Discussion Points in Preparation for Drafting Federal Legislation Called

The Individual Privacy Act

Prepared by

May 2019, updated August 2021

Contents

BACKGROUND

As an alliance of charities and service providers to charities, members of The Nonprofit Alliance care about people. Our member charities care about and help people in need, care about our environment, and care about important issues in our culture. Caring and helping is what we do. Members of The Nonprofit Alliance devote their life and career to helping. We find cures for dread diseases, help underprivileged children, preserve natural habitats, protect wildlife, house and clothe people worldwide, rescue abused animals, feed the hungry, and care for our injured veterans. Basically, we do good things that need to be done.

Caring about people in an additional way, by protecting their Sensitive Personal Information, fits perfectly with who we are. In fact, nonprofit organizations rely on outreach to individuals and households for mission awareness. Public trust is foundational to nonprofits' ability to raise funds and provide vital services.

The critical function of consumer personal data in the American economy cannot be understated, yet the growing volume of personal data in Americans' lives has greatly increase the risks to individual privacy. The Nonprofit Alliance calls on Congress to enact a robust, national privacy statute providing uniformity for all parties' expectations to protect donors and allow for the legitimate use of data for public education and fundraising purposes.

The Nonprofit Alliance's efforts on Capitol Hill have been both bipartisan and bicameral, working with members of Congress toward enacting a comprehensive privacy statute. Passing such a statute is no small task. However, the urgency for such legislation becomes more evident every year, with additional states passing their own privacy statutes in the absence of a federal solution. The result is a growing patchwork quilt of various an inconsistent state privacy laws.

Our position: One clear national standard for data collection and use would best serve both consumers and nonprofit organizations.

The Nonprofit Alliance believes that among the critical elements of a national privacy statute are:

- A uniform set of national standards and guidelines to create a clear, consistent framework for the handling of data, rather than varying requirements from state to state.
- A clear preemption of any current or future state privacy statutes outside of areas historically regulated jointly by the states and Congress, e.g., education or medical.
- An consistent national consumer privacy choice framework, with clear and accessible disclosure and control for consumers, reasonable compliance requirements, and accountability.
- A reasonable framework for applying higher levels of restriction to data historically considered as highly sensitive in the United States, including protected health information as defined by HIPPA, information related to children defined by COPPA, financial account numbers and access codes and social security numbers and other unique government-issued identifiers.
- A requirement that litigation relative to a federal privacy statute be filed in federal court to provide greater national uniformity of enforcement.
- Exclusion of a private right of action, which would result in a proliferation of lawsuits, many of which would be designed not so much to vindicate rights, but rather for attorneys, rather than

consumers, to profit from litigation. For the many nonprofits and small businesses with limited legal resources, their mission effectiveness – or even existence – would be under constant threat.

- Compliance and enforcement residing in the Federal Trade Commission, which has a long history of assertive and balanced enforcement under both Democratic and Republican administrations.
- Differentiation between the few big tech companies and the many other businesses and nonprofit organizations that collect and use data. Legislation written with big tech primarily in mind will likely overreach and/or overburden the vast majority of entities that will be expected to comply, and will likely serve to further entrench massive companies that can afford expensive regulatory burdens and legal risk.

It has been, and continues to be, the goal of The Nonprofit Alliance to work with Congress to help in the effort toward enactment of a comprehensive national privacy statute.

INTRODUCTION

There is wide variance in individual opinion concerning regulation of personal information.

1. Polar View 1: No New Law or Regulation. Some individuals are unconcerned or have little or no concern about privacy. They express their opinion with phrases such as, "I have nothing to hide," or "It's a data world. Everyone knows everything about everyone. That's fine with me."

2. Polar View 2: Ban Use of Data. Other individuals are very concerned. They express their opinion with phrases such as, "My information is my business, and no one else's business," or, "No one should keep track of anything about me."

3. The Wise and Prudent View. The vast majority of individuals do not hold either of the Polar Views. Instead, they believe that Sensitive Personal Information should be well-protected and that other information should be used appropriately to benefit society and individuals.

Congress should not ignore the privacy topic because of Polar View 1. Similarly, Congress should not adopt excessive measures in reaction to Polar View 2. As is often the case with legislation, arriving at the right mix of restriction and free enterprise should be the goal.

The first step toward adoption of a new Individual Privacy Act is to understand the topic and its many implications. One aspect of attaining such understanding is to consider both Individual Privacy Interests and Societal Interests.

Balancing Analysis Is Required

Any federal privacy law should determine what specific protections are necessary for particular uses of personal information[1] based on a well-reasoned Balancing Analysis that takes into account two categories of interests.

[1] When this policy statement refers to personal information, it should be considered in the context of the party who has access to that information. If that party associates information with an identified individual or could reasonably do so, the information would be considered

1. Individual Privacy Interests. An individual's interest in his/her own privacy and autonomy and in being treated fairly.

2. Societal Interests. The interest of society in supporting charitable causes, safety, innovation, economic growth and opportunity, robust competition and other such interests held by society as a whole.

Individual privacy interests and societal interests must be viewed relative to one another to determine the appropriate protections, almost as if individual privacy interests were on one side of a scale and societal interests were on the other side of the scale. For example, an individual's interest to protect personal financial information from disclosure is valid, but the need of the government and financial institutions to detect fraud is also valid. As we evaluate the relative balance of the scale, we can better determine the protections that are appropriate to preserve individual privacy interests while fostering societal interests.[2]

Neither category of interest is preeminent. Inappropriate deference to individual privacy interests could harm many other individuals that comprise society. Similarly, societal interests cannot completely control policy without regard to an individual's interest, because society itself is made up of many individuals, and can only thrive where individuals have reasonable protection of their privacy interests.[3]

For example, undue restriction of charities, working with their critical for-profit service providers, to contact individuals to request a donation or to use data to more effectively accomplish their mission would clearly harm their ability to feed the hungry, protect our environment, cure dread diseases, help sick children, house and cloth people worldwide, rescue abused animals and increase global quality of life. Similarly, undue restriction of businesses to announce new products, conduct product research, and promote their product or service to individuals likely to be interested would

---

personal information. The Individual Privacy Act should be written to encourage organizations to reasonably de-identify information so that it is not associated with an identified individual, but is instead associated with a "de-identified" profile or unique ID (we refer to this type of information in this policy statement as de-identified information). Where an organization institutes and can demonstrate that it does not associate particular information with a specific identified individual, whether enforced through technological measures or organizational policies (or both), it would be appropriate in many cases not to consider that information personal information. In situations involving data that would otherwise be sensitive personal data, third party verification such as through an appropriate seal program or through detailed internal analyses by the organization that can be demonstrated to a third party if concerns arise would be a method to help ensure appropriate procedures are actually being followed that protect Individual Privacy Interests.

[2] See comments from the Information Accountability Foundation dated November 6, 2018, which were provided to the National Telecommunications and Information Administration in connection with the Administration's request for public comments entitled "Developing the Administration's Approach to Consumer Privacy." http://informationaccountability.org/wp-content/uploads/Information-Accountability-Foundation-Filing.pdf These comments contain helpful discussion on balancing individual and other interests and how that has been achieved in historical U.S. privacy laws like the Fair Credit Reporting Act.

[3] The Bill of Rights in the U.S. Constitution is a clear recognition of the critical role individual rights play in a vibrant democratic society.

[4] Recent experience in Europe is instructive. A number of U.S. companies, many of which are small to medium sized businesses, have pulled out of Europe because of the vague requirements and threat of liability that is outsized to the business they conduct. Examples:

1. https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04
2. https://www.fastcompany.com/40578069/these-popular-sites-are-dark-in-the-eu-thanks-to-gdpr
3. https://digiday.com/media/impact-gdpr-5-charts/

drive companies out of business and generally harm innovation, the economy and the choices available to individuals.

On the other hand, allowing unrestricted use of personal information to accomplish an objective could lead to extreme individual concern, doubt and harm. For example, enabling any person to have access to medical information might lead some researcher to find the cure for a horrible disease, but it could also expose individuals to embarrassment and decrease their likelihood of seeking medical care, which is why U.S. law has for many years treated this information as sensitive and subject to specific protections.

Another critical consideration is that an unduly burdensome set of protections relating to use of personal information would inevitably result in decreased competition and innovation. Huge companies would have sufficient capital to comply, but smaller, newer companies, which are frequently the ones to bring groundbreaking new products to market, could not. [4]

This policy discussion seeks to provide well-reasoned suggestions for how legislators should view the individual privacy topic and what protections should be imposed in order to promote the common good without undue burdens or harm.

Impact Determined By Data Type and Benefit to Society as a Whole

The degree to which Individual Privacy Interests are impacted by use of personal information depends on the type of data involved and the type of use being made of the data. When data that most individuals would consider sensitive is used, the potential impact to individual privacy interests is highest and the Individual Privacy Interest weighs heavily on the scale. Conversely, as less sensitive data is used, the potential impact to individual privacy interests is lowest.[5]

The degree to which Societal Interests should be considered depends primarily on the importance of the Societal Interest to society as a whole. Societal Interests such as public safety, fraud prevention, law enforcement, and the ability to accomplish economic transactions are so critical to society that they weigh very heavily on the scale. Similarly, many uses of data may have benefits to society, but they may not be as critically important as those mentioned above; they still should be accounted for in determining the right mix of protections.

---

[5] Our framework focuses on the expanded protections that are appropriate for personal information based on whether the information itself is Sensitive Personal Information or Other Personal Information. The Balancing Analysis in the context of **sensitive uses** of information has long been reflected under existing U.S. privacy laws and is not separately addressed in our framework, and the concept should be preserved through existing laws. For example, any kind of personal information when assembled and used for credit, housing, employment or insurance decisions is considered a "consumer report" under the Fair Credit Reporting Act (enacted in 1970) (FCRA). Because Individual Privacy Interests are significantly impacted by these types of decision (most people would agree they are sensitive uses), Expanded Transparency, Individual Input and Accountability are required for this type of use. However, to protect the Societal Interest of being able to extend credit, not all types of Expanded Protection are available. For example, an individual may not request full deletion of their data (other than inaccurate data) and the individual's affirmative consent is not required for data to be used in this manner. Similarly, laws like the Fair Credit Reporting Act, Equal Credit Opportunity Act and the Fair Housing Act already include expanded protections in decisions regarding credit and housing, the Genetic Information Non-Discrimination Act of 2008 prohibits discrimination in employment or insurance on the basis of genetic information and CAN SPAM and associated rules require specific protections in the context of sending email.

One area that is often misunderstood and frequently taken out of context concerns personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sexual orientation, or citizenship or citizenship status.

The critical standard, which puts this issue in proper context, is in how this data being used. For decades, the United States has prohibited discrimination on the basis of protected class and restricted the use of these types of data for decisions relating to credit, housing and employment, under the FCRA. But at the same time, this data has commonly been used in marketing and nonprofit outreach efforts for affirmative efforts to reach the consumers most likely to be interested in a product, service or cause. The types of heightened restrictions, like those represented by FCRA, should only apply when this type of data is used to make decisions that produce legal or similarly significant effects concerning a consumer.

Accordingly, this standard properly protects consumers against discrimination, while allowing the flow of information vital to organizations to connect with consumers having a religious affiliation, ethnic origin, or other criteria that make them most likely to be interested in a particular message or offer. For example, a religious organization seeks to provide information to, or solicit donations from, other members of its faith. Here the intent is clear – to find people of a particular religious belief or denomination and effectively communicate with them for the betterment of the group. Again, there is absolutely no motive to discriminate or harm anyone through the use of data in this manner.

PROPOSED PROTECTIONS

We propose four general types of protections: Transparency, Individual Input, Accountability and Prohibition. The specific protection chosen for a particular data type or data use should be established based on the Balancing Analysis described above. Each type of protection can range from very basic to very expansive, depending on the Balancing Analysis. Basic protections are generally appropriate for non-sensitive types of personal information. Expansive protections are generally appropriate for sensitive types of personal information. Limited protections are appropriate when critical Societal Interests are involved. Within each category of protection, different mechanisms may be best for achieving the right balance in different circumstances, and not every mechanism is appropriate for every type of personal data. The requirements of the Individual Privacy Act should be carefully crafted to ensure the mechanisms prescribed seek to achieve that balance.[6]

Transparency

Transparency deals with the extent to which an organization must disclose to individuals the nature and extent of personal information being used and type of use. Transparency protects individual privacy interests in several ways. It gives individuals confidence about where "private" spaces in life can be found, thus encouraging free expression and a sense of autonomy. It also bolsters the effectiveness of other types of protection. It gives individuals a method to exercise any Individual

[6] For example, for some types of Sensitive Personal Data, Expanded Transparency through government registration may not properly protect Individual Privacy Interests while fostering key Societal Interests, and instead Expanded Transparency might better be achieved by requiring specific disclosures to be made to consumers or regulators by the organization using the Sensitive Personal Information.

Input and makes it more likely that organizations will act in an accountable manner when using personal information.

Basic Transparency applies to use of non-sensitive data. Basic Transparency requires:

1. That an organization publicly discloses the general types of personal information it uses and ways it uses the data, and that upon request from an individual, the organization provides the same information to that individual. The disclosure is general rather than specific because the burden of specific disclosure on small companies would be disproportionate for these non-sensitive types of data and data use.

2. That, at the time an organization collects personal information from an individual, the organization discloses to the individual the personal information it collects, how it uses the data, and the third parties with whom it shares the data and for what purpose.

3. That, upon request, an organization discloses to an individual the specific data that the individual has submitted to the organization and how it is used.[7]

Expanded Transparency applies to use of sensitive data. Expanded Transparency requires, in addition to Basic Transparency, that, upon request, an organization also discloses to an individual any other specific personal information the organization has about the individual.

Individual Input

Individual Input deals with enabling an individual to impact whether, how and by what organizations their personal information is used.

Basic Individual Input applies to use of non-sensitive data. This may include:

1. Allowing an individual to opt out of a particular use of the individual's personal information.

2. Allowing an individual to correct information the individual provided to the organization.

3. Requiring that an individual be able to instruct an organization to discontinue use of the individual's personal information.

Expanded Individual Input applies to use of sensitive data. This may also include, in addition to Basic Individual Input:

[7] In this proposal, where an individual is allowed to request that an organization disclose information about that individual, the concept of a "verified request" is assumed. This means that the organization requires the individual to prove in a reasonable manner that the individual is who the individual alleges to be. Organizations should be given latitude to require sufficient verification of identity. To do otherwise would actually harm privacy by augmenting the risk of disclosing data that actually pertains to another individual. The Individual Privacy Act will include guidelines that describe the parameters of how verification will work. It will be a risk based approach in that the level of verification required for disclosure of Sensitive Personal Information may be much higher than the level of verification required for Other Data.

1. Requiring affirmative, specific consent of an individual to use personal information in a particular way.

2. Providing a neutral forum, such as a well-respected third-party industry group, for an individual to object to use of the individual's data or to request correction or modification of the data. However, in cases where existing laws such as HIPAA[8] assign responsibility to another entity, individuals will continue to register their complaints to the entity specified within that law.

Accountability

Accountability means ensuring that organizations using personal information develop appropriate internal standards for such use. Accountability also means that organizations, where appropriate, are subject to and honor standards created by external groups.

Basic Accountability applies to use of non-sensitive data. This may include:

1. Establishing an internal function that is tasked with ensuring that uses of personal information are understood, documented and reviewed periodically.

2. Ensuring that corrective actions are taken when necessary to appropriately enforce internal standards.

3. Establishing appropriate security policies and practices.

4. Aligning internal policies to externally created standards such as those required by law or promulgated by industry self-regulatory groups.

5. Being capable of demonstrating to regulators the organization's accountability mechanisms and their effectiveness.

Expanded Accountability applies to use of sensitive data. This may include:

1. Mandatory disclosures, certifications or seal programs where an organization's internal policies are aligned with and measured relative to an externally developed standard; or specific, detailed internal analyses of how Individual Privacy Interests and Societal Interests are balanced through the organization's policies and processes can be disclosed upon request to a third party.

2. Requirements for external audits of organizational security according to third party standards (for example, privacy or security standards such as those promulgated by NIST, ISO, etc.).

[8] The Health Insurance Portability and Accountability Act of 1996. References in this policy statement to HIPAA also refer to subsequent amendments or companion laws and regulations like The Health Information Technology for Economic and Clinical Health Act (HITECH).

3. Registration with a government or industry self-regulatory body.

Prohibition

In some cases, the balance of high Individual Privacy Interests relative to much lower or non-existent Societal Interests may require prohibiting specific types of use.

SENSITIVE PERSONAL INFORMATION REQUIRES EXPANDED PROTECTIONS

When Sensitive Personal Information is involved, significant weight must be given to Individual Privacy Interests. In all cases, except to the extent that the Balancing Analysis indicates that Societal Interest justifies an exception, Sensitive Personal Information requires Expanded Transparency, Expanded Individual Input and Expanded Accountability. In some cases, Prohibition may apply. We must look to the type of use involved to determine whether a countervailing Societal Interest exists that would suggest lesser protections are appropriate.

"Sensitive Personal Information" Defined; Permitted and Prohibited Uses Specified

Sensitive Personal Information is defined to include specific types of information, as set forth below. Permitted and Prohibited uses of Sensitive Personal Information are specified.

1. Hospital, Doctor, and Other Health Care Provider and Health Insurance Records: this is inclusive, covering all hospital, doctor, and other health care provider and health insurance records, including therapy or other sessions with non-medical staff. Absolutely all such information, whether it is prescriptions written, health conditions diagnosed, illnesses treated, genetic information, medical claims submitted or paid, or other information from health provider or health insurance files, charts, databases, or other records, is Sensitive Personal Information. This is essentially co-extensive with current HIPAA definitions of "Protected Health Information."

    a. Permitted Use: HIPAA provides for Expanded Transparency, Individual Input and Accountability. Use in accordance with HIPAA and related laws and regulations is permitted. Because of the critical Societal Interest in conducting health research, allowing use of this type of data for research when Expanded Transparency and Input are provided to the individual is appropriate. In addition, when the data has been anonymized according to HIPAA standards, it would not be considered Sensitive Personal Information.

    b. Prohibited Use: Use that does not meet the requirements above is illegal. It is also illegal to make materially inaccurate statements or to omit material information required to make a statement, taken as a whole, not misleading, in the context of Transparency or Individual Input.

2. Medical and Health Information Other Than Hospital, Doctor, and Other Health Care Provider and Health Insurance Records: It is technically possible to collect and utilize medical and health information about an individual using online search terms, browsing behavior, text of email messages, listening devices, direct mail surveys, use of

over-the-counter genetic and health predisposition tests, or other methods. Regardless of the source or method, individually identifiable information of this type is Sensitive Personal Information. Information that is maintained in de-identified or summarized form (and when summarized, if summarized to a level that includes 100 or more individuals), is not Sensitive Personal Information.

a. Permitted Use: Expanded Accountability and Transparency apply. This data must be maintained in a secure, private manner and must be disclosed to the individual upon request. Sensitive Personal Information of this type may be utilized by the original party who received or obtained the data for the sole purpose of interacting with or responding to the individual to whom the information applies. Only with Expanded Individual Input and Transparency may it be used for any other purpose. Such Expanded protections must include very specific, clear, express consent by the individual to a specific use by a specific party and the right to access and require deletion of the data.

b. Prohibited Use: Use that does not meet the requirements above is illegal. It is also illegal to make materially inaccurate statements or to omit material information required to make a statement, taken as a whole, not misleading, in the context of Transparency or Individual Input.

3. Data Held by Financial Institutions: Data relating to a financial product or service received, generated or held by a financial institution. This is essentially co-extensive with current definitions of "Nonpublic Personal Information" and the Gramm-Leach-Bliley Act (GLBA).

a. Permitted Use: GLBA and associated rules pursuant to the Dodd-Frank Act provide for Expanded Transparency, Individual Input and Accountability. Use in accordance with GLBA/Dodd-Frank and related laws and regulations is permitted.

b. Prohibited Use: Use that does not meet the requirements above is illegal. It is also illegal to make materially inaccurate statements or to omit material information required to make a statement, taken as a whole, not misleading, in the context of Transparency or Individual Input.

4. Financial Account Numbers & Government Identity Numbers: Social Security Numbers, Credit/Debit Card Numbers, Medicare Account Numbers, Driver's License Numbers, Bank Account Numbers, Investment Account Numbers, Retirement Account Numbers, Loan Numbers, and other financial account numbers are considered to be Sensitive Personal Information, and in many cases, they are held and used by organizations other than the financial institutions discussed above.

a. Permitted Use: Expanded Accountability and Transparency apply. Any company or organization may store Financial Account Numbers and Government Identity Numbers in a secure environment and for the sole purpose of using them in normal course of its own relationship with these individuals.

Significant Societal Interests exist to have widespread access to credit, convenient, efficient payment systems and to detect and reduce fraud. Therefore, government entities and companies that are authorized to do so under federal law, such as under the Fair Credit Reporting Act, may receive Financial Account Numbers from any legitimate source and may store, process, and use them in a secure, private environment to verify individual identity and to provide services to banks, credit unions, and other financial institutions that have good standing under a federal or state charter or other license. However, Expanded Transparency applies, and, upon request, the organization must disclose to the individual this information.

Companies involved in payment processing, including but not limited to companies such as Visa, MasterCard, and Discover, may receive Financial Account Numbers from an entity to which payment is due, and may store, process, and use the Financial Account Numbers in a secure, private environment as required to provide their service. However, Expanded Transparency applies, and, upon request, the organization must disclose to the individual this information.

b. Prohibited Use: Use that does not meet the requirements above is illegal. It is also illegal to make materially inaccurate statements or to omit material information required to make a statement, taken as a whole, not misleading, in the context of Transparency or Individual Input.

5. Signatures: All signatures, other than those distributed for commercial purposes (e.g. signed memorabilia) regardless of whether the signature is on paper, digital, or in some other form, are considered Sensitive Personal Information.

   a. Permitted Use: Expanded Accountability applies. The company or organization to which an individual provided a signature may use it and retain it on file in a secure environment. Significant Societal Interest exists in fraud prevention and detection and for verification of contracts as part of financial evaluation/audit procedures. Therefore, signatures may be disclosed to qualified auditors, regulatory bodies, stock exchanges or service providers who use and retain the signature in a secure environment and use it for fraud prevention and detection and for verification of contracts as part of financial evaluation/audit procedures. Expanded Individual Input is limited, because an individual cannot be allowed to require deletion of this information as that could eliminate the ability to verify contracts, etc.

   b. Prohibited Use: Use that does not meet the requirements above is illegal. It is also illegal to make materially inaccurate statements or to omit material information required to make a statement, taken as a whole, not misleading, in the context of Transparency or Individual Input.

6. Biometric Data:

   a. Permitted Use: Significant Societal Interests exist for using biometric data in new ways. With the advent of new biometric technologies, individuals are using their fingerprints or eyes to unlock devices, enter their homes or authenticate themselves with organizations more quickly and securely. Facial recognition software can be

used to prevent fraud and protect public safety. However, the voluntary submission of biometric data by individuals for specific purposes has outpaced laws that protect against inappropriate uses or misappropriation of biometric data. Significant Individual Privacy Interests exist because misused or stolen biometric information can transform the promised increases in security into a conduit for theft or fraud, and unlike other authentication mechanisms like a password or PIN, it is no simple matter to "reset" biometric data. Expanded Transparency, Individual Input and Accountability apply. Use of biometric data is permitted solely to perform the action for which the data was submitted by the individual (such as storing and using biometrics voluntarily submitted by an individual for authentication of identity). Expanded Transparency and Individual Input through clear, specific consent of the individual to a clearly specified use of biometric data are appropriate in most situations. In some cases, Societal Interests may necessitate less Transparency or Individual Input. For example, public safety or anti-fraud uses of biometric data may not always allow for Individual Input through prior consent, but, in such cases, Expanded Individual Input may be necessary to allow an individual to object to misidentification. Regardless, Expanded Accountability is critical in nearly every case to ensure this information is adequately protected.

b. Prohibited Use: Use that does not meet the requirements above is illegal. It is also illegal to make materially inaccurate statements or to omit material information required to make a statement, taken as a whole, not misleading, in the context of Transparency or Individual Input.

7. Private Video Rental/Viewing: This includes traditional video rental as well as online video streaming.

a. Permitted Use: The Federal Video Privacy Protection Act (the VPPA) provides for Expanded Transparency, Individual Input and Accountability. Use in accordance with the VPPA is permitted. This includes provisions for allowing sharing of video rental/viewing with social media and other sources when the individual provides express consent.

b. Prohibited Use: Use that does not meet the requirements above is illegal. It is also illegal to make materially inaccurate statements or to omit material information required to make a statement, taken as a whole, not misleading, in the context of Transparency or Individual Input.

8. Precise Location Information:

a. Permitted Use: Expanded Transparency, Individual Input and Accountability apply. Significant Societal Interests exist in encouraging innovation in the use of geolocation information because it can significantly impact public safety (warning individuals of natural disasters or safety hazards, providing the fastest routing for emergency responders, locating missing loved ones, etc.), the ability to accomplish charitable outreach (e.g., connecting with isolated senior citizens, hungry families or those who may benefit from another type of aid), increasing economic efficiency (allowing businesses to significantly reduce prices by optimizing routing both in

delivery of goods and services and foot traffic within retail locations, delivering goods to the consumers who want them at the lowest price by allowing businesses to optimize decisions on where to invest in retail expansion, providing consumers with better pricing based on their likely proximity to locations where they may desire to purchase a good or service, etc.). And yet, geolocation information could also be used in many ways that significantly harm Individual Privacy Interests.[9] Use is permitted when solely to give effect to an individual's request (such as precise location to pick up a passenger who requested a ride through a smartphone app) or when in accordance with a specific disclosure given to and accepted by an individual (such as an app downloaded for the primary purpose of receiving location-based discount offers could then utilize the individual's location to provide these offers). The Individual Privacy Act should also encourage and allow expanded uses where geolocation information is maintained in de-identified form, because this has the capacity to greatly reduce the risk to Individual Privacy Interests while enabling many Societal Interests. In these cases, Expanded Transparency or Individual Input may not be needed and Basic Transparency and Individual Input may be appropriate. For example, a retail store could use beacon, WiFi or cellular based anonymous routing to analyze traffic patterns and improve consumer experience in the store and disclose this on its website or through signs in the store. However, due to the very sensitive nature of geolocation information if associated with a specific individual, Expanded Accountability should still be required to ensure that this information remains de-identified (in particular, seal programs and mandatory verification from a highly reliable, independent third party or the requirement to create detailed internal organizational analyses that are demonstrable to a third party, if concerns arise, could be particularly useful in this context to certify both the party gathering the information and any party receiving the information, thus establishing a "trusted ecosystem" of users of de-identified geolocation information).

b. Prohibited Use: Use that does not meet the requirements above is illegal. Making materially inaccurate statements or omitting material information required to make a statement, taken as a whole, not misleading, in the context of Transparency, Individual Input or Accountability is illegal.

9. Verbal Communications Collected by any Connected or "Smart" Device[10]:

a. Permitted Uses: Technology is moving extremely fast and does not easily lend itself to traditional privacy rules dealing with written communications/data. Accordingly, Expanded Transparency Individual Input and Accountability are absolutely critical.

[9] The U.S. Supreme Court noted in *Riley v. California (2014)*, that geolocation information combined with information that identifies a person such as the person's name and likeness, when done at the scale that is possible through modern mobile devices, can allow "the sum of an individual's private life" to be reconstructed.

[10] There are sometimes debates about the extent to which a device is a "smart" device or "connected" device. See the definition and discussion regarding "Connected Devices" in the Data & Marketing Association Guidelines for Ethical Business Practice, 2017 at https://thedma.org/accountability/ethics-and-compliance/dma-ethical-guidelines/. For purposes of this item, the key features of a device discussed in this item is that it can observe and respond to verbal commands and has the ability to interact or respond to those demands through a remote service such as via the internet. Personal assistant devices like Amazon Alexa enabled devices, Google Home devices, smart televisions and the like are intended to be covered by this item.

Significant Societal Interests exist in encouraging the availability of voice enabled devices to benefit public safety (e.g. use in cars to allow drivers to obtain directions while keeping eyes on the road), allow for enhanced group interactions, assist those with disabilities to gain independence, decrease isolation of the elderly or help enable less technically savvy individuals to benefit from access to the vast information on the internet.[11] Significant Individual Privacy Interests also exist because these devices are frequently found in spaces considered to be private, such as homes or automobiles, and in theory they could be used to observe every private conversation in those spaces. Use is permitted when solely to give effect to an individual's request (such as responding to a voice activated information request or setting and providing a reminder requested by an individual). Given the sensitive spaces in which these devices are often operated, it is critical that the Individual Privacy Act encourage and require practices that limit access to the substance of private conversations. For example, in order to create and improve these types of devices, it is often necessary to utilize real-world conversations to troubleshoot and perform quality assurance, which is permitted, but organizations should use Expanded Accountability mechanisms like data minimization and de-identification to greatly reduce any risk of private discussions being disclosed on an identifiable basis. Expanded Individual Input may need to take a form other than individual consent for these types of devices.[12]

b. Prohibited Uses: Association of recordings or transcripts of private conversations with specific individuals is illegal unless for user support with the express consent of at least one party to the conversation (such as when a device owner calls for technical support regarding a potential malfunction of the voice activated technology and requests that a technician review a transcript to identify whether a product was ordered or not). Disclosure of recordings or transcripts of private conversations observed by these devices is illegal. Making materially inaccurate statements or omitting material information required to make a statement, taken as a whole, not misleading, in the context of Transparency, Individual Input or Accountability is illegal.

10. Information Collected via Web Browsers, Mobile Applications, and Other Technology-Enabled Means:

a. Permitted Uses: Significant Individual Privacy Interests exist. The internet has opened a new chapter in human interaction, free speech and the spread of knowledge and ideas. Allowing for a private space for web browsing and apps encourages individual curiosity and learning and individual self-expression,

[11] There are numerous articles documenting some positive impacts voice enabled devices provide to various constituencies in society. https://medium.com/vui-magazine/the-societal-benefits-of-smart-speakers-274073cfe7ae. https://www.aarp.org/home-family/personal-technology/info-2018/isolation-loneliness-technology-help.html

[12] Consent may be a misaligned Individual Input mechanism for this type of data. For example, in many cases, these devices must "listen" for commands from users actively all the time in order to fulfill their intended functions. But many users of the device may never have participated in the purchase or activation of the product or had opportunity to be presented with any type of Transparency disclosure (how many of us have asked Alexa or Google a question at a friend's residence?). In fact, many guests whose voices may be picked up by device microphones may not be aware there is a product of this nature in the space at all.

especially of those who need to connect to individuals outside their physical community to have any realistic opportunity of achieving these outcomes. However, the mere presence and availability of much of the free internet that enables this access is largely based on the ability of publishers to sell advertising that is best suited to the interests of the website visitors or app users. Use of individual identity associated with web browsing or app use behavior is permitted solely within and for the internal purposes of an organization when an individual has submitted the individual's identity to the organization through the web browsing or app behavior (such as by entering the information in a signup or survey form and affirmatively submitting it). For example, the organization may use this information to cultivate a relationship with the individual or improve its products. However, Expanded Transparency, Expanded Individual Input and Expanded Accountability would be required to disclose personal information together with web browsing behavior or mobile app usage to third parties or to associate web browsing behavior or app usage behavior with personal information of individuals who have not affirmatively submitted their personal information to the organization. The Individual Privacy Act should also encourage and allow expanded uses where web browsing or app usage behavior is maintained in de-identified form, because this has the capacity to greatly reduce the risk to Individual Privacy Interests while enabling many Societal Interests. In these cases, Expanded Transparency or Individual Input may not be needed and Basic Transparency and Individual Input may be appropriate. For example, websites may be able to effectively serve relevant advertising based on a de-identified or anonymized individual profile that can be kept completely separate from the individual's identity. However, Expanded Accountability should still be required to ensure that this information remains de-identified (in particular, seal programs and mandatory verification from a highly reliable, independent third party or the requirement to create detailed internal organizational analyses that are demonstrable to regulators could be particularly useful in this context to certify both the party gathering the information and any party receiving the information, thus establishing a "trusted ecosystem" of users of de-identified geolocation information).

b. Prohibited Use: Use that does not meet the requirements above is illegal. Making materially inaccurate statements or omitting material information required to make a statement, taken as a whole, not misleading, in the context of Transparency, Individual Input or Accountability is illegal.

11. Data about Children: Our children are precious. Protecting them as best we can during their formative years should be a primary objective.

a. Permitted Uses: COPPA[13], FERPA[14] and the PPRA[15] already provide Expanded Transparency, Individual Input and Accountability in the context of online services directed to children and students' educational records, respectively. They should remain in place, unaltered. Significant Societal Interests exist in providing children with access to educational opportunities. Significant Individual Privacy Interests also exist in allowing parents to protect and guide access to the personal data of their children and preventing children from being harmed by contact with unscrupulous parties or inappropriate content. One key topic that is addressed by existing law and should be considered in the Individual Privacy Act is that different protections may be appropriate for different ages of children. For example, COPPA deals with children under the age of 13, and FERPA and the PPRA provide different protections for data as children approach and reach age 18. In general, advertising directed to individuals known to be children under the age of 18 should not be permitted without an Expanded Individual Input mechanism that allows parents to provide the consent. One exception would be advertising by accredited educational institutions and branches of the military directed to children believed to be over the age of 16, in order to encourage children to explore opportunities for post-secondary education. Other appropriate exceptions may exist. In any case, Enhanced Accountability is required to protect the data of children with appropriate security.

b. Prohibited Uses: Advertising to or selling[16] the data of individuals known to be under the age of 18 is prohibited in the absence of express parental consent to a specific category of advertising. It is prohibited to use the data of children for purposes of promoting pornography or any category of product for which marketing to children is currently prohibited by law. Making materially inaccurate statements or omitting material information required to make a statement, taken as a whole, not misleading, in the context of Transparency, Individual Input or Accountability is illegal.

12. Personnel Records of Employers: Employers are required by law to document certain information, including wages and hours, tax withholding, benefits, and workplace injuries and illnesses. There is currently no federal law governing personnel files. Some states legally allow employees to view or copy portions of their personnel records, including performance reviews and documentation of promotions and salary adjustments. However, the employer does not generally need to disclose letters of reference from former employers, test results, or records of an investigation into criminal conduct or violation of workplace rules.

[13] The Children's Online Privacy Protection Act.

[14] The Family Educational Rights and Privacy Act of 1974.

[15] The Protection of Pupil Rights Amendment.

[16] The prohibition would include sharing identifiable children's data with third parties when the sharing allows a third party to use it for its own purposes. This is contrasted with a situation where an organization merely engages a third party to perform services on the organization's behalf without any right to use identified data of children for another purpose, which would not be prohibited.

a. Permitted Uses: Appropriate employment-related use of information, as directed by state law(s).

b. Prohibited Uses: Any other use is prohibited without express consent.

13. Person-to-Person Content that the Individual Did Not Post Publicly: This includes content of all types, whether they are keyed (including but not limited to email, text, and chat), voice (including but not limited to voice messages left for a friend, family member, or customer service representative), or other type of person-to-person communications that are not publicly disclosed by the individual but instead directed to an individual or a limited group of individuals. The timeliest attention to this matter is regulation of the intentional distribution of non-consensual sexual images, or "revenge porn." Currently 41 states and the District of Columbia have laws governing revenge porn, but these are new and evolving. We suggest that Congress further consider this issue as part of individual privacy protection regulations.

14. Telephone Communications: Existing law on this issue includes the Telephone Consumer Protection Act (TCPA), enacted in 1991 and amended in 2015, which was designed to safeguard consumer privacy by restricting telemarketing communications via voice calls, SMS texts, and fax; and Telemarketing Sales Rule (TSR) which requires specific disclosures, prohibits misrepresentations, sets limits on times telemarketers may call consumers, and prohibits calls to a consumer who has asked not to be called again. The National Do Not Call Registry, established by the FTC in 2003, introduced regulations that prohibit commercial telemarketers from making unsolicited phone calls. We suggest that Congress should review the existing regulations within the context of new privacy legislation to determine whether updates are needed.[17]

"OTHER PERSONAL INFORMATION" REQUIRES BASIC PROTECTIONS

"Other Personal Information"; Permitted And Prohibited Uses Specified

Other Personal Information is defined as any personal information that is not included in the defined meaning of Sensitive Personal Information set forth in Section IV, above. Permitted and prohibited uses of Other Personal Information are specified. Other Personal Information requires Basic Transparency, Individual Input and Accountability.

1. Permitted Uses of Other Personal Information: Other Personal Information may be used for any purpose. In all other cases Basic Transparency, Individual Input and Accountability apply. Organizations should adopt a risk based approach to determine which Individual Input and Accountability mechanisms to select.

2. Prohibited Uses of Other Personal Information: Other Personal Information may not be used in any of the following ways:

   a. Prohibited Use of Contact Information: Generally, it is not illegal to contact people using their name and address, an online ID, or other identifier. Outreach between

[17] We note that a separate category of "wiretap" laws exist, and Congress may wish to consider in the context of the Individual Privacy Act whether updates to these laws are appropriate.

individuals and between companies and individuals is a proper and legal part of our society. However, use of contact information to make certain types of contacts is illegal. Whether via advertising or on a person-to-person or other basis, the following types of contacts are illegal: vulgar, profane, or pornographic contacts; contacting someone for commercial purposes and failing to immediately identify who is doing the contacting in sufficient detail that the party receiving the contact could easily return the contact; all anonymous commercial contacts; phone calls from a spoof telephone number; commercial contacts from a phone number that if return-called is not answered by the entity that actually placed the original call; commercial direct mail that does not include the name and physical address of the sender. Use of contact information for these and other anonymous commercial contacts, whether or not listed here as examples, are illegal.

b. Misleading Disclosures: It is also illegal to make materially inaccurate statements or to omit material information required to make a statement, taken as a whole, not misleading, in the context of Transparency or Individual Input.

ASSIGNS RESPONSIBILITY FOR ENFORCEMENT

Sensitive Personal Information

Enforcement authority for requirements relating to Sensitive Personal Information will be divided as follows:

1. Existing Regulator and Regulated Subject Matter

   Where a specific enforcement regime already exists (e.g. HIPAA) the Individual Privacy Act will not put in place new enforcement responsibility. Current regulators will continue to enforce and interpret those laws.

2. New Subject Matter

   Where the type of Sensitive Personal Information is very similar to something already covered by another law (e.g. health data that is not currently covered by HIPAA would be similar to protected health information already covered by HIPAA) it may be appropriate that requirements for the newly regulated Sensitive Personal Information be enforced by the existing regulator(s) for the existing law. In all other cases, the Federal Trade Commission will have authority to enforce the new requirements.

Other Personal Information

The Federal Trade Commission will have authority to enforce legal requirements relating to Other Personal Information when used in a way not subject to other existing federal law. And as previously noted, the FTC has a long history of assertive and balanced enforcement of privacy issues.

IMPOSES PENALTIES FOR VIOLATIONS

The Individual Privacy Act should establish a structure that strongly mandates compliance while allowing for penalties only in circumstances where Individual Privacy Interests are significantly affected based on the amount and nature of personal information involved.[18]

FEDERAL PREEMPTION

It is critical that a single, uniform law applies to all types and uses of personal information by the organizations to be covered by the Individual Privacy Act (as described in Section XI, below). For Societal Interests to be adequately protected, personal data must efficiently flow throughout the United States and must also be properly used and protected no matter in which state the use occurs. Having a patchwork of varying state laws on this topic would greatly increase the compliance burdens for organizations, multiplying many times over the negative effects described in the Introduction to this policy statement, and could also result in varying protection of Individual Privacy Interests across the country. The Individual Privacy Act will therefore preempt any state laws on the subject matter of individual privacy rights other than those that are expressly permitted by other Federal laws that govern use of certain types of Sensitive Personal Information.

ORGANIZATIONS COVERED

The Individual Privacy Act will govern any individual or organization other than individuals acting for purely personal purposes. For example, information in an individual's personal address book used to interface with friends, family and acquaintances for personal reasons would not be governed, but customer information of a business or donor information of a nonprofit organization would be governed.

[18] It should be noted that large penalties for minor violations of the law could effectively limit use of personal information to very large organizations and significantly harm small to medium sized organizations, including most charitable organizations. This would undoubtedly have a major negative impact on Societal Interests and in fact could serve to further entrench the largest organizations who use personal data at the expense of competition and innovation.