question and options available to lawmakers in considering the FTC's role in federal privacy legislation. There are four categories of questions:

- What type of rulemaking authority should the FTC be given and under which laws should that authority be granted?

- For which aspects of a data security and privacy law should the FTC be granted targeted rulemaking authority?

- How will the FTC handle the enforcement of federal privacy legislation (e.g., assessing violations, determining whether a warning is warranted, determining fines) and should the FTC provide regular guidance to companies beyond enforcement?

- How should these efforts be funded and organized (e.g., budget amount, personnel needed, phased funding, new FTC bureau)?

Below, we explore these considerations and options, bringing together our assessments of four major federal privacy bills (two Democratic, two Republican), interviews with stakeholders, and a review of existing research.

Consideration #1: Current Authorities Under Which the FTC Can Operate

The FTC is the nation's consumer protection body and it generally operates under the FTC Act and additional rules that it promulgates pursuant to the Magnuson-Moss Warranty Act (MMWA) of 1975. This differs from other federal agencies in that the Administrative Procedures Act (APA) is more commonly the primary rulemaking authority.

Although Section 18 of the FTC Act authorizes the Commission to create rules specifying and governing unfair and deceptive acts or practices (currently the Commission's key tool for addressing data privacy and security), MMWA rulemaking requires a much more lengthy and cumbersome process (to include publishing an Advanced Notice of Proposed Rulemaking, publishing a Notice of Proposed Rulemaking for public comment, holding informal hearings, publishing the final rule, and—after all of this—any person may seek judicial review within 60 days), which is largely why the authority has rarely been used since its inception in 1975.

The APA is the standard authority granted to most federal agencies to create, amend, or appeal rules. The authority, which is known as "notice and comment," requires agencies to publish a notice of proposed rulemaking in the federal register and provide ample time for public comment, among other requirements. APA authority must be specifically granted to the FTC by Congress in legislation; currently, the FTC has been directed to use this authority for specific laws, such as the Children's Online Privacy Protection Act (COPPA) and the Telemarketing and Consumer Fraud and Abuse Prevention Act. According to the U.S. Chamber of Commerce, rules promulgated under APA authority on average took less than a year to adopt versus five years for those under MMWA.

To address the lengthy rulemaking procedures of MMWA, the FTC recently worked to streamline the process; however, it must be noted that, despite the changes (including as the Commissioner's statement notes: "providing the Commission with greater accountability and control over Section 18 rulemaking, deciding the final list of disputed material facts to be resolved, deciding who will make oral presentations to the Commission and who will cross examine or present rebuttals submissions"), the requirements are still difficult to meet and may not eliminate many of the obstacles that held up previous attempts at rulemaking under the authority. However, the FTC has stated that it intends to use these updated procedures in new rulemakings on privacy issues—an approach encouraged by the Biden Administration to address privacy and security because Congress has not yet been able to. This has drawn concern with regard to the lack of oversight and the agency's capacity to enforce such rules.

Consideration #2: Areas for Rulemaking

Under the current MMWA rulemaking procedures, the FTC is theoretically free (notwithstanding its resource limitations) to create multiple rules to address "unfair and deceptive practices." In its Statement on Regulatory Priorities, the Commission indicated that it intends to create, among other areas, rules to curb lax security practices, limit surveillance abuses and ensure that algorithmic decision-making does not result in unlawful discrimination. This has caused some concern among stakeholders across the spectrum. On one end, companies fear unchecked rulemaking and enforcement; on the other, advocates fear the inability to oversee and enforce these rules broadly.

Four of the main legislative proposals—Sen. Maria Cantwell's (D-Wash.) Consumer Online Privacy Act (COPRA), Sen. Roger Wicker's (R-Miss.) SAFE Data Act, Sen. Sherrod Brown's (D-Ohio) DATA 2020 (which would create a Data Accountability and Transparency Agency rather than place principal enforcement and rulemaking authority with the FTC) and Sen. Jerry Moran's (R-Kan.) Consumer Data Privacy and Security Act (CDPSA)—have collectively identified the following areas for FTC rulemaking:

- Determining which data elements qualify for enhanced protections under the term "sensitive covered data" (COPRA, SAFE Data Act and CDPSA)
- Designating approved processes for covered entities to implement to allow individuals to opt out of transfers of covered data (COPRA)
- Identifying circumstances that would require organizations to obtain individuals' explicit consent for processing personal data (CDPSA and SAFE Data Act)
- Setting requirements for covered entities to adequately respond to individuals' rights requests in a timely fashion, including requests to access, correct and delete personal data (CDPSA)
- Establishing regulations for biometric data (COPRA)
- Identifying unlawful, unfair, deceptive or abusive acts or practices in connection with the collection, use or sharing of personal data (under a new data protection agency; DATA 2020)
- Identifying processes (in consultation with the National Institute of Standards and Technology [NIST]) for receiving and assessing information regarding vulnerabilities to the security of covered data that are reported to the covered entity (SAFE Data Act)

Consideration #3: Enforcement

The FTC's role in the enforcement of the law and subsequent rules is also important to navigate smoothly. Legislation from both sides of the aisle generally aligns on the scope of FTC enforcement: With the exception of Brown's DATA 2020 Act (which calls for an entirely new agency), each of the four main bills described above provides that a violation of the privacy law (or a regulation promulgated under the privacy law) "shall be treated as a violation of a rule." These provisions would allow the agency to seek monetary relief "to redress injury to consumers," including refunds, damages and "public notification respecting the" underlying violation. Such authority would supplement—not replace—other FTC enforcement mechanisms, including penalty authority.

Here, we present the most controversial and intractable issues of FTC enforcement: the collection of penalties and associated frameworks, the right to cure, the role of state attorneys general and how fines would be used.

- **Collection of penalties**—As with the other provisions described in this document, the aim of robust enforcement is compliance and protection, not lawsuits and collection of penalties. If left undefined, the parameters of first-time fining authority could be viewed as controversial by businesses, resulting in overly burdensome fines on well-meaning companies on one end and insufficient mechanisms for halting egregious and continuing harms on the other.

Each of the four main bills grants the FTC (or another future data protection agency) the authority to collect civil penalties in violation of the law (or rules promulgated under the law) and to treat violations as unfair and deceptive practices under the FTC Act. Historically, business groups have balked at this, claiming that the FTC has failed to provide specific, detailed guidance on what is deemed "unfair and deceptive."

The CDPSA is more prescriptive in the authority it would grant the FTC; it limits penalties per violation "up to $42,530 multiplied by the number of individuals affected" and designates a number of considerations for the FTC in determining penalties, such as the degree of harm; intent in committing the violation; size, complexity and resources of a covered entity; reasonable expectations; degree of compliance; self-reporting; and steps taken to address the violation. This is similar to how COPPA determines its penalties but differs from the current enforcement of unfair and deceptive practices for general privacy violations. However, it must be noted that many experts have commented on the difficulty of translating privacy harms into quantitative amounts.

Although the CDPSA is more specific in outlining how the FTC may seek penalties, it does not determine where penalties would go or how they would be used. The other main bills identify the creation of a victims' relief fund, which the Commission could draw from to issue payments to victims of harmful data practices. Some have stated that the funds should be deposited into the general U.S. Treasury and be usable by the federal government for general public good. Others have suggested that the funds not only go toward victims' relief but also toward helping small and medium businesses bolster their data privacy and security compliance. We present the following options:

- Penalties obtained by the FTC and the attorney general could be deposited into a Data Privacy and Security Victims' Relief Fund which would provide redress, payments or compensation, or other monetary relief to individuals.

- Funds could also be used "for the purpose of consumer or business education relating to data privacy and security or for the purpose of engaging in technological research that the Commission considers necessary to enforce."

- Funds could also be used to help with data privacy and security compliance for small- and medium-sized businesses, especially in the early years of the

law, and could be shared with the Cybersecurity and Infrastructure Security Agency (CISA) to assist with their outreach and services.

Consideration #4: Capacity

Most stakeholders agree that the FTC is not appropriately resourced (in either staff or budget) to regulate or enforce privacy. The Commission's current annual budget is approximately $351 million, but in its privacy mission, it employs 61 people at $13 million. For context, the United Kingdom's Information Commissioner's Office has a budget of approximately $90 million with 822 permanent staff, and Ireland's Data Protection Commission has a budget of approximately $18 million with 138 permanent staff. Both countries have more data privacy officers than the United States but have significantly fewer citizens to protect. The U.S.'s capacity to address data security and privacy is out of sync with the degree of potential harms and threats.

In a letter written to Representative Frank Pallone (D-N.J.) in 2019, then-FTC Commissioner Joe Simons laid out what he could do with additional funding: With $50 million of funding per year, the FTC could hire and retain 160 more staff members; with $75 million, the FTC could hire and retain 260 more staff members; and with $100 million, the FTC could hire and retain 360 more staff members. Those staff members would join the 40 current (at that time) staff members in the Division of Privacy and Identity Protection, expanding the Commission's capacity to bring approximately 20 cases per year to 180 cases per year and enabling the agency to enforce not only any future federal data privacy and security law but also COPPA and the Fair Credit Reporting Act. Simons also estimated that he would need an additional 10 to 15 technologists to join the 5 on staff at that time and cited the need for additional infrastructure, such as office space.

Although the major federal bills (with the exception of DATA 2020, which argues for the creation of a new data protection agency) designate the FTC as the enforcement body and note that the FTC is currently under-resourced, they differ on the approaches they recommend to bolster those resources. The CDSPA grants the FTC the ability to grow to 440 personnel but doesn't authorize specific funding to get there (though it does note the need for additional experts like technologists). The CDPA also directs the FTC in its regulation and enforcement authority but designates no specifics for its growth in funding or personnel. COPRA directs the creation of a new FTC bureau but leaves out specifics on budgetary and personnel needs. Of note, the Build Back Better (BBB) infrastructure bill also proposed $500 million over seven years for the development and growth of a new FTC bureau to enhance its ability to work on data privacy and security matters.

RECOMMENDATIONS

After assessing the many considerations and options for the role of the FTC above, below we list our recommendations and rationales. Of note, we do not recommend safe harbor provisions or the right to cure. Our goal is to strike a balance between ensuring safety for the consumer; preserving the ability to innovate and deliver services to businesses; and protecting our national security. We acknowledge that we cannot satisfy every stakeholder's wish, but we have taken key interests into account and offer below what we believe to be the most prudent courses of action.

Recommendation #1: Authority—A federal privacy bill should grant the FTC targeted rulemaking authority under Section 5, Administrative Procedure Act.

A bill should grant authority under Section 5 of the Administrative Procedure Act. Targeted rulemaking under the APA allows Congress to provide necessary oversight while not slowing the process—thus allowing the FTC to be agile and responsive to changing technological conditions and privacy harms. We recommend the following additional considerations:

- As a prerequisite to rulemaking, the FTC must demonstrate any harm brought about by new technology and business models.
- The law should specify ample time for stakeholders to comment (no less than 90 days).

Recommendation #2: Targeted Rulemaking Areas—Rules must be made clear with limited interpretation left to organizations.

It is impossible to enumerate all the areas for which the FTC should create rules without having a bill—or a crystal ball—to consult. But the point of rulemaking is to ensure that the law can keep up with evolving technology, business models and the harms that develop with them. Therefore, targeted rulemaking means that the FTC should be allowed to update regulatory provisions as defined by Congress that it has deemed inadequate to address the new harms brought about by technological change, but the agency must clearly demonstrate the need to do so through its rulemaking procedures. As such, a federal privacy law must determine the standard for proof of harm. Furthermore, to ensure the best enforcement of data security, the FTC should be directed to work in coordination and consultation with the relevant security agencies (e.g., CISA, NIST, Office of the National Cyber Director).

Recommendation #3: Enforcement—The aim of a federal law should be for broad compliance and increased consumer data security and privacy, not to collect fines.

To move toward improvements and ensure a balanced bill, Congress should designate the FTC as the primary federal enforcer and allow state attorneys general to bring suit on behalf of that state's constituents—but not in parallel. Congress should also grant the FTC and state attorneys general the authority to collect civil penalties for violations of a data privacy and security law and rules promulgated as part of that law. However, the following conditions should be met:

- Congress should give covered entities two years to comply with the basic provisions laid out in legislation once the law is signed before the FTC is authorized to enforce it.

- Clear penalty criteria and explanatory framework should be developed based on the type of covered entity, the intent and actions to correct, and the measure of harm as defined by Congress (such as how Sen. Moran's CDPSA bill does).

As a matter of practice to ensure broad compliance, the FTC should use warning and remediation letters and should issue and update best-practice guidance regularly. Specific recommended tactics include:

- Warning letters describing violations and steps for remediation should be issued to covered entities when needed.

- Congress should require the FTC to release regular and specific guidance around the law and subsequent rules to help covered entities understand and

comply, especially small and medium businesses and nonprofits with limited means.

- Fines should go into a victims' relief fund mirroring COPRA and CDPA and a data privacy and security fund (a split that Congress should determine).

Recommendation #4: Capacity—The FTC needs staffing and budget increases to be fully effective.

Continuing with the status quo will result in little-to-no increase in resources for the FTC to carry out its duties, especially if federal privacy legislation is passed. Failure to provide more resources to the FTC would hamstring its ability to protect consumers by limiting its capacity to investigate suspected or alleged violations and enforce rules.

Therefore, Congress should allocate an additional $500 million for a new FTC Bureau of Data Security and Privacy, allowing it to grow to 360 personnel over the next five years, which is in line with former FTC Commissioner Joe Simons' recommendations. We also recommend an additional $100 million for capital infrastructure and technology upgrades. It's worth noting the need to focus on hiring diverse staff to address the varied nature of privacy threats and harms. Therefore, we recommend that bills require the hiring of technologists, privacy experts and other experts from varying fields to appropriately identify harms and ways to combat them. Although different stakeholders are advocating for both lower and higher resource and staff allotments for FTC privacy functions, our recommendation reflects the middle ground in the debate.

About this series: *This is part of a series considering the major stumbling blocks of federal data security and data privacy efforts. It draws upon existing research and interview data to identify the most salient issues within data security and data privacy and recommend the most appropriate courses of action in an effort to find compromise on federal legislation.*

INTRODUCTION – The Path to Reaching Consensus for Federal Data Security and Privacy Legislation

PART 1 – Preemption in Federal Data Security and Privacy Legislation

PART 2 – The Role of the Federal Trade Commission in Federal Data Security and Privacy Legislation

PART 3 – Limiting a Private Right of Action in Federal Data Security and Privacy Legislation

EXPLAINER – Answer to Tough Questions: The Framework of a Federal Data Security and Privacy Law

REAL SOLUTIONS

Limiting a Private Right of Action in Federal Data Security and Privacy Legislation

BY TATYANA BOLTON, BRANDON PUGH, SOFIA LESMES, LAUREN ZABIEREK, EXECUTIVE DIRECTOR, CYBER PROJECT AT HARVARD KENNEDY SCHOOL'S BELFER CENTER, CORY SIMPSON, SENIOR ADVISOR, CYBERSPACE SOLARIUM COMMISSION

ISSUES: CYBERSECURITY POLICY, DATA SECURITY AND DATA PRIVACY

JUNE 7, 2022

Enforcing national data security and privacy legislation presents challenges in both scope and scale. Congress's decision regarding who they choose to empower—be it individuals, state attorneys general, one or more federal agencies, or a combination thereof—will dictate the true shape of the law, once passed. If individuals are empowered with an enforcement role—that is, if a private right of action (PRA) is established—it is important to outline the structure, procedures and limits to craft a fair and functional law.

But reaching a consensus on whether federal data security and privacy legislation should even include a PRA has been particularly challenging. Many advocates of a PRA see it as a necessary component to a meaningful enforcement regime, as a properly drafted PRA could fulfill at least three strategic goals: empowering consumers to advocate for themselves, incentivizing the compliance of covered entities and allowing consumers to be made whole for damages—a supplement to potential Federal Trade Commission (FTC) authority to order monetary relief or impose fines. On the other hand, opponents warn that a PRA in federal data security and privacy legislation would likely result in widespread litigation, including frivolous lawsuits and overly broad legal exposure for the private sector. These skeptics believe enforcement by a federal agency or by a combination of a federal agency and state attorneys general would result in a more effective, cohesive and predictable enforcement regime.

In deciding whether to create a PRA, Congress must balance the diverse priorities and perspectives of different stakeholders. It must consider industry and consumer concerns, the adequacy of remedies, the role of states, and regulatory capability and capacity. While a PRA has its drawbacks, the consensus position that takes these issues into account has settled around a limited PRA as a backstop against shifting political winds and executive branch control over privacy enforcement. Just as in other areas, however, Congress should avoid an all-or-nothing approach in striking this balance, taking into account the role of enforcement by the FTC and state attorneys general under state laws and any new federal privacy law. In addition, if Congress chooses to create a PRA, it should empower everyday Americans to assist in the enforcement of the new law in a clear, confined and meaningful way that protects both the American consumer and innovation.

This publication—the last in a series of three main articles—explores the various considerations and options for structuring such an enforcement mechanism and then presents our key recommendations for reaching a consensus.

CONSIDERATIONS AND OPTIONS

Consideration #1: Applicability of a PRA

A PRA could either apply broadly in statute or exclusively to specific provisions. The broadest approach would allow a PRA for any individual alleging a violation of the federal law or regulation to be brought in either state or federal court. This could permit suits for violations of all provisions from a right to access to data breaches. However, a PRA could be limited to apply to specific violations of the statute like a data breach. For example, California's privacy legislation permits a PRA only in the case of a data breach, whereas other enforcement mechanisms permit broader action (e.g., the state attorney general is empowered to address all violations of the statute).

Consideration #2: Consumer Standing

The Constitution requires that individuals have "standing" in order to bring a civil suit. This means they must have suffered a real and individualized harm to bring a successful lawsuit. Demonstrating such harm as a result of privacy violations can be challenging because the harm may not be direct or apparent and would therefore present a constitutional standing challenge. This challenge would be exacerbated by the fact that traditional legal concepts are hard to apply to the digital world.

Indeed, in Spokeo, Inc. v. Robins, the U.S. Supreme Court held that demonstrating a violation of the statute alone, without showing a real and individualized harm, is insufficient to meet the constitutional standing requirement. Of note, there is one prominent instance in privacy law in which individuals can bring suit without alleging harm beyond a violation of their rights under the statute; it is in the case of one particular type of data (biometrical) in one specific state (Illinois).

In determining whether an individual has standing, courts are required to look to traditional harms for comparisons, like those caused by defamation and theft. The Court noted in Spokeo that Congress can play a role in assisting the courts by clarifying the harm in privacy violations that may give an individual standing. Subsequently, in TransUnion LLC v. Ramirez, the Court underscored that "Congress's creation of a statutory prohibition or obligation…does not relieve courts of their responsibility to independently decide whether a plaintiff has suffered a concrete harm…any more than, for example, Congress's enactment of a law regulating speech relieves courts of their responsibility to independently decide whether the law violates the First Amendment."

Concrete harm appears to be a constitutional standing requirement, and the court has continued to look to traditional harms when determining whether a harm has occurred in a particular case. The Spokeo and TransUnion holdings create uncertainty in terms of the harms that may be sufficient to give an individual standing to bring suit for privacy violations. Future court decisions to clarify this issue are necessary and likely. While this area of the law develops, Congress could articulate a harm in statute, specifically considering the violations the harm would apply to, what traditional harms would be similar, and what alternative enforcement mechanisms would exist if standing were inadequate. Thankfully, legislative bodies and academic institutions across the country have identified practical frameworks under which privacy harms can be better understood.

Some of these frameworks have attempted to articulate what harms should be legally cognizable (i.e., sufficient) to provide an individual standing to bring suit. Recent literature categorizes the harms into seven areas: physical, economic, reputational, psychological, autonomy, discrimination and relationship. Some of these have a clear basis in existing law and might help future courts consider harm in the privacy context.

Other frameworks see a duty of loyalty as being a solution to standing issues, where entities should act in the best interest of those who expose their data, and the integrity of the relationship guides the duties. A breach of a duty of loyalty is the injury itself and has long been recognized by courts as a legally cognizable harm. In contrast, a duty of care is not based solely on the relationship, and specific harm is needed.

In the Consumer Online Privacy Rights Act (COPRA), privacy harms are included under the duty of loyalty provisions, covering the definitions of deceptive data practices and harmful data practices. Under harmful data practice, five injuries are established: physical; financial; reputational; physical or other offensive intrusion upon the solitude or seclusion of the individual; and "other" substantial injury. The former acting chair of the FTC, Maureen Ohlhausen, discussed injury similarly—the five types of injury she identified through cases brought by the FTC were financial; health and safety; reputational; unwarranted intrusion; and deception injury and subverting consumer choice.

Consideration #3: Advocacy Groups as Enforcers

Groups could be designated at the state level to bring lawsuits in lieu of consumers. If groups were empowered to bring lawsuits instead of consumers, this would lower the number of potential litigants and most likely reduce litigation. Some Senate bills have included provisions permitting a protection and advocacy (P&A) organization to bring a civil action against a covered entity, allowing each state to designate one organization. Of note, there is precedent in federal law for this approach: The Developmental Disabilities Assistance and Bill of Rights Act of 1975, for example, established state P&A systems to advocate, investigate abuses and ensure enforcement. That system also permits class litigation in some cases.

Consideration #4: Sunrise and Sunset Provisions

Sunrise and sunset provisions can impact when a PRA would become effective and how long it would last. A sunrise provision allows for a portion of a law to apply to a specific period of time before the main body of the law becomes active. A sunset clause, on the other hand, provides that an entire statute or portion thereof ceases to exist after a fixed amount of time or certain statutory conditions are satisfied. These mechanisms could be a way to keep legislation in check by timing more aggressive enforcement and incentivizing lawmakers to assess the law's effectiveness continually. The mechanics of such provisions would be important to outline, including: whether time alone triggers the provision; whether certain conditions in the statute need to be met; what other provisions in the legislation might have a sunrise and/or sunset provision; or whether additional congressional approval is needed.

Consideration #5: A Right to Cure

A right to cure, also known as an opportunity to cure, refers to an opportunity for entities to address complaints by consumers before litigation. This process can be managed by a federal agency or court and, when an individual files a complaint, the agency or court is responsible for ensuring that the complaint is addressed; if it is not sufficiently addressed, a PRA could commence. A recent report suggests this could go hand in hand with a right to recourse—an entity's internal process through which a consumer can resolve potential violations and/or privacy concerns. For either to work, standards would need to address what is "corrected enough," whether it should apply to all companies or just smaller ones, how much time should be allowed to resolve the issue and what entity makes and enforces these rules.

Consideration #6: Filing of Complaints with Particularity

Filing complaints “with particularity” means that a plaintiff must provide “in great detail, all the relevant facts forming the basis of her belief” with facts for any malice, intent, knowledge and other conditions of a person’s mind that may be alleged generally. Some argue that privacy claim pleadings now are not mapped to harms, and, after the passage of a federal bill, should be mapped to statutorily granted harms. This is similar to the process undertaken for Securities and Exchange Commission filings or for fraud claims under the Federal Rules of Civil Procedure.

Consideration #7: Feasibility Review

Frivolous lawsuits present a challenge to a PRA. Suit under a PRA could address this concern by being subject to a screening before proceeding to the courts. A review could answer questions of legitimacy, basic adequacy and motivation. Multiple existing state and federal bodies could serve as a model for this type of board, including the Massachusetts Medical Malpractice Tribunal, federal administrative review boards and the U.S Equal Employment Opportunity Commission. Any screening model selected would need to set specifications for duration of review, impartiality, sufficiency standards and resource determinations.

Consideration #8: Injunctive Relief

Injunctive relief is mandated legal action that forces an individual or entity to stop or start a behavior or to carry out a certain action. Injunctive relief could mandate that behavior that is causing harm to an individual or group of individuals be stopped. If enforcement encompasses injunctive relief, it could help reduce lawsuits motivated by financial reasons. However, despite injunctive relief's potential usefulness as an enforcement tool, its effectiveness depends on the specific harm in question. For example, injunctive relief could be granted to require a company to improve its security controls to prevent future similar attacks, but it would not offer other remedies available to litigants in traditional litigation.

Consideration #9: Tiered Rights and Damages

Damages could be structured in several ways to account for the potentially competing variables at play, which include how to make harmed individuals whole, ensure that punishments are appropriate for specific violations and prevent excessive judgments. One proposed concept suggests that dynamic standards be tied to the different provisions in legislation. It would require harms be recognized as invasions of privacy, discrimination or financial loss in one way; violations that affect privacy be recognized in another way; and that all other types of violations be recognized a third way, with a different level of knowledge or intention to be subject to different degrees of liability.

Other considerations related to tiered rights and damages include capping damages to limit exposure; escalating enforcement for willful and repeated violations; determining the types of damages to be awarded like statutory damages and/or punitive damages; and covering other expenses like attorney fees and litigation costs.

Consideration #10: Limiting Legal Exposure

Measures could be implemented to help covered entities limit their legal exposure. There are two common ways of approaching this issue: establishing a safe harbor and making a breach by a nation-state actor an affirmative defense.

A safe harbor, or an affirmative defense, can provide legal protection for a covered entity against a data breach claim if certain steps are taken. By following an established data protection and security framework, such as the standards set out by the National Institute of Standards and Technology, covered entities can be shielded entirely or have their liability limited in precise and predictable ways. A safe harbor serves as an incentive for covered entities to implement data protection measures in favor of incurring litigation expenses and damages. Some states, like Ohio and New Jersey, have already begun the process of framing safe harbors in their respective state laws. To ensure adherence, covered entities can make a certification that is subject to penalties if later proven to be false and/or be subject to independent assessment by a government agency.

A breach caused by a nation-state actor could also be an affirmative defense to prevent companies from being liable. For example, if a company is breached by a Russian advanced persistent threat, lawsuits arising out of that breach would be reserved for governmental prosecution. This could be useful, as some insurance companies are already excluding coverage for hacks and breaches from nation-state actors. Of note, a safe harbor established under similar motivation was enacted after the September 11 attacks with the Terrorism Risk Insurance Act and has been proposed by the Cyberspace Solarium Commission for systemically important critical infrastructure entities.

Consideration #11: Arbitration

An alternative method of resolving disputes is using an arbitrator or a panel of arbitrators instead of litigating in court—a process that would require most cases to be settled outside of court. There is ongoing debate, however, as to whether arbitration should be considered within the confines of a data security and privacy law.

RECOMMENDATIONS

If Congress decides to include a PRA in federal legislation, it must balance an individual's right to be made whole for a privacy violation with a covered entity's concern over excessive lawsuits. If included, it must also strive to create more consistency in enforcement and avoid disparities between courts.

Opponents to a PRA cite drawbacks such as frivolous class-action lawsuits and high costs to businesses, which are concerns we share. Therefore, to achieve a consensus on this issue, we believe a more limited PRA is the solution for addressing these concerns and breaking the deadlock of an all-or-nothing approach. A limited PRA can be viewed as a backstop against the politicization of federal and state enforcement of individual damages, especially for marginalized communities that may be underserved by enforcement agencies. Below, we present our three key recommendations for balancing these objectives and finding a path forward.

Recommendation #1: The structure of a PRA needs to be carefully crafted to ensure it is workable.

If Congress decides to include a PRA in legislation, it should address the mechanics for how a PRA will operate, including specific methods to address standing uncertainty, a delayed start and automatic termination.

- **Specify a right to bring suit in statute, but vary outcomes based on the type of harm**—Demonstrating harm has been a challenge in privacy cases, and recent Supreme Court cases create even more uncertainty as to what level and type of harm is sufficient to bring suit. Congress has a role in defining injuries that can help form the basis of a case, although that does not automatically satisfy standing requirements. Still, Congress could create statutory procedures to allow an individual to sue if, for example, their individual data was unlawfully disclosed—with a one-year statute of limitations from the period the individual knew or should have known about the breach. Congress could also specify the type of data that could constitute sufficient harm. For example, it could be all data covered by the definition of data, or it could be narrowed to a smaller subset.

  In addition, individuals should be permitted to exercise a PRA in cases where actual harm can be demonstrated. This accounts for scenarios in which data was shared or disclosed in violation of the statute outside of a data breach and resulted in a measurable harm.

  Permitting a PRA for other violations covered by federal legislation may present standing issues, including for a right to opt-in or access data. Congress should include statutory procedures to allow for a suit for these violations, but injunctive relief—after a statutorily required compliance period—should be the default instead of monetary damages. This would help reduce the risk of future harm.

There are at least two exceptions to this recommendation: FTC fines and civil rights litigation. The FTC should maintain its right to levy fines in cases it deems necessary. Likewise, in civil rights litigation, individuals should maintain their rights to file suit under civil rights statutes.

- **Privacy harms should be specific, substantive, measurable and enforceable**—As Ohlhausen said in her speech on consumer injury, "Government does the most good with the fewest unintended side effects when it focuses on stopping substantial consumer injury instead of expanding resources to prevent hypothetical injuries." The seven harms identified in recent literature (physical, economic, reputational, psychological, autonomy, discrimination and relationship)—while informative—are too expansive and are not ready to be used as the framework for privacy legislation. Because this list of harms does not have clear recognition and support by courts or consensus policy support, a narrower list of eligible harms should be enumerated by Congress.

  Based on the position taken by the FTC and the definition of harms in COPRA, consensus exists around at least five harms: physical, financial, reputational, deception and unwarranted intrusion. These should form the basis of the data security and data privacy law harm provisions.

Congress should also consider the implications of injury constraint provisions and ensure that decisions on privacy harms in this bill do not negatively impact common law understandings of harms in areas such as property and contracts. Moreover, Congress should make these determinations with the understanding that any standards established for harms are bound by the inherent checks on the ability to use a PRA in the First Amendment, Section 230 and the rules of standing.

- **Do not allow sunrise or sunset provisions**—A sunrise provision would create a window for covered entities to revisit internal compliance structures ahead of enforcement and allow courts the necessary preparation time. However, this also means that consumers would have limited recourse for addressing violations because agency enforcement will initially be slow, given the need to hire additional staff and establish procedures. This makes PRA even more essential at the outset of a federal law.

  A sunset provision would provide covered entities with security that a PRA would be revisited after a certain period or it would end. However, if the PRA were to end abruptly, it could harm consumer recourse, and there is no guarantee that Congress would again revisit the statute to pass updates to the legislation. Congress should instead revisit the legislation holistically after a period of time and revise the PRA as needed.

Recommendation #2: Procedural steps should be implemented before a PRA can be exercised.

This approach will help reduce the number of lawsuits and allows for fixes to be made before litigation. Important aspects of this approach include:

- **Establish a right to cure as a step to solve issues before litigation**—Consumers and covered entities should have a way to address privacy concerns and make complaints before exercising a PRA. As some argued was the case after the passage of the American with Disabilities Act of 1990, initial compliance can create crushing and antagonistic suits without doing much in the way of improving compliance. It can also threaten to put some companies out of business. Addressing initial compliance and creating a cure period can help achieve the aims of consumers (who want to ensure the security and privacy of their data) and of covered entities (who need to use data as a function of their business). There are, however, limits to the usefulness of a right to cure. In cases where the harm was done already, such as a data breach or publication of private images, a right to cure would offer little utility. The focus should therefore remain on the majority of instances where a right to cure is both feasible and useful.

  The ultimate end goal of any enforcement approach is to ensure compliance. A right to cure paired with injunctive relief would likely result in that goal, as the cure period would require a company to implement data protection and privacy safeguards with some immediacy. This has an overall broader beneficial effect on individual consumers as a whole, with faster action and compliance, rather than the limited effect of relief for individual litigants that may come before the court.

Specifically, for a five-year period after enactment, companies should be given a 30-day window to fix violations before a lawsuit should proceed to allow for a transition period. Courts should be the arbiters in cases of whether a company cured a violation (i.e., instead of federal agencies), and companies should be encouraged to develop an internal process to address violations by working with consumers. This is advantageous because informal resolution may be possible before escalating the issue.

- **Privacy complaints should be filed with particularity**—Filing with particularity is a common-sense solution to address the concern that privacy claims could be overly broad. More specifically, in privacy legislation, Congress should include language that specifies that in any private action, the complainant should be required to specify allegations, each violation alleged, and the reasons they believe that to be the case. In cases in which the plaintiff makes allegations against a company (i.e., that it violated the act, made an untrue statement of a material fact, committed a harmful data practice, conducted a deceptive data practice or violated the rights set forth in the act), the complaint should specify each violation alleged and the reason why the claimant believes it to be a violation. In addition, if an allegation regarding the behavior is made on information and belief, the complaint shall state with particularity all facts on which that belief is formed.

  Moreover, in any private action in which the plaintiff may recover monetary damages only on proof that the defendant acted with a particular state of mind, the complaint should state with particularity facts giving rise to a strong inference that the defendant acted with that state of mind.

- **A review process should be a future consideration**—Having a process in place for a federal agency or state attorney general to screen potential lawsuits would be a way to prevent those without merit from proceeding. Of course, specific safeguards would be necessary to ensure that consumers have access to courts in appropriate situations without being limited by a federal or state entity. This is not recommended at the present time because there are inadequate resources at the federal level to accomplish it. If such a federal screen were to be conducted by the FTC, additional resources would be needed. In the case of the passage of federal privacy legislation, the FTC's resources would all go to establishing the privacy bureau and would not be available to establish another new process.

Recommendation #3: Limits should be established for a PRA.

A PRA needs to be restricted with the goal of limiting lawsuits with inconsistent and excessive monetary awards while still providing relief to consumers. Specific ways to limit a PRA include:

- **Incorporate injunctive relief to avoid or mitigate further harm**—The specifics of injunctive relief will depend on the final provisions of a federal privacy bill. Injunctive relief is especially warranted when a consumer alleges that their rights under federal legislation were violated, but a breach has not occurred.

A challenge is that injunctive relief is not always effective after a breach has occurred and works most effectively in situations where immediate remedy is necessary. After a breach, an individual's data has already been disclosed. In such cases, injunctive relief could serve to prevent greater disclosure, but it would not correct what has already transpired in the same way that monetary damages could.

- **Place limitations on damages**—Having constraints on damages would prevent uncapped legal exposure for companies, create more consistent results and interpretation across the courts, and help reduce financially motivated lawsuits. For data breaches and cases where actual harm is demonstrated, individuals should be entitled to actual damages without statutory damages. If the harm is caused by willful behavior, punitive damages should be permitted up to a cap. As has been typical in recent years, courts should also have the authority to order a company to pay for credit monitoring for those who have been affected. For all other violations of federal privacy law, the actions of the company should be willful or repeated to be recoverable. Those cases should be eligible for actual damages and discretionary punitive damages up to a capped amount.

- **Establish a safe harbor**—Entities that take proactive steps or experience a breach from exceptional circumstances should not face the same liability as those who have failed to take affirmative measures to comply with statutory requirements, remain susceptible to known attacks or fail to address longstanding and known vulnerabilities. First, there should be a safe harbor for entities that voluntarily conform to a stated security framework. This would incentivize stronger cybersecurity programs by potentially limiting legal costs. The challenge will be assessing compliance beyond certifications by industry actors. A federal agency should evaluate compliance if a company seeks a proactive evaluation, which would serve as evidence for review by a court. However, a court needs to be able to reject that evaluation and independently evaluate it should an entity not go through agency review first.

  In addition, liability for data breaches caused by nation-state actors should not be the responsibility of covered entities. Safe harbor for covered entities does not preclude those entities from their responsibilities to protect their networks, but it does acknowledge that nation-state, adversary-caused incidents are beyond the normal scope of network defense and liability. In such situations, proof should be required that the breach was caused by a nation-state. With such proof, the company should be able to have an affirmative defense and should not be subjected to monetary penalties.

About this series: *This is part of a series considering the major stumbling blocks of federal data security and data privacy efforts. It draws upon existing research and interview data to identify the most salient issues within data security and data privacy and recommend the most appropriate courses of action in an effort to find compromise on federal legislation.*

INTRODUCTION – The Path to Reaching Consensus for Federal Data Security and Privacy Legislation

PART 1 – Preemption in Federal Data Security and Privacy Legislation

PART 2 – The Role of the Federal Trade Commission in Federal Data Security and Privacy Legislation

EXPLAINER – Answer to Tough Questions: The Framework of a Federal Data Security and Privacy Law

Image: fizkes