Written Testimony

HEARING BEFORE THE UNITED STATES SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

February 27, 2019

Testimony of Michael Beckerman

President and CEO, Internet Association

Chairman Wicker, Ranking Member Cantwell, and members of the Committee, thank you for inviting me to testify. My name is Michael Beckerman and I am President and CEO of Internet Association, which represents over 45 global leading internet companies.[1] Our members include enterprise and consumer-facing businesses that vary in size and business model. Internet Association's mission is to foster innovation, promote economic growth, and empower people through the free and open internet. The internet creates unprecedented benefits for society and the economy, and as the voice of the world's leading internet companies, we ensure stakeholders understand and can take advantage of all the benefits the internet has to offer.

We appreciate the Committee holding this hearing to advance the conversation around an American approach to data privacy. Internet Association members support a modernized U.S. privacy framework that provides people meaningful control over their data across all industries, makes companies accountable, and includes meaningful enforcement. A globally respected American regulatory framework must prioritize protecting individuals' personal information and foster trust through meaningful transparency and control. We believe this can be done by empowering people to better understand and control how personal information they share is collected, used, and protected. People should also be able to access, correct, move, and delete their personal information except where there is a legitimate need or legal obligation to maintain it. Consumers deserve the right to control the use of their personal information, and we want to see the president sign a new law this year.

The internet industry and IA member companies are far from perfect. And we understand that we fail or succeed based on people's trust with our products and services. Our members are committed to doing better, and that commitment is driven by the top executives in all of our companies and supported by employees across all parts of the company, including product and technical teams. The transparency[2] and tools[3] that exist online today are a direct result of our industry's commitment to adapting to consumer feedback, and we remain committed to making new improvements every day. People expect more from our industry and we will deliver.

As we consider the important topic of modernizing America's approach to data privacy, it is important to remember that data has revolutionized every part of our economy and daily lives. It allows us to easily stay in

---

[1] Internet Association members include Airbnb, Amazon, Ancestry, Coinbase, DoorDash, Dropbox, eBay, Etsy, Eventbrite, Expedia, Facebook, Google, Groupon, Handy, HomeAway, IAC, Intuit, letgo, LinkedIn, Lyft, Match Group, Microsoft, Pandora, PayPal, Pinterest, Postmates, Quicken Loans, Rackspace, Rakuten, reddit, Snap Inc., Spotify, Stripe, SurveyMonkey, Thumbtack, TransferWise, TripAdvisor, Turo, Twilio, Twitter, Uber Technologies, Inc., Upwork, Vivid Seats, Yelp, Zenefits, and Zillow Group.

[2] For example, https://transparencyreport.google.com, https://transparency.twitter.com, https://transparency.facebook.com, https://www.linkedin.com/legal/transparency, https://help.pinterest.com/en/article/transparency-report, https://www.redditinc.com/policies/transparency-report, https://www.snap.com/en-US/privacy/transparency/.

[3] Examples of privacy tools include: https://myaccount.google.com/privacycheckup, https://www.facebook.com/help/325807937506242, https://twitter.com/settings/safety, https://www.linkedin.com/psettings/,

touch with loved ones from a distance, get to work on time with efficient navigation, find the perfect playlist based on curated recommendations, and build communities around shared interests. Data also enables farmers to manage their costs of doing business, doctors to provide patients with precision healthcare, and teachers to inform their classroom practices.

Internet Association has travelled around the country and heard directly from small business owners and community leaders who use data and internet platforms to grow their businesses, communicate with their customers, bring the community together, and hire new employees. We met with a high school sophomore in Shelby, North Carolina who started a local monogram clothing business by taking orders on social media. After two years, demand became so high that she opened a physical store. In Claremont, New Hampshire, we heard from an animal shelter that said animal adoptions tripled since they started posting about their pets online. These are just a few of the millions of stories that exist from non-tech small businesses and nonprofits in every state. These are the real winners of a data-driven community. And if we fail to get this legislation right or end up with a patchwork of state laws, it will be these small businesses that lose out.

The U.S. has long been a global leader in political and technological innovation, empowering our citizens by establishing the world's oldest constitutional democracy, and by investing in the technology that laid the foundation for the internet as we know it today. We need to develop an approach to privacy legislation that is in keeping with the founding principles of our democracy and the spirit of innovation that underpins America's technological leadership. An American approach to privacy can deliver strong, enforceable privacy protections while allowing for continued U.S. leadership in technology.

Internet Association and our member companies are fully committed to supporting the passage of meaningful federal privacy legislation. We have been active participants in the robust public debate currently taking place in the U.S. around data privacy, and we released Privacy Principles[4] last year to further the discussion around what an American approach to privacy may look like. We encourage the committee to consider our Privacy Principles as it looks to craft federal privacy legislation.

All businesses – from search engines to local pizza shops – depend on data to do things like enhance their services, manage inventory, and strengthen relationships with customers. Non-profits also use data to engage their communities, recruit volunteers, and reach new donors. To provide meaningful and comprehensive privacy protections, a federal privacy law must cover all parts of the economy and eliminate the risk that a confusing patchwork of state laws could impose conflicting obligations on companies that serve customers in multiple states. Americans should have consistent experiences and expectations across state lines and industries – regardless of whether they're interacting with a company online or offline.

A federal privacy law should also be grounded in a risk-based approach and avoid overly prescriptive methods that may not be appropriate for all business models. A national framework should consider the sensitivity of the personal information, the context of its collection and use, and the risk of tangible harm for its misuse or unauthorized access. Not every single piece of data is the same, and it's important to consider the risks, the harms, and the consequences associated with different types of data.

User trust is fundamental to the success of internet companies, and responsible data practices are critical for earning and keeping user trust. Any company processing personal data should do so responsibly, acting as a good steward by taking steps to ensure that data is handled in a manner that conforms to consumers' reasonable

[4]https://internetassociation.org/files/ia_privacy-principles-for-a-modern-national-regulatory-framework_full-doc/

expectations. A federal law can promote the proliferation of responsible data practices by allowing for the use of privacy enhancing techniques such as de-identification or use of aggregated data. California's new law, in contrast, fails to clearly allow these techniques to be applied to personal information, actually making people less protected.

The internet industry is among the most consumer-centric industries in the world. Internet companies enable direct, real-time customer interactions and feedback, which help our companies better understand consumers needs to improve and upgrade their services, including on privacy.

Today, with less than five clicks, we can change the privacy settings on our favorite social media site or streaming service. Online platforms also proactively create contextual tools that help us better understand and control our privacy settings. With or without a law, our members will continue listening to their customers and providing them with more control over their data. But, ultimately, we firmly believe that consumers and companies both will benefit from certainty in the rules that govern how data is collected, used, and protected. The burden should not solely lie with individuals.

Individuals Deserve Strong, Unified National Protections

The internet industry supports a federal framework that provides all individuals the same fundamental privacy protections regardless of which state they live in, whether they prefer to do business on or offline.

While protections exist today, the current landscape is too complex and disjointed for people to understand. There are privacy laws that impact many aspects of a person's life, but those laws differ depending on which state they are in, who they share their personal information with, and the type of information they share. There are federal sectoral protections in the health and financial services areas that apply to certain types of businesses, but don't protect health and financial information generally. There are laws in some states which give residents of those states protections when dealing with an entity that is covered by the law. Those protections end at the state line. This means that residents of some states benefit from more privacy protections than residents of other states. It also means that residents of a state with privacy protections do not enjoy those protections when they travel, when they purchase from retailers who don't do business in their state, or when they deal with local entities that may not be covered under their state's laws[5]. People should not be expected to know which rules apply depending on where they are and who they dealing with. IA believes that it is possible to give individuals strong consistent privacy protections while allowing for innovation and economic growth. In fact, we believe that strong consumer privacy laws are critical to the continued success of our industry.

A nationwide standard for the protection of personal information would enhance trust in data uses by providing individuals with a consistent set of expectations that they can rely on in every aspect of their lives. Congress should take action to set an economy-wide privacy standard to ensure individuals have clear expectations in terms of how their personal information will be collected, used, and protected.

There is significant energy in the states to provide new privacy protections to their residents. But this does not solve the complexity issue for individuals or fill all the gaps in privacy protections. In fact, as new privacy laws are passed and come into effect, this landscape becomes more confusing and difficult to understand. State privacy laws are only becoming more splintered, taking widely varying approaches and affording different rights and protections to their residents. This makes it impossible for people, who do not track state privacy legislation as a

[5] *See* Cal. Civ. Code § 1798.140(c), which exempts non-profit and small businesses from obligations established by the California Consumer Privacy Act.

full-time job, to understand what choices and rights they may have across the different parts of their lives.

IA member companies have heightened awareness of not just the challenges for individuals, but also for businesses that must comply with the patchwork of laws. Most IA members have business models that grow and support small to medium-sized businesses - and know first-hand that compliance burdens fall heaviest on growing businesses that have to devote scarce resources to developing compliance plans to meet each state's requirements.

Federal Privacy Legislation Should Focus On Individual Rights

A federal privacy law should be centered around the individual in three important respects. First, federal legislation should ensure that individuals have access to information about the personal information that is collected from or about them, including how that data will be used, shared, and protected. Second, federal legislation should support the development of tools to give users more control over their personal information. Third, federal legislation should give individuals the ability to access, delete, correct, and move their personal information.

Transparency

IA's members are leaders in providing users with transparency, granular control, and the ability to exercise rights and choices. IA members have been subject to legal and regulatory obligations to have privacy policies specific to the online environment for years and do the best they can under the current legal framework to ensure their policies are understandable and digestible. FTC enforcement as well as state laws and state attorney general enforcement have built on the requirements for privacy policies. Privacy policies must be carefully written to meet legal requirements and also to avoid enforcement actions if a regulator believes a company has acted in a manner that is inconsistent with their privacy policy. Even though this may naturally end up being the domain of corporate lawyers, IA members have been innovating with privacy policies for years, writing in plain English and making the policies more easily understood. IA member companies create new tools and services, such as privacy centers, that make long policies more modular and easier for users who care about specific issues to quickly find those items and to delve further into details. Many IA members summarize the key elements of their policies at the top and also through short, easy to follow videos. Some member companies also invest in consumer research to determine more effective ways to present information to consumers. All IA members are committed to continuing to improve the ways in which they share information about how data is collected, used, and protected.

Outside the internet industry, there is still much work to be done to educate people about how their personal information is handled. In some cases, individuals have little to no information about how businesses obtain their personal information, let alone how that information will be used or with whom it may be shared. The lack of a comprehensive federal privacy law and scattered state laws have left entire industries without any legal requirements to inform consumers about their personal information practices. This cannot continue. Heavily data-driven industries gather personal information from and about individuals, but do so without using the internet or even direct consumer interaction. The public only finds out about these businesses' practices when their stores of personal information are the subject of a data breach. Individuals deserve information on who is collecting their information, regardless of the means, and how it is being used. Federal law should shine a light on these practices by requiring entities subject to the law to provide an appropriate level of transparency about data practices.

The inverse of too little information is also problematic for consumers. At the other end of the spectrum, people are overloaded with information that may not be helpful in making important decisions about their privacy. This is

particularly true in highly specialized or technical areas where a thorough understanding of the technology infrastructure is necessary to explain in detail how information is collected, the types of information collected, how it may be shared, and the individual's choices about those practices. Though well-intentioned, Europe's new privacy law, the General Data Protection Regulation (GDPR), has exacerbated this problem with new requirements requiring companies to provide even more information. It is not clear that more information benefits EU residents. For example, cookie banner requirements have resulted in consumers being bombarded with notices that in truth offer little choice. A U.S. approach to transparency could show global leadership by developing notice practices that are focused on the desired outcome – individuals understanding the risks and rewards of the use of their data and making informed choices about those risks.

User Control

Once consumers are better informed about data practices, they may want to actively manage the information they share and how it is used. IA's Privacy Principles include the principle that "[i]ndividuals should have meaningful controls over how personal information they provide to companies is collected, used, and shared, except where that information is necessary for the basic operation of the business or when doing so could lead to a violation of the law." For example, a social networking company may offer different settings for users to control who is able to find their profile or how much information is shared with different types of contacts. On platforms that infer interests from use of the service to make content recommendations or for advertising purposes, providers may share those interests with the user, and allow them to remove interests they no longer want associated with the platform or service. Members who are part of the online advertising ecosystem participate in codes of conduct from the National Advertising Initiative (NAI) and Digital Advertising Alliance (DAA), which give individuals the option to opt-out of third party tracking for advertising purposes.

This level of granularity is not appropriate to all enterprises or all contexts. For example, many companies use different providers to help operate their businesses. These could be payment processors, delivery companies, or a website host or cloud provider. It would not make sense for consumers to have a choice over the use of these providers since it would interfere in the company's basic business operations, as well as the ability to perform services the consumer requested.

Personal Information Rights

IA members also support user rights to access, deletion, correction, and portability. These rights provide users control over their personal information by allowing them to take action after the information has been collected. IA included these rights in the IA Privacy Principles:

- **Access**. Individuals should have reasonable access to the personal information they provide to companies. Personal information may be processed, aggregated, and analyzed to enable companies to provide services to individuals. Safeguards should be included to ensure that giving an individual the ability to access their personal information does not unreasonably interfere with other individuals' privacy, safety, or security, or a company's business operations.
- **Correction**. Individuals should have the ability to correct the personal information they provide to companies, except where companies have a legitimate need or legal obligation to maintain it.
- **Deletion**: Individuals should have the ability to request the deletion of the personal information they provide to companies where that information is no longer necessary to provide the services, except where companies have a legitimate need or legal obligation to maintain it.
- **Portability**. Individuals should have the ability to obtain the personal information they have provided to

one company and provide it to another company that provides a similar service for which the information is necessary.

IA members have been leaders in implementing tools to empower individuals to have control over the data they share. Not only are individuals given the controls described above, but they are often able to access the personal information they have shared with an internet company in real-time, without submitting a special request. They may be able to download that data directly in a commonly-used file type with a few simple mouse clicks, or by submitting an online request to the provider. Individuals may be able to directly edit their customer records and even remove records about their past use of the service – such as messages and photos, searches performed, products purchased, or streaming content viewed. This type of access to data that facilitates the exercise of user rights, existed in the internet industry years before GDPR and the California Consumer Privacy Act (CCPA), and should be expanded to all entities that control personal information.

Elements Of Comprehensive Privacy Legislation

IA believes that federal legislation should create individual personal information rights and rules for entities that process personal information on a nationwide basis, covering all unregulated sectors or harmonizing with sectoral regulation, and applying equally to online and offline environments – particularly for companies that don't have direct relationships with consumers or where people didn't sign up for a company's product or service. For this legislation to be successful in building trust in the entities that process personal information, without adversely impacting innovation, the legislation will have to be flexible, capable of evolving with changes in technology, and focused on privacy outcomes rather than prescribing how to achieve them.

For a federal standard to address privacy across sectors, organizations of different scale, and different business models, it will need to be flexible enough to adapt to a range of entities processing personal information in varying contexts and for different purposes. A federal standard should not introduce barriers to entry for small and new businesses. As organizations grow, the expectations regarding the measures they implement to protect personal information can also grow. The FTC has recognized the importance of adjusting security and data protection compliance obligations to match the size and complexity of organizations, and a federal legislative framework that mirrors this approach will benefit consumers and businesses alike.

A federal standard must also be written so that it can adapt to currently unknown, but nevertheless inevitable changes in the technology used to collect, store, use, and transmit data. To that end, it is better to build structures that focus on assessing and mitigating risk. Many of the services that have revolutionized our daily lives, such as home assistants, using our fingerprints or cameras to unlock devices, real-time traffic information, and GPS trackers for fitness would have seemed scary and full of risk 20 years ago. These products and services only exist because government policies have been largely successful in preserving individual rights while allowing technological innovation, including in the field of encryption, to flourish. We should not interfere with the next generation of advances.

To withstand the passage of time, a law also needs to be careful not to be overly prescriptive about the processes, technologies, or requirements for meeting a privacy objective. We do not have to look hard to find examples of data-focused laws that embraced the prevalent technologies of their time, but have struggled to keep pace with innovation. The Electronic Communications Privacy Act ("ECPA") is a good example. Congress was wise to recognize so early that electronic communications would revolutionize both business and personal interactions, but notwithstanding that foresight, the legislative language expressly applies to specific categories of service providers that existed at the time, and the types of data they collected, stored, and used. As technology and

services evolved, ECPA fell behind. Before cloud-based email became a prevalent mode of communication, many viewed emails kept for more than 6 months as inconsequential information that did not require a search warrant. Today, email is often used as a personal lock box, and government may rely on lesser privacy standards to access electronic copies of personal information, even though a search warrant would be required to access that same information in the physical world. Federal data privacy legislation should be drafted to focus on desired outcomes and should not be specific to technology, to allow organizations to determine the best way to achieve that outcome in their operating environment, including other privacy laws.

Flexibility in federal privacy law is also important to allow harmonization with global privacy laws that impact the operations of many U.S.-based organizations. The U.S. should adopt rules that make sense for the American public, while also enabling the U.S. to maintain important mechanisms that facilitate cross-border data flows and add to the developing global consensus around the core building blocks of personal privacy laws.

A Risk-Based Approach

IA believes that we have the opportunity to develop a strong and uniquely American approach to privacy that focuses on addressing the risk of harm to the individual, and that by focusing on identified risks we can deliver more meaningful privacy protections without imposing unnecessary burdens and restraints on innovation. IA's Privacy Principles explain:

- **Risk-based framework**. A national privacy framework should be grounded in a risk-based approach, based on the sensitivity of the personal information, the context of its collection and use, and the risk of tangible harm for its misuse or unauthorized access. Consistent with FTC data security order provisions and the FTC's unfairness standard, companies should identify and address reasonably foreseeable risks to the privacy and the security of personal information where the result of failing to address the risk would cause, or be likely to cause, tangible consumer harm.

An American approach to privacy should consider the context of the interaction between the individual and the entity collecting the data. For example, you expect a car rental company to be able to track the location of a rented vehicle that doesn't get returned. You don't expect the car rental company to track your real time location and sell that data to the highest bidder. By focusing our efforts on addressing unexpected uses of data that pose risks to individuals, we can protect privacy without inundating people with information about things – like notices about cookies – if they are consistent with consumers' reasonable expectations. We should focus on providing people with the most important information they need to make informed choices about their privacy.

We are at an inflection point where it is critical that privacy and security considerations be integrated into risk management frameworks for organizations that process personal information, and into the product development process for organizations that build data-driven products. Efforts like NIST's Privacy Framework may provide important tools that organizations across all sectors and of all sizes can use to assess privacy risks on an ongoing basis. It can also educate organizations on potential options for risk mitigation. Federal legislation can support this cultural shift by incentivizing the use of tools like the NIST frameworks on privacy and security, security certifications, privacy certifications, sector specific tools like codes of conduct, and FTC education efforts designed to raise awareness of individuals.

Responsible Data Security Practices

User trust is fundamental to the success of internet companies, and responsible data practices are critical for

earning and maintaining user trust. Any company processing personal data should do so responsibly, acting as good data stewards. While less visible to individuals, an organization's internal controls can be as important, if not more important, to protecting the privacy of personal information as external facing information and mechanisms. These controls do not have to be formal or elaborate to be effective, but they must be focused on identifying and mitigating risk. They should consider the entire lifecycle of personal information within the organization and ensure the information is properly collected, used, shared, and secured.

Reasonable security measures are critical to maintaining the privacy of personal information, and IA believes that no comprehensive privacy law will be complete without a requirement that covered entities adopt appropriate technical and organizational measures to protect the confidentiality, integrity, and availability of personal information. The best privacy policy and user controls mean little if an individual's personal information can be easily compromised by a bad actor.

IA also believes that security breach notification is an important element of comprehensive legislation to protect personal information. Breach notification allows individuals to take action to protect themselves from the risks that result from having personal information acquired by unauthorized parties. This could include monitoring for identity theft, credit freezes, and password changes. IA has long[6] supported federal breach notification laws and has included breach notification as a key element for federal privacy legislation in the IA Privacy Principles. All 50 states and many U.S. territories now have breach notification requirements. A federal standard for breach notification would ensure that residents throughout the United States benefit from the same level of protections and receive consistent access to key information when their personal information is compromised.

Security requirements and security breach notifications are important elements of privacy legislation, but IA is also sensitive to the risk that the more elements added to legislation, the more complex it is for it to become law. There are existing breach notification requirements covering most of the United States, thus the level of urgency for a federal breach law is not as high as it is for an economy-wide federal privacy law.

Meaningful Enforcement

Companies that engage in unfair and deceptive trade practices that harm consumers should be held accountable. The FTC is the appropriate agency to enforce consumer-focused data privacy and security laws. The FTC has demonstrated expertise in privacy and security and a commitment to engaging in enforcement activity designed to improve the level of protections that consumers receive across entire sectors, not just from a single company.

The goal to have a federal standard for personal information protection will require a strong lead regulator. This is not to say that the FTC must be the only regulator who can enforce a federal privacy law, but that it should retain oversight on enforcement activities to ensure consistent application of the law.

A federal privacy law that covers all entities that process personal information that are currently unregulated will clarify and expand the FTC's enforcement authority and responsibility. IA member companies strongly support providing the FTC with the resources needed to execute those responsibilities. IA member companies also believe the FTC should continue its mission of educating individuals on their rights and protections under the law, and this effort should be encouraged and appropriately resourced. The FTC also educates organizations on their obligations and best practices through efforts such as the Cybersecurity for Small Business campaign. These types of campaigns and guidance documents provide vital resources for smaller businesses that need additional clarity on

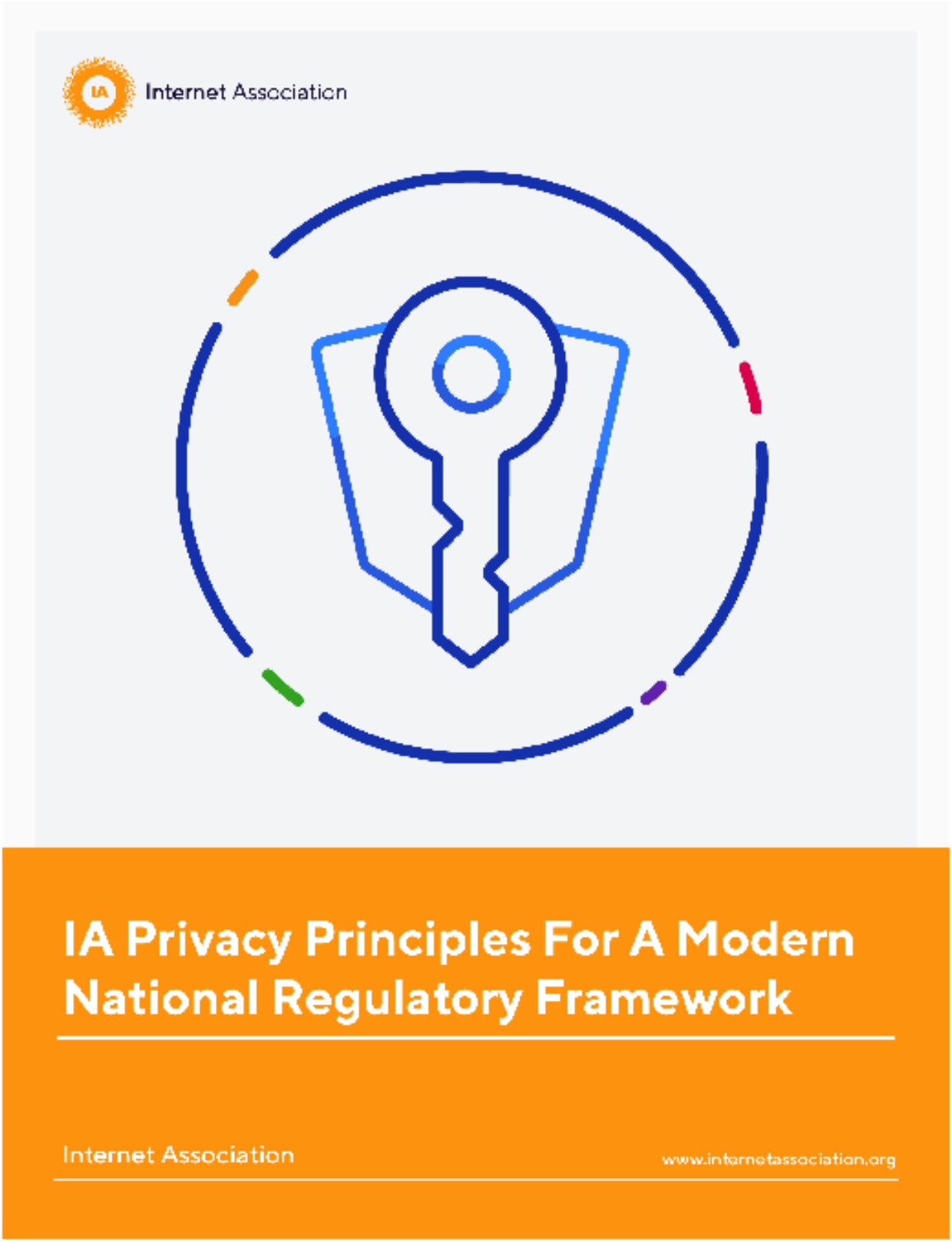
[6]https://internetassociation.org/031815datasecurity/

how legal obligations apply to their specific organizations.

An enforcement regime should foster a culture of accountability and responsibility and will depend on the rest of the bill.

Conclusion

Internet Association and our member companies stand ready to work with this Committee and all other interested parties on an American approach to protecting people's privacy that allows for continued U.S. leadership in technology. The time is now for a national privacy law that provides consumers in every state both on and offline meaningful control over data in all sectors of the economy. Our goal is to see bipartisan legislation signed by the president this year.


Internet Association
IA Privacy Principles For A Modern National Regulatory Framework
Internet Association
www.internetassociation.org

Introduction

The time is right to modernize our federal rules and develop a national framework for consumer privacy. That framework should be consistent nationwide, proportional, flexible, and should encourage companies to act as good stewards of the personal information provided to them by individuals.

As policymakers and stakeholders work on an updated approach to privacy, we must ensure that a national privacy framework:

- Protects individuals' personal information and fosters trust by enabling individuals to understand their rights regarding how their personal information is collected, used, and shared;
- Meets individuals' reasonable expectations with respect to how the personal information they provide companies is collected, used, and shared, and the context-dependent choices they have;
- Promotes innovation and economic growth, enabling online services to create jobs and support our economy;
- Demonstrates U.S. leadership in innovation and tech policy globally;
- Is mindful of the impact of regulation on small- and medium-sized companies; and
- Applies consistently across all entities to the extent they are not already regulated at the federal level.

Context For Principles

Our country's vibrant internet ecosystem provides individuals with unprecedented personal, social, professional, educational, and financial benefits, contributing an estimated 6 percent of U.S. GDP and nearly 3 million American jobs. The internet enables all levels of government and every sector of the economy to become more citizen- and consumer-centric by providing innovative tools, services, and information, and allowing for a more efficient use of resources.

IA companies believe trust is fundamental to their relationship with individuals. Our member companies know that to be successful they must meet individuals' reasonable expectations with respect to how the personal information they provide to companies will be collected, used, and shared. That is why our member companies are committed to transparent data practices, and to continually refining their consumer-facing policies so that they are clear, accurate, and easily understood by ordinary individuals. Additionally, our member companies have developed numerous tools and features to make it easy for individuals to manage the personal information they share, as well as their online experiences.

There are a range of strong privacy, data security, consumer protection, and anti-discrimination laws that exist today. These include Section 5 of the FTC Act and the Clayton Act, as well as more than 15 other federal statutes and implementing regulations that are sector specific or relate to particular activities.[7] Additionally, there are

[7] These are the Children's Online Privacy Protection Act ("COPPA") and the FTC's COPPA Rule; the Gramm-Leach-Bliley Act, and the FTC's Privacy and Safeguards Rules; the Electronic Fund Transfer Act; the Fair Credit Reporting Act; the Fair and Accurate Credit Transactions Act; the Equal Credit Opportunity Act; The Truth in Lending Act; the Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN-SPAM") Act of 2003 and the FTC's CAN-SPAN Rule; the Telephone Consumer Protection Act; the Restore Online Shopper's Confidence Act; the Video Privacy Protection Act; the Cable Act; the Electronic Communications Privacy Act; the Computer Fraud and Abuse Act; the Stored Communications Act; the Telemarketing and Consumer Fraud and Abuse Prevention Act and the FTC's Telemarketing Sales Rule, including the Do Not Call Rule and Registry; and the U.S. Safe Web Act.

myriad state laws relating to privacy and data security, enforced by state attorneys general or private litigants, including state data breach notification statutes and unfair and deceptive acts and practices statutes; data security and encryption laws; and a variety of other privacy laws that relate to online privacy, social security numbers, and data brokers. Our member companies comply with these current laws as well as with self-regulatory principles and rules that govern how they operate and do business.[8] However, this array of laws also creates a "patchwork" effect that complicate compliance efforts and lead to inconsistent experiences for individuals. A new, comprehensive national framework would create more consistent privacy protections that bolster consumers' privacy and ease compliance for companies.

This document sets forth: (1) principles for a national privacy framework, and (2) considerations for policymakers when evaluating such a national privacy framework.

Privacy Principles

These privacy principles aim to protect an individual's personal information, which we define as any information capable of identifying a specific individual or a device that belongs to that individual.

- **Transparency**. A national privacy framework should give individuals the ability to know whether and how personal information they provide to companies is used and shared with other entities, and if personal information is shared, the categories of entities with whom it is shared, and the purposes for which it is shared.
- **Controls**. Individuals should have meaningful controls over how personal information they provide to companies is collected, used, and shared, except where that information is necessary for the basic operation of the business or when doing so could lead to a violation of the law.
- **Access**. Individuals should have reasonable access to the personal information they provide to companies. Personal information may be processed, aggregated, and analyzed to enable companies to provide services to individuals. Safeguards should be included to ensure that giving an individual the ability to access their personal information does not unreasonably interfere with other individuals' privacy, safety, or security, or a company's business operations.
- **Correction**. Individuals should have the ability to correct the personal information they provide to companies, except where companies have a legitimate need or legal obligation to maintain it.
- **Deletion**: Individuals should have the ability to request the deletion of the personal information they provide to companies where that information is no longer necessary to provide the services, except where companies have a legitimate need or legal obligation to maintain it.
- **Portability**. Individuals should have the ability to obtain the personal information they have provided to one company and provide it to another company that provides a similar service for which the information is necessary.

The adoption of the principles identified above would enhance individuals' personal privacy and ensure individuals' trust. To ensure the effectiveness of a national privacy framework, these principles must be balanced against: (1) competing individual rights, including freedom of speech and expression; (2) other parties' privacy interests; (3) data security interests; (4) companies' needs to protect against fraud or other unlawful activity, or individual safety; (5) companies' requirements to comply with valid law enforcement requests or judicial proceedings; (6)

[8] These self-regulatory bodies have developed their own codes of conduct, including the Data and Marketing Associations Ethical Business Practices; the Network Advertising Initiative's 2018 Code of Conduct; the Digital Advertising Alliance's set of Self-Regulatory Principles relating to online advertising, which are enforced by theAccountability Program of the Council of Better Business Bureaus; and the Payment Security Industry Data Security Standards (PCI-DSS), for those that accept payment cards.

whether the exercise of the rights afforded individuals are unduly burdensome or excessive in specific instances; and (7) whether individuals' exercise of their rights would require companies to collect or process additional personal information about that individual.

Proposed Considerations for Policymakers

Fostering privacy and security innovation. A national framework should not prevent companies from designing and implementing internal systems and procedures that enhance the privacy of each individual's personal information. Companies should take into account privacy and data security when they design and update their services, for example, by de-identifying, pseudonymizing, or aggregating data.

A national data breach notification law. A national framework should specifically preempt the patchwork of different data breach notification laws in all 50 states and the District of Columbia to provide consistency for individuals and companies alike. This national standard should protect individuals and their personal information through clear notifications, define a harm-based trigger for notification to avoid notice fatigue, and allow companies flexibility in how they notify individuals of unauthorized access to their personal information.

Technology and sector neutrality. A national privacy framework should include protections that are consistent for individuals across products and services. Such a framework should be both technology neutral (no specific technology mandates) and sector neutral (applying to online and offline companies alike).

Performance standard based approach. A national privacy framework should focus on accomplishing privacy and data security protections, but laws and regulations should avoid a prescriptive approach to doing so, as such an approach may not be appropriate for all companies and may well become obsolete in light of rapidly developing technology.

Risk-based framework. A national privacy framework should be grounded in a risk-based approach, based on the sensitivity of the personal information, the context of its collection and use, and the risk of tangible harm for its misuse or unauthorized access. Consistent with FTC data security order provisions and the FTC's unfairness standard, companies should identify and address reasonably foreseeable risks to the privacy and the security of personal information where the result of failing to address the risk would cause, or be likely to cause, tangible consumer harm.

A modern and consistent national framework for individuals and companies. A national privacy framework should be consistent throughout all states, preempting state consumer privacy and data security laws. A strong national baseline creates clear rules for companies and ensures that individuals across the United States can expect consistent data protections from companies that hold their personal information. A national privacy framework should primarily be enforced by the FTC at the federal level and by state attorneys general at the state level, where the FTC declines to act.