The Software & Information Industry Association's Response to NTIA's Request for Comments on Developing the Administration's Approach to Consumer Privacy Docket No. 180821780-8780-01 November 9, 2018

The Software & Information Industry Association (SIIA) is the principal trade association for the software and digital content industries worldwide. The association provides global services in government relations, business development, corporate education, and intellectual property protection to its members, the leading companies that are setting the pace for the digital age.

SIIA appreciates the opportunity to respond to the request for comments from the National Telecommunications and Information Administration on developing the Administration's approach to consumer privacy. SIIA favors the passage of a new national privacy law that can provide strong substantive consumer privacy protections and promote innovative and socially beneficial uses of personal data as well. SIIA encourages the Administration to work with all stakeholders in industry, consumer groups, think tanks and academia and with the Congress to develop a new privacy law that has broad bi-partisan support. The comments that follow are directed toward this legislative initiative.

Overview: the purpose of privacy law

The rethinking prompted by the NTIA privacy notice and the movement toward Congressional consideration of new national privacy legislation creates an opportunity for clarity about the purposes and intended outcomes of privacy law.

However, the notice is not very clear about this basic question. At one point it says "the consent of an informed user is the end-goal of most approaches to consumer privacy" and "the desired outcome is a reasonably informed user, empowered to meaningfully express privacy preferences."

But this confuses means and ends. The real purpose and desired outcome of privacy law is the protection of people from injuries resulting from the collection, dissemination or use of personal information. Allowing reasonably informed people to express privacy preferences is one way to get to this result, and in some cases, it might be essential. Nevertheless, privacy law should protect people even if the ubiquitous collection and use of personal information characteristic of today's data environment overwhelms their ability to discern the purposes of data use and to judge whether such uses are safe for them.

The notice recognizes this difficulty of relying solely or principally on individual control as a means of privacy protection, calling instead for companies to provide "products and services that are inherently designed with appropriate privacy protections, particularly in business contexts in which relying on user intervention may be insufficient to manage privacy risks."

SIIA welcomes this focus on managing privacy risk, rather than relying solely or primarily on user consent and urges NTIA to clarify the role of consent and harm in its approach to privacy.

Relying solely on people to have enough information to detect all privacy risks is counterproductive both from the point of view of protecting people from harm and from the point of view of promoting innovation and the beneficial uses of data. Since people will never have enough information to adequately assess privacy risks, relying solely on notice and consent is a recipe for consumer abuse. In addition, blocking information use until each individual fully understands the details of all immediate and future uses of personal information and has clearly assented to these uses would be a recipe for thwarting innovation and socially valuable data uses.

Privacy scholar Helen Nissenbaum makes these points clearly, saying "requiring consent for every use isn't reasonable and may prevent as many good outcomes as bad ones. Imagine if new science suggests a connection between a property, or cluster of properties, and a particular cancer treatment. Returning for consent may impose obstacles that are impossible to overcome."

She rejects the idea that "incremental improvement in consent mechanisms is the solution" for a more fundamental reason – consent is not what privacy should be all about. "My position is not that modeling "true" consent in this age of digital technologies is hard or even impossible, but that in the end, it's simply not a measure of privacy!"

If policymakers move beyond privacy as individual control, there are two alternative views of privacy. Nissenbaum endorses the idea that law should reinforce the reasonableness or appropriateness of data flows in the social context in which it takes place.

This focus on social context reflects an important characteristic of personal information that is neglected by the individual consent model of privacy protection. Almost all personal information is relational, directly or indirectly revealing characteristics, preferences, beliefs and other features of more than one person. If I exchange something with you, you have as much of an interest in the information about that transaction as I do. A picture or recording of several people concerns all of them. Consequential information about me such as my political beliefs, my credit worthiness and my sexual orientation can be gleaned by examining information about people who are like me or who are part of my social network, even if I chose never to reveal such information to outside parties.

This social nature of information is the general case, not an outlier. Information solely pertaining to a single individual is a vanishingly small fraction of all information. Confining privacy rights to a single data subject is indeterminate, since all parties would have some claim to the protection of information related to their interactions and transactions. Rights and responsibilities of the different parties have to be assigned more granularly, based on the policy objectives sought, not through the wholesale grant of privacy rights to one party to an interaction.

However, there is a tension between this view of privacy as a matter of protecting the social entrenched "reasonable expectations" that people have in particular contexts and privacy as matter of protecting people against consumer harm. They don't always come to the same thing. For instance, a practice such as being tracked by a smart TV might be totally unexpected but have no real harm associated with it. Moreover, a practice such as a novel data analytic technique that can personalize and improve student learning or medical treatment might be outside traditional expectations and yet provide for substantial benefits.

The new privacy law needs to address this tension in some way. One way forward is to treat what people might normally expect in context as something to be considered when determining if a practice is reasonable. The basic standard is harm, but when a practice is at extreme variance from ordinary expectations, that might in some circumstances make it unreasonable.

On the other hand, an unexpected data use might advance the goals of a particular social practices such as education or medicine, or have wider public benefits. It should not be ruled out simply because it is a non-traditional, novel use of data. Nissenbaum recognizes that relying on what most people expect favors "entrenched norms." But she also says that privacy law and policy need to allow for "norms to change — sometimes slowly, other times rapidly — not because these changes are foisted upon us by tech companies, but because they promote interests and values."

The particular facts and circumstances can help a privacy enforcement agency such as the Federal Trade Commission to decide in specific cases.

Other privacy scholars have focused on this notion of privacy as a form of consumer protection. For instance, Ben Wittes thinks that privacy law should provide for a right to be protected against "databuse" that is, "a negative right—a right against the unjustified deployment of user data in a fashion adverse to the user's interests." Former FTC Chairman Tim Muris and former head of the FTC Bureau of Consumer Protection Howard Beales also adopted a harms approach arguing that privacy law and regulation should focus on consequences, not consent. It also generally coheres with the idea articulate by the Information Accountability Foundation (IAF) that information should be collected and used for beneficial purposes.

This focus on privacy as a way to protect consumers from harm should be distinguished, however, from the idea, developed by legal scholar Jack Balkin, that privacy law should require data collectors to act as information fiduciaries who must act solely in the interests of the individual whose data they collect, or at least not to undermine those interests. Balkin says, "information fiduciaries have special duties to act in ways that do not harm the interests of the people whose information they collect, analyze, use, sell, and distribute."

IAF identifies the flaw in this information fiduciary conception of privacy. They acknowledge that "…individuals may expect that organizations will process data that pertains to them in a fashion that creates benefits for them, or if not them a broader community of people," but they also note that "there are times when objective processing does not serve the needs of each and every individual, while serving the broader needs of society."

Sometime the legitimate interests of companies and the broader needs of society take precedence over individual preferences in information use. For instance, a person engaged in legal hate speech might have an interest in successfully spreading this material. If companies were required to use personal information solely to further the individual interest of their users, or mandated not to use personal information to thwart their users' individual interests, they would be unable to use personal information to block this material, even though it is in violation of their terms of service and harmful to wider community interests.

Moreover, it is not clear whose interests the fiduciary should prioritize. Companies also use personal information to deliver messages to the recipients of hate speech, thereby acting against the interests of recipients in freedom from exposure to this material.

To take another example. Everyone has an interest in lower prices. But a fair and efficient credit system will use personal information to charge higher interest rates for riskier loans, which might violate an information fiduciary's duty to protect a risky individual's interest in obtaining a low-cost loan.

The productive way forward is to focus on ways to allow data flows that generally prevent consumer harm while allowing innovative and beneficial uses of data. As Nissenbaum says, "It's time to stop bashing our heads against a brick wall figuring out how to perfect a consent mechanism when the productive approach is articulating appropriate constraints on dataflow that distributes costs and benefits fairly and promotes the purposes and values of social domains: health, democracy, education, commerce, friends and family, and so on."

NTIA's suggested "outcomes-based approach" seems to embody this forward-looking approach in that it "emphasizes flexibility, consumer protection, and legal clarity can be achieved through mechanisms that focus on managing risk and minimizing harm to individuals arising from the collection, storage, use, and sharing of their information."

SIIA endorses this approach and urges NTIA to expand on it and clarify it as a contribution to the ongoing discussion of national privacy legislation.

Federal Legislation

SIIA endorses national privacy legislation that can provide robust consumer protections throughout the United States. We summarize here our views on what it should contain. The law should:

- Contain a specific declaration that unreasonable or harmful data practices are violations of law.
- Cover notice, control, access, correction, deletion, and portability and should constrain these provisions appropriately so they provide for both privacy protection and innovation.
- Exclude publicly available information such as public records.
- Have an explicit exemption for information about people in their business capacity.
- Be narrowly crafted to protect against substantial harms in order to meet the requirements of the First Amendment.
- Be implemented, interpreted and enforced through the Federal Trade Commission under its existing consumer protection standards and not through private rights of action.
- Cover only types of information and information practices that are not already provided for under sector-specific Federal privacy laws.
- Not contain unrelated provisions such as data sharing that create privacy and security risks.

Provisions of new privacy law: unreasonable use of information

If the purpose of privacy law is to prevent consumer harm in connection with the collection, dissemination or use of personal information through an outcomes-based approach, then one way to accomplish this goal through a new privacy law is through a specific provision that clearly articulates the principle that unreasonable or harmful data practices are violations of law. In particular, the new privacy law should contain a provision declaring that the collection, dissemination or use of personal information that is

unreasonable or harmful is a violation of Section V of the Federal Trade Commission Act banning "unfair or deceptive acts or practices."

In addition, the law could identify some of the consumer injuries that the law seeks to prevent. The harms involved must be real, tangible harms, not theoretical or speculative harms. But what are they? Clearly harms go beyond financial harm but where should the line be drawn?

During her tenure as chair of the Federal Trade Commission, Maureen Ohlhausen identified several types of consumer informational injuries that she extracted from examining cases brought under the FTC's authority to prohibit unfair or deceptive acts or practice. This broad, but determinate notion of informational injury provides a good guide for identifying privacy risks in a new national privacy law.

These informational injuries include deception, financial injury, health and safety injuries, unwanted intrusion, and reputational injuries.

Deception occurs when a company misleads consumers with a materially false claim or omission about a product or service. This injury arises from some, but not necessarily all, failures to notify consumers. The lack of full disclosure constitutes a legal injury when reasonable consumers might have chosen differently if they had fuller information.

Consumers are harmed financially when fraudsters use consumer data to steal money or commit identity theft. Misuse of data can cost consumers loss of time and earnings when they have to report fraud and identity theft and take steps to protect themselves from further losses.

Injuries to health and safety arise in privacy and data breach cases. For instance, the unauthorized disclosure of personal information can expose people to harassment and surveillance from stalkers and abusive spouses. Revenge porn sites often expose their victims to threats and other harassment.

The prevention of unwarranted intrusion into people's private lives was one of the motivations for the FTC's Do Not Call rule, which allowed consumers to opt out of intrusive marketing calls. Similar intrusions can take place through the installation of spyware on computers that enable the recording of users engaged in private activities.

The same abusive conduct that can give rise to these informational injuries can also cause reputational damage. An early FTC online privacy case involved a pharmaceutical company that harmed the reputation of its customers by disclosing online a list of patients using Prozac. The reputational damage from unauthorized disclosure of a person's psychological or medical condition or social activities could lead to job loss.

Many who embrace the notion that privacy rules should protect consumers against harm also want to restrict the notion of harm to economic or tangible harm. But that is far too narrow. Privacy risks go beyond economic losses.

Former FTC chair Tim Muris, a leading proponent of treating privacy as harm-prevention, said at a recent FTC workshop that people have more in their utility functions than money. David Vladeck, former head of the FTC's Consumer Protection Bureau, agreed that the fallout from misuse of consumer information extends beyond economic loss. Both urged the current FTC to issue guidance clarifying that the FTC's

notion of consumer injury for privacy purposes is broader than economic loss and should be understood to include other harms like the invasion of privacy tort.

An FTC guidance document in this area would be helpful, but this understanding of the broader range of harms covered under the notion of informational injury should be incorporated into the new national privacy law.

In addition, the law could contain some specification of the types of acts or practices that constitute unreasonable uses of information, and some safe harbor uses that are determined to be per se reasonable. For instance, the use of information only for advertising that conforms to the code of best practices established by various trade associations and that is used for no other purpose might be deemed reasonable. Similarly, use of information for legitimate scientific research would be reasonable. In contrast, the use of information for identity theft or to commit fraud would be per se unreasonable.

Provisions of new privacy law: notice, control, access, correction, deletion, and portability

SIIA generally endorses the principles articulated by the Internet Association and similar measures proposed by the Information Technology Industry Council.

The Internet Association proposes the following principles:

- **Transparency.** Individuals should have the ability to know if and how personal information they provide is used and shared, who it's being shared with, and why it's being shared.
- **Controls.** Individuals should have meaningful controls over how personal information they provide to companies is collected, used, and shared, unless that information is legally required, or is necessary for the basic operation of the business.
- **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.
- **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 when it's no longer necessary to provide services, except where companies have a legitimate need or legal obligation to maintain it.
- **Portability.** Individuals should have the ability to take the personal information they have provided to one company and provide it to another company that provides a similar service.

ITIC proposes the following principles to guide national privacy legislation:

- **Consent:** Individuals should have the right to expressly and affirmatively consent to the use of their sensitive personal data, unless such use is necessary based on the context or otherwise permitted under applicable law.
- **Access:** Individuals should have the right to access in a timely manner personal data collected from them.
- **Right to Object:** Individuals should have the right to object to the use of their personal data.
- **Accuracy:** Individuals should have the right to rectify, complete, or delete inaccurate or incomplete personal data.

- **Deletion:** Individuals should have the right to have an entity delete their personal data.
- **Portability**: Individuals should have the right to obtain and port personal data they provided to a company across different services.

The Internet Association calls for a risk framework based on the risk of "tangible" harm. SIIA agrees provided the notion of tangible harm is expansive enough to cover the range of information harms identified above, and is not limited to financial harm.

SIIA recommends that the ITI provision on consent be clarified (in red) as follows:

- **Consent:** Individuals should have the right to expressly and affirmatively consent to the use of their sensitive personal data, unless such use is necessary to prevent fraud and illegal activity or is based on the context or otherwise permitted under applicable law.

SIIA recommends that the ITI provision on the right to object be clarified (in red) as follows:

- **Right to Object:** Individuals should have the right to object to the use of their personal data except where companies have a legitimate need or legal obligation to maintain it.

SIIA recommends that the ITI provision on deletion be clarified (in red) as follows:

- **Deletion:** Individuals should have the right to have an entity delete their personal data except where companies have a legitimate need or legal obligation to maintain it.

These recommended clarifications are consistent with the spirit and intent of the ITI proposals.

The provisions related to access and correction are important to ensure that information is accurate and that those who have a bird's eye view of its accuracy, namely the data subjects, have the opportunity to correct errors. However, consumer privacy legislation should not endorse gaming the system or suppressing information needed for important public purposes such as preventing fraud and other illegal activities.

SIIA thinks that any legislative provision related to access and correction should not interfere with the public's right to know legitimate information including information necessary to prevent fraud and illegal activity and should contain specific language to that effect.

The Internet Association and ITI specify that the deletion and portability right should cover information that consumers "provide to companies." SIIA agrees and thinks that the provisions should be further clarified. It should not extend to information that a company has observed about the person while using the service that records transactions with the company or interactions with other users. It should also not include inferred information that the company has created through analytics or information about the data subject that the company has compiled from other sources.

Without these constraints, the portability right could turn into a general right for consumers to take the entirety of the business records of companies with whom they have done business and transfer it to any other company including competitors or information intermediaries who could provide it for sale to interested purchasers. There is no privacy justification for such an expansive data portability right.

Both the Internet Association and ITI call for legislation to provide for data breach notification. SIIA agrees and has supported national data breach notification bills in the past. But it is crucial that the trigger for notification should be a real risk of harm. ITI's language on this point is effective: to require notification only when there is a risk of "concrete and measurable harm" to data subjects or their rights. In addition, a new privacy law should reaffirm and clarify the FTC's authority over information security.

Provisions of new privacy law: Exemption for publicly available information.

The legislation should explicitly exempt publicly available information. The easiest way to do this is through the definition of personal information, making it clear that the term "personal information" does not include publicly available information. For the purposes of the new law, "publicly available" means information that is lawfully made available from federal, state, or local government records, or that is available to the general public. The ITI principles contain such an exemption.

The fundamental reason for this exception is to ensure the continued availability of public records, an open information system that enables a wide variety of publicly beneficial activities.

Public records play a vital role in ensuring that the press can provide citizens with the facts and information they need to be informed citizens, fulfilling Louis Brandeis' dictum for democratic government that "sunlight is the best disinfectant."

These records enable rapid and inexpensive access to credit for consumer purchases and business expansion. They have democratized finance, allowing individuals and small business to demonstrate their credit-worthiness so that, as Fred Cate noted in his 1999 study of the uses of publicly available information, "economic opportunities are based on what you have done and can do instead of who you are and who you know."

National security and law enforcement officials rely on access to public records keep the public safe by tracking terrorists and organized crime figures and to bring to justice perpetrators of everyday crimes.

Companies, government agencies, investors and other institutions need information about individuals in their business capacity and about public companies drawn from public records such as state business registries, filings with the Securities and Exchange Commission, company websites and court documents on liens and bankruptcies to perform essential corporate due diligence, risk management and business intelligence functions.

Public records are used to locate missing family members, witnesses in criminal and civil matters, parents who are delinquent in child support payments, and owners of recalled automobiles.

Businesses use public records to accurately and efficiently identify consumers likely to be interested in a given product or service.

Crucial participants in this information infrastructure are the commercial resellers who invest billions to gather information from open government sources and aggregate it into useable digital files which they maintain, update and make available to the public and institutional customers. It would be as wasteful for news organization, child safety centers, law enforcement, business intelligence services and companies in all sectors of the economy to create and maintain their own public record data bases as it would be for

them to generate their own electricity. They rely on these information intermediaries for accurate, relevant and up-to-date information from public records.

To preserve this open system, the laws governing public access to government information treat pubic release as the default and redaction to protect privacy interests as the exception. For instance, the Federal Freedom of Information Act requires the disclosure of all records other than personnel, medical (and similar files) and law enforcement records whose disclosure would "constitute a clearly unwarranted invasion of personal privacy."

This exemption does not mean that the collection, dissemination and use of data sets that combine private information and public records escape coverage of a new national privacy law. Combining public records with privately assembled information about an individual's behavior in the marketplace and using advanced data analytic techniques can provide detailed individual digital portraits. These merged data sets would be subject to the specific measures in the bill relating to notice, control, access, correction, deletion, and portability and to the general prohibition on the unreasonable use of information.

While merged data sets should be covered under the new national privacy law, the states have not done a good job of providing Congress with models of effective public data governance regimes. The Vermont data broker law, for example, requires companies that collect and use public records to register with the state of Vermont, for no apparent reason or discernible public purpose.

The California privacy law appears aimed at companies that collect information from their customers and then transfer it to third parties, and provides customers with the ability to opt out of such transfers and to access, correct or delete information pertaining to them. But it also extends these rights to public records if the use of the public record data is "not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained."

Unless revised or clarified, this obscure use constraint will almost certainly obstruct valuable public safety uses of public records databases, potentially enabling fraudsters, terrorists and criminals to hide their misdeeds.

One reason to move ahead quickly with a national privacy law is to ensure that these state measures are replaced with equally protective national measures that do not create the same risks of interference with beneficial uses of public records information.

Provisions of new privacy law: Exemption for people acting in their business capacity

Consumers and people acting in their business capacity have very different expectations of privacy. People acting as officers, directors, shareholders or principles of companies and engaged in financial and commercial transactions with suppliers, customers and partners are aware that their conduct is open to evaluation in a public fashion. In contrast, individual consumers are generally interested in engaging in transactions and interactions with others primarily for personal, family or household purposes and assume that these interactions will be subject to some degree of privacy protections.

Moreover, people acting in their own business capacity as economic actors playing important roles in commercial activities have strong expectations that they will be able to learn about the prior business activities of the people with whom they do business or want to do business. They understand that bad business actors have an incentive to conceal their bad behavior, and that a consumer right to privacy

should not be misinterpreted as a right to conceal disreputable business behavior from other commercial actors.

The law recognizes this distinction in some places. For instance, the Uniform Commercial Code at U.C.C. § 9-102(22)-(26) clearly defines consumer goods, transactions and obligations incurred by consumers as related primarily to "personal, family, or household purposes."

However, there is a danger that inadvertently consumer privacy laws could be written that fail to observe a distinction between consumers and people acting in their business capacity. California's Consumer Privacy Act, for instance, defines "consumer" so broadly that it could include individuals even in their business activities. As a result, it might allow fraudsters and other bad actors to opt out of information collection or to delete information about their disreputable business activity, a result clearly not intended by the statute's authors.

To preserve the integrity of business risk assessments, SIIA urges NTIA to adopt a clear distinction between consumer information and information about people in their business capacity. This would continue to allow information service companies to detect individuals with fraudulent pasts or who have acted as a front for illegal activity who would otherwise be able to defraud unsuspecting victims. Making this distinction would further enable companies to satisfy due diligence requirements that are required in the United States and in many jurisdictions around the world. Data relevant to any determination related to potential business fraud or illegal activity should not be subject to consumer privacy provisions for opt-out or deletion.

In particular, NTIA should make it clear that information on credit fraud and publicly available data including suits, liens and judgments should not be included in any opt-out or deletion provision as these are absolutely necessary to ensure an accurate risk assessment to protect individuals and businesses with needed protections against nefarious actors.

A new national privacy law must pass a First Amendment test

In 1997, the Federal Reserve Board told Congress, "It is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy."

The board was especially concerned to preserve the U.S. system of open public records. But the use of personal information raises First Amendment issues generally. Legal scholar Eugene Volokh starkly encapsulated the conflict between free speech and privacy, saying "the right to information privacy-my right to control your communication of personally identifiable information about me--is a right to have the government stop you from speaking about me."

This is not just the opinion of a single law scholar. Under settled Supreme Court case law, most recently the 2011 Sorrell v. IMS case, the collection, dissemination, and use of information, even personal information, is speech and subject to heightened constitutional scrutiny.

The approach SIIA advocates for a new national privacy law of narrowly tailoring privacy rules, especially around public records, to achieve the specific government purpose of protecting consumers from information injuries is not only good policy. It helps privacy law pass First Amendment muster.

In the U.S. system the First Amendment is primary. Its demands must be satisfied before furthering other public policy interests. Privacy law can and should still flourish under this Constitutional system. The Fair Credit Reporting Act, for example, reflects this primacy by allowing companies to share data that they have observed, even though under the Act's provisions this freedom is narrowed by requirements that the data be used for permissible purposes and the rights of individuals to dispute inaccurate information.

The narrow approach SIIA advocates will prevent new privacy rules from running afoul of the First Amendment. An element in a new privacy law that is more restrictive of the free flow of information than is necessary for the achievement of its public purpose of protecting privacy would not pass judicial review.

Federal Trade Commission Enforcement

The Federal Trade Commission has extensive experience in acting to prevent unfair or deceptive acts or practices involving privacy and security. The examples listed above in the section about informational injuries describe the extent to which the FTC has acted in the privacy area. In addition, the FTC has acted over 50 times in the past 20 years against companies whose security practices were unreasonable. This authority was upheld in FTC v. Wyndham, and not significantly weakened in LabMD v FTC, although the latter case suggests some reforms of the FTC's enforcement practice might be needed.

The new national privacy law should reaffirm the ability of the FTC to act in this area, clarifying that unreasonable security practices and data practices are violations of Section V.

In addition, the FTC should have the authority to implement, interpret and enforce the specific measures in the new privacy law relating to notice, control, access, correction, deletion, and portability.

The new law should specifically instruct the FTC to use this new authority to interpret, implement and enforce these provisions under the FTC's existing standards for regulating unfair or deceptive acts or practices. Such a provision would make it clear that the FTC's interpretation, implementation and enforcement of the measures provided for in this new law will be consistent with its existing standards for consumer protection generally. In this way, the FTC would not be free to interpret the measures in the new law as if they are unrelated to its general authority to guard against and remedy unfair and deceptive acts. This provides the needed constraint to ensure that this authority will not be applied in unpredictable and novel ways.

With this level of strong Federal enforcement in place, a general private right of action for individuals to enforce the provisions of the law would not be necessary. By fragmenting enforcement, and subjecting it to myriad court interpretations of the meaning of each provision, private enforcement through litigation would inject uncertainty and unpredictability into the new regime of privacy protection and disrupt business plans and citizens expectations for privacy protection for an indefinitely long transition period.

Incremental Scope of New Privacy Law

SIIA is pleased that the approach outlined in the NTIA request for comment "does not propose changing current sectoral federal laws" which "include, but are not limited to, the Children's Online Privacy and Protection Act, Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), and the Fair Credit Reporting Act."

SIIA strongly encourages NTIA to explicitly add the Family Educational Rights and Privacy Act of 1974 (FERPA) to this list. Its provisions governing privacy for educational records should not be disturbed by any new general consumer privacy law.

These laws have been on the books for decades, have a long history of effective operation and substantial case law and regulatory interpretation to guide the company functions that fall under them. It serves little purpose to open these laws up for potentially radical change. The new privacy law should focus on providing broad coverage of the data practices and activities not already covered by Federal sector-specific privacy laws.

Legislation should not contain measures unrelated to privacy and security

Advocates for reform of the competition laws are turning to other policy areas, including privacy, in an effort to inject competition into markets they perceive as dominated by large technology companies. For instance, Marshall Steinbaum and Maurice E. Stucke say, "In today's data-driven markets, for example, policymakers must consider other laws, like consumer protection and privacy, to promote competition." But this attempt to enlist privacy law to achieve competition policy objectives is mistaken. A new national privacy law should be narrowly focused to protect consumers against harms arising from the collection, dissemination and use of personal information.

Measures designed to promote tech competition might have adverse consequences for consumer privacy or security. Recently, Professor Viktor Mayer-Schönberger and journalist Thomas Ramge proposed that companies above a certain size should be required to disgorge subsets of their data to competitors. Amazon, for example, would be required to make available its sales data so that anyone could create an alternative recommendation engine.

Such a mandatory data sharing suffers from many flaws and should not be incorporated into new privacy legislation for that reason alone. For one thing, it creates substantial privacy risks. If people are willing to share their information with one company, it doesn't follow that they want to share it with all the competitors of these companies. Forced data sharing runs against any notion of effective privacy protection. Companies with data management practices that go above current legal requirements and that many consumers find attractive would be required to pass personal information on to other companies who do the minimum to comply, thereby defeating consumer choice in data protection practices.

Mandated data sharing would create overwhelming disincentives to invest in data base construction. The construction and maintenance of accurate, up to date relevant systems of records is an enormously expensive tasks characterized by steep economies of scale. These data bases are often a treasured company asset, with values at transfer in the billions of dollars. It is hard to see why any company would invest in this effort if the fruit of its work would be immediately made available to all competitors at no or minimal charge.

Myer-Schonberger thinks data sharing is needed to ward off system failures that could arise from centralization. For instance, when one company provides the best recommendation engine that most people want to use, what happens when the service makes a mistake? There's nowhere to go to get an alternative answer that could correct the mistake. The result could be catastrophically misleading search results, consumer recommendations, and news feeds. In addition, centralization could create data

security risks. When one company controls all the data, what happens if there's a security breach? It's a single point of failure that could have catastrophic results for the entire system.

But upon examination these risks are illusory. Forced data sharing doesn't make the data vanish from the original data collector. So whatever security risks were present are still there. And with data sharing, every new entity who receives the original data is a new point of failure.

Moreover, if a company gets its personalized results wrong, consumers don't need to go to a competitor to be informed of the mistake. It's like getting the wrong sized shoe; you know it doesn't fit because it hurts. So, what happens with personalization mistakes? You don't read the suggested article, you don't buy the recommended product and you don't click on the proffered search results. And the algorithm learns from that and tries to get it better next time.

If it doesn't, then there are alternatives. Perhaps the biggest blind spot in the centralization argument is the idea that the large tech companies have no competition at all, as if Amazon doesn't have competitors like Wal-Mart, Facebook doesn't have competitors like Snapchat, Twitter and LinkedIn, and Google doesn't have competitors in search like Bing, DuckDuckGo, Yelp, and Travelocity and competitors in advertising such as Facebook and Amazon. Systematic, regular and widespread failure of these services would not be catastrophic except for the companies themselves, who would immediately see their market share eroded as people exit in mass to these alternatives.

The existence of these competitive alternatives suggests that data sharing, with its substantial flaws for other policy objectives, should be considered as a competition policy tool only with substantial proof of anticompetitive conduct, and only after less draconian measures have been determined to be ineffective in protecting consumers from this conduct.

But regardless of its merits, data sharing is not a measure designed to advance the privacy interests of consumers. It is intended as a solution to perceived competition difficulties. Even if it could, somehow, be freed of its difficulties for privacy, security and innovation incentives, it belongs in a separate measure aimed at promoting competition policy objectives, not in a new national privacy law.

Conclusion

SIIA appreciates the opportunity to comment in this important proceeding and encourages NTIA to move forward with its own recommendations for national privacy law. The support of the Administration in pursuing new privacy legislation will be an important element in reaching the critical mass needed to move legislation through Congress next year.