COMPARING PRIVACY PRINCIPLES FOR THE 116TH CONGRESS

Analysis of Key Considerations for Privacy Legislation from the Following Organizations

Business Roundtable (BRT)
Business Software Alliance (BSA)
Computer and Communications Industry Association (CCIA)
Google
Information Technology Industry Council (ITI)
Intel
Internet Association (IA)
U.S. Chamber of Commerce

SCOPE	*What types of organizations should baseline privacy legislation apply to?*
BRT	A national consumer privacy law should apply a consistent, uniform framework to the collection, use, and sharing of personal data across industry sectors…Care should be given to how or if small companies that do not process much personal data or engage in low risk processing of data should be covered, with consideration of how those companies may be covered under existing law.
BSA	N/A
CCIA	Covered organizations or entities include all organizations that process personal information regardless of whether they have a direct or commercial relationship with an individual whose information they hold.
Google	Aside from the context of particular relationships that have existing rules, like with one's employer or attorney, legislation should apply to all economic sectors and all types of organizations that process personal information.
IA	A national privacy framework should include protections that are consistent for individuals across products and services. Such a framework should be both technology neutral (no specific technology mandates) and sector neutral (applying to online and offline companies alike).
Intel	Covered entities includes organizations under FTC authority, common carriers, non-profits organizations, an organizations related to a covered entity by common ownership or control. The definition excludes organizations with fewer than 25 employees and that collect or utilize the personal data of fewer than 50,000 individuals and entities involved in purely transmission, routing, and connecting the personal data between or among covered entities.
ITI	This framework is a robust, technology and business model-neutral approach for the protection of privacy and personal data that advances the interests of all stakeholders, including consumers, businesses, individuals, and governments.
US Chamber	[The Chamber] recognizes that businesses not under FTC jurisdiction are subject to the jurisdiction of other agencies and will be subject to enforcement by those agencies. The U.S. Chamber adopted privacy principles that apply to all industry sectors that handle consumer data and are not specific to any subset of industry sectors. These principles shall be applied consistently across all industry sectors.

PERSONAL DATA	*How should personal information be defined?*
BRT	Personal data should be defined as consumer data that is held by the organization and identifies or is identifiable to a natural, individual person. This information may include but is not limited to: name and other identifying information, such as government-issued identification numbers; and personal information derived from a specific device that reasonably could be used to identify a specific individual. Personal data should exclude de-identified data and data in the public domain.
BSA	N/A
CCIA	Personal information or data include any data under the control of a covered organization, that is not de-identified or otherwise generally available to the public through lawful means, and is linked or practically linkable to a specific individual, or linked to a specific device or account that is associated with or routinely used by an individual.
Google	The scope of legislation should be broad enough to cover all information used to identify a specific user or personal device over time and data connected to those identifiers, while encouraging the use of less-identifying and less risky data where suitable. The law should clarify whether and how each provision should apply, including whether it applies to aggregated information, de-identified information, pseudonymous information or identified information.
IA	These privacy principles aim to protect an individual's personal information, which we define as any information capable of identifying a specific individual or a device that belongs to that individual.
Intel	The term "personal data" means any information relating to an identified or identifiable natural person, other than those specific categories of personal data which the Commission exempts from this definition by promulgation of a final rule as deemed appropriate to carry out the purpose of this Act.
ITI	"Personal data" is any data that is reasonably linkable to or associated with, either directly or indirectly, a specific natural individual...Data that is anonymized, pseudonymized and protected, or otherwise publicly available is not personal data.
US Chamber	The term "personal information" means information that identifies a consumer. Information is not personal information if it is aggregated information, deidentified information, pseudonymized information or publicly available information that is lawfully made available to the general public.

TRANSPARENCY	*What notice should organizations provide regarding their use of personal data?*
BRT	Consumers should have reasonable access to clear, understandable statements about the organization's practices and policies with respect to personal data, including: information on the types of personal data collected; the purposes for which the personal data will be used; whether and for what purposes personal data may be disclosed or transferred to non-affiliated third parties; the choices and means for exercising individual rights with respect to personal data…Statements should be in a format that is reasonable and appropriate…
BSA	Organizations should provide clear and accessible explanations of their practices for handling personal data, including the categories of personal data they collect, the type of third parties with whom they share data, and the description of processes the organization maintains to review, request changes to, request a copy of, or delete personal data.
CCIA	Covered organizations must be transparent about the types of personal information that they are collecting and how they are collecting and using it…[they] should be clear about whether the personal information may be transferred to third parties, how long information may be retained, and what choices and controls individuals have with respect to their personal information…[they] should make reasonable efforts to actively inform individuals…
Google	Organizations must be transparent about the types of personal information they collect, why they collect it, and how they use or disclose it, particularly when used to make decisions about the individual. Regulators should encourage organizations to actively inform individuals about data use in the context of the services themselves…
IA	A national privacy framework should give individuals the ability to know whether and how personal information they provide to companies is used and shared with other entities, and if personal information is shared, the categories of entities with whom it is shared, and the purposes for which it is shared.
Intel	A covered entity shall provide explicit notice to an individual prior to the collection from that individual of personal data that is likely to create significant privacy risk…[it] shall publish, and make publicly available…a privacy policy generally articulating the processing practices of the covered entity…[it] shall publish and make publicly available…a description of the covered entity's collection and processing of personal data…
ITI	Individuals should be informed about the collection and use of their personal data in a fashion that is meaningful, clear, conspicuous, and useful to the individual. Such notices should…include information regarding: (1) the types of personal data collected; (2) the entity that is collecting their personal data; (3) how the personal data will be used; (4) how long the personal data will be retained…
US Chamber	A business shall, upon receipt of a verifiable request directly from the individual consumer, disclose to that consumer within a reasonable time period — (1) The categories of the personal information pertaining that to the consumer collected, used or shared by the business; (2) The business or commercial purpose for collecting, using or sharing such personal information; and (3) The categories of third parties with whom the business shares such personal information.

CONSUMER CHOICE	*How can organizations give consumers meaningful choices regarding data collection?*
BRT	Consumers should have opportunities to exert reasonable control with regard to the collection, use, and sharing of personal data. No one specific mechanism for consumer control is suitable in all instances, and organizations should be permitted flexibility in how these controls may reasonably be exercised in light of the sensitivity of the personal data, as well as the risks and context of the specific data processing and sharing with non-affiliated third parties. Where organizations rely upon "consent" to collect and use personal data, the type of consent required should be contextual, taking into account the nature of both the personal data and its proposed uses…
BSA	Organizations should provide consumers with sufficient information to make informed choices and, where practical and appropriate, the ability to opt out of the processing of personal data. BSA recognizes that certain data, such as financial account information or health condition, may be particularly sensitive…If the use of sensitive data implicates heightened privacy risks, organizations should enable consumers from whom they collect sensitive data to provide affirmative express consent.
CCIA	Covered organizations must provide appropriate mechanisms for individual control, considering the service. Individuals should be able to object to data processing where it is feasible, but specific consent should not be mandatory for every aspect of data processing, which could create an overly complex and confusing experience for the individual and divert from the overall goals that the policy seeks to achieve. Policymakers should also keep in mind that the responsible processing of personal information is necessary to simply operate some services.
Google	Organizations must provide appropriate mechanisms for individual control, including the opportunity to object to data processing where feasible in the context of the service. This does not require a specific consent or toggle for every use of data; in many cases, the processing of personal information is necessary to simply operate a service. Similarly, requiring individuals to control every aspect of data processing can create a complex experience that diverts attention from the most important controls without corresponding benefits.
IA	Individuals should have meaningful controls over how personal information they provide to companies is collected, used, and shared, except where that information is necessary for the basic operation of the business or when doing so could lead to a violation of the law.
Intel	The consumer privacy and data security program should be designed to…facilitate individuals' control over their personal data and enable them to participate in decision-making regarding the processing of their personal data…
ITI	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…Individuals should have the right to…object to the use of their personal data.
US Chamber	A business, including a third party, must honor the verifiable request received directly from the individual consumer to not share the consumer's personal information with third parties…known as opt-out consent…

USER CONTROL	*What controls should consumers have over their data, such as the rights to access, correct and delete information they have provided to an organization?*
BRT	Consumers should have a reasonable right to access and correct any inaccuracies in personal data collected about…Consumers should be able to require an organization to delete their personal data collected…when such data is no longer required to be maintained under applicable law or is no longer necessary for legitimate business purposes of the organization. Organizations may limit a consumer's right to delete in circumstances where the rights of other individuals outweigh deletion, or the data is required for freedom of expression and information. Deletion should not be required where disposal is not reasonably feasible…
BSA	Consumers should be able to request information about…data. They should be able to request a copy of the data, challenge the accuracy of that data, and, as appropriate, have the data corrected or deleted. Organizations that determine the means and purposes of processing personal data should be primarily responsible for responding to these requests. Organizations may deny such requests where the burden or expense of doing so would be unreasonable or disproportionate to the risks to the consumer's privacy…
CCIA	Individuals must be able to access the personal information…organizations should afford users with the ability to correct and/or delete the data that they provide to that organization when it would be practical and provided that deletion would not implicate the personal information of others. Covered organizations should make reasonable efforts to enable authenticated users to obtain data they provide to that…provided that these data portability tools do not implicate the personal information of others.
Google	Individuals must have access to personal information they have provided to an organization, and where practical, have that information corrected, deleted, and made available for export in a machine-readable format.
IA	Individuals should have reasonable access to the personal information they provide to companies…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. Individuals should have the ability to request the deletion of the personal information they provide to companies where that information is no longer necessary to provide the services, except where companies have a legitimate need or legal obligation…
Intel	A covered entity shall provide…[a] means of promptly obtaining: (1) confirmation of whether personal data concerning the individual is processed by the covered entity; (2) descriptions of the categories of personal data that are processed by the covered entity…(4) reasonable access to the personal data and the ability to correct erroneous personal data; (5) correction or supplementation of the personal data with additional information offered voluntarily by the individual to address data quality requirements…
ITI	Individuals should have the right to…access in a timely manner personal data collected from them; rectify, complete, or delete inaccurate or incomplete personal data; have an entity delete their personal data.
US Chamber	A business…shall make a good faith effort to delete and require its service providers to delete personal information upon a verifiable request received directly from the individual consumer.

DATA SECURITY	*What responsibilities should organizations have in protecting and securing the confidentiality, integrity, and availability of user data?*
BRT	Organizations should implement reasonable…safeguards designed to reasonably protect against the unauthorized access to or disclosure of personal data, or other potentially harmful misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened and the sensitivity of the personal data. Regulation should not prescribe or otherwise require specific safeguards, tools, strategies, or tactics.
BSA	Organizations should employ reasonable and appropriate security measures designed to prevent unauthorized access, destruction, use, modification, and disclosure of personal data based on the volume and sensitivity of the data, size and complexity of the business, and cost of available tools.
CCIA	Users should expect that organizations handling their data will do so carefully and responsibly with reasonable measures to protect personal information from unauthorized access, misuse, modification, disclosure, loss, and destruction.
Google	Organizations must implement reasonable precautions to protect personal information from loss, misuse, unauthorized access, disclosure, modification, and destruction, and should expeditiously notify individuals of security breaches that create significant risk of harm. Baseline precautions should apply to any collection of personal information, and additional measures should account for and be proportionate to the risk of harm.
IA	A national privacy framework should focus on accomplishing privacy and data security protections, but laws and regulations should avoid a prescriptive approach to doing so, as such an approach may not be appropriate for all companies and may well become obsolete in light of rapidly developing technology.
Intel	A covered entity shall develop, document, implement, and maintain a comprehensive data security program that contains…safeguards for personal data that are appropriate to the size and complexity of the covered entity, the nature and scope of the covered entity's activities, and the sensitivity of any personal data... Such a data security program shall…(1) safeguard the security, confidentiality, integrity, and availability of personal data; (2) protect against any anticipated threats or hazards to the security or integrity of such personal data; (3) protect against unauthorized processing of such personal data…
ITI	Companies should implement comprehensive security programs that are reasonable and proportionate to the size and complexity of their operations, the nature and scope of their activities, and the sensitivity of the personal information they knowingly use or that is under their control…
US Chamber	Congress should include risk-based data security and breach notification provisions that protect sensitive personal information pertaining to individuals. Keeping this information secure is a top industry priority. Security is different for individual businesses and one-size-fits-all approaches are not effective; therefore, companies should have flexibility in determining reasonable security practices.

PROPORTIONALITY	*How can organizations have flexibility in meeting the requirements of a federal privacy law given their size, resources, and data practices?*
BRT	Specific risk-based practices should not be prescribed by regulation or otherwise required; rather, organizations should have flexibility in how they leverage risk-based privacy practices.
BSA	N/A
CCIA	Reasonable data protection practices may differ across covered organizations. Context, including an organization's scale and resources, the sensitivity of the data it holds, and its uses for that data, should inform the measures that it puts in place to protect data.
Google	The application of the law should also take into account the resource constraints of different organizations, encouraging new entrants and diverse and innovative approaches to compliance.
IA	As policymakers and stakeholders work on an updated approach to privacy, we must ensure that a national privacy framework… Is mindful of the impact of regulation on small- and medium-sized companies…
Intel	N/A
ITI	N/A
US Chamber	N/A

PREEMPTION	*Should federal baseline privacy law override overlapping requirements at the state level?*
BRT	It should eliminate fragmentation of regulation in the United States by harmonizing approaches to consumer privacy across federal and state jurisdictions through a comprehensive national standard that ensures consistent privacy protections and avoids a state-by-state approach to regulating consumer privacy…a national consumer privacy law should pre-empt any provision of a statute, regulation, rule, agreement, or equivalent of a state or local government for organizations with respect to the collection, use, or sharing of personal data.
BSA	Any uniform federal privacy law should harmonize requirements in state law.
CCIA	A national, privacy framework should be consistent throughout the United States, so state laws concerning data privacy, security, and breach notifications should be preempted where appropriate.
Google	N/A
IA	[A national privacy framework] should be consistent throughout all states, preempting state consumer privacy and data security laws. A strong national baseline creates clear rules for companies and ensures that individuals across the United States can expect consistent data protections from companies that hold their personal information.
Intel	For a covered entity that is subject to this subtitle, the provisions of this subtitle shall preempt any civil provisions of the law of any State or political subdivision of a State to the degree they are focused on the reduction of privacy risk through the regulation of personal data collection and processing activities…
ITI	N/A
US Chamber	The provisions of this Act shall supersede any provisions of the statutes, laws, regulations, rules, ordinances, requirements, or the equivalent, of any State, or any locality or political subdivision of a State, including, but not limited to, any tort, duty, or consumer protection or unfair practice law, to the extent that such provisions relate to, or serve as the basis for enforcement action as it relates to, the privacy or security of personal information. No State, or any locality or political subdivision of a State, shall adopt, maintain, enforce, impose, or continue in effect any such provision after the effective date of this Act.

ACCOUNTABILITY	*How should organizations be held accountable for complying with their duties under the privacy framework?*
BRT	[A national federal privacy framework] should include robust protections for personal data that enhance consumer trust and demonstrate U.S. leadership as a champion for privacy by including clear and comprehensive obligations regarding the collection, use, and sharing of personal data, and accountability measures to ensure that those obligations are met.
BSA	Organizations should develop policies and procedures that provide the safeguards outlined in this framework, including designating persons to coordinate programs implementing these safeguards and providing employee training and management; regularly monitor and assess the implementation of those programs; and, where necessary, adjust practices to address issues as they arise.
CCIA	Covered organizations should be held accountable for meeting the requirements set out in these Privacy Principles. Covered organizations should regularly assess the privacy risks associated with their collection, processing, and use of personal information; develop systems to mitigate risks in a reasonable and proportionate manner; and monitor services for bias and disparate impacts. Organizations should practice privacy by design, building products and services that prioritize privacy, security, reliability, and reduce the likelihood of vulnerabilities, which will help earn user trust. Policymakers should set baseline requirements but enable flexibility to meet those requirements and promote industry accountability programs and safe harbors.
Google	Accountability can and should come in many forms. Lawmakers and regulators should set baseline requirements and enable flexibility in how to meet those requirements. Industry accountability programs and safe harbors can incentivize best practices, particularly in providing more flexible approaches to dealing with evolving technologies.
IA	N/A
Intel	A covered entity shall ensure compliance with this Act by developing and implementing an ongoing accountability program that includes: (1) Policies…(2) Internal leadership, staffing and oversight…(3) Staffing and delegation...(4) Education and awareness... (5) Ongoing risk assessment and mitigation…(6) Program risk assessment oversight and validation…(7) Incident management and complaint handling…(8) Internal enforcement…(9) Redress.
ITI	Companies should maintain records pertaining to risk assessments and security programs so that they are auditable by the designated authority in the event of an incident. The development of technical capacity within the oversight body to ensure robust enforcement of these principles is an important consideration in any privacy regime.
US Chamber	N/A

ENFORCEMENT	*What agency should be the primary enforcement authority for ensuring compliance with federal privacy rules?*
BRT	The FTC is the appropriate federal agency to enforce a national consumer privacy law, unless a determination is made that it is appropriate for a different regulator to be the enforcement agency. Care should be taken to avoid duplication of enforcement across federal agencies. The FTC should have adequate funding and staffing to effectively enforce the consumer privacy law. A national consumer privacy law should not provide for a private right of action.
BSA	The Federal Trade Commission, which has a strong record of robust enforcement, should have the tools and resources necessary to carry out its mission effectively.
CCIA	A robust federal baseline would provide clear standards for covered organizations and ensure that individuals across the United States can expect consistent data protections from organizations that retain their data... This framework should be enforced primarily by the FTC at the federal level, but it should allow for enforcement by state attorneys general where the FTC has declined to act.
Google	N/A
IA	A national privacy framework should primarily be enforced by the FTC at the federal level and by state attorneys general at the state level, where the FTC declines to act.
Intel	Compliance with the requirements imposed under this subtitle may be enforced pursuant to the Federal Trade Commission Act (15 U.S.C. 41 et seq.) by the Commission with respect to persons subject to this Act. All of the functions and powers of the Commission under the Federal Trade Commission Act are available to the Commission to enforce compliance by any person with the requirements imposed under this title. [Also provides for criminal enforcement by the Attorney General under certain circumstance]
ITI	N/A
US Chamber	The [Federal Trade] Commission shall enforce the requirements of the Act. Notwithstanding section 5(a)(2) of the Federal Trade Commission Act, the Commission shall have authority over common carriers subject to the Communications Act of 1934 to enforce this Act.

GLOBAL INTEROPERABILITY	*How can a U.S. privacy regime promote the free flow of data across national borders?*
BRT	It should facilitate international transfers of personal data and electronic commerce and promote consumer privacy regimes that are interoperable, meaning it should support consumer privacy while also respecting and bridging differences between U.S. and foreign privacy regimes.
BSA	Privacy frameworks should enable and encourage global data flows, which underpin the global economy. Where differences exist among varying privacy regimes, governments should create tools to bridge those gaps in ways that both protect privacy and facilitate the free flow of data.
CCIA	Cross-border data flows are essential to the modern economy. Organizations and individuals benefit from consistent compliance programs based on widely shared principles of data protection. These principles are intended to be interoperable and consistent with existing cross-border data transfer mechanisms, industry standards, and other cross-organization cooperation mechanisms.
Google	Mechanisms allowing for cross-border data flows are critical to the modern economy...Countries should adopt an integrated framework of privacy regulations, avoiding overlapping or inconsistent rules whenever possible. Regulators should avoid conflicting and unpredictable requirements, which lead to inefficiency and balkanization of services and create confusion in consumer expectations…Privacy regulation should support cross-border data transfer mechanisms, industry standards, and other cross-organization cooperation mechanisms that ensure protections follow the data, not national boundaries.
IA	N/A
Intel	N/A
ITI	While building on the strengths of existing global approaches, this framework is grounded in the principles of accountability, context, and mitigation of privacy risk to the individual and offers several key advantages including creating alignment with the privacy protections of other privacy regimes across the globe and enabling interoperability with these global approaches.
US Chamber	Congress should adopt policies that promote the free flow of data across international borders for consumer benefit, economic growth and trade. A national privacy framework will bolster continued U.S. leadership internationally and facilitate interoperable cross-border data transfer frameworks.

BREACH NOTIFICATION	*How should organizations provide notice of data breaches?*
BRT	A consumer privacy law should establish a national standard for breach notification that preempts state laws. Consumers have the right to be notified within a reasonable timeframe if there is a reasonable risk of significant harm as a result of a personal data breach.
BSA	N/A
CCIA	If a security breach occurs, organizations should notify individuals expeditiously when there is a significant risk of harm.
Google	Organisations…should expeditiously notify individuals of security breaches that create significant risk of harm.
IA	A national framework should specifically preempt the patchwork of different data breach notification laws in all 50 states and the District of Columbia to provide consistency for individuals and companies alike. This national standard should protect individuals and their personal information through clear notifications, define a harm-based trigger for notification to avoid notice fatigue, and allow companies flexibility in how they notify individuals of unauthorized access to their personal information.
Intel	N/A
ITI	Individuals should have the right to redress mechanism...and to be notified in a timely manner if a breach of their personal data triggers a risk of concrete and measurable harm to them or their rights.
US Chamber	[See Data Security]

RESEARCH & INNOVATION	*What role can the government play in promoting the emergence of modern best practices for protecting privacy and security?*
BRT	[A national consumer privacy law] should be technology neutral and take a principles-based approach in order for organizations to adopt privacy protections that are appropriate to specific risks as well as provide for continued innovation and economic competitiveness in a dynamic and constantly evolving technology landscape.
BSA	N/A
CCIA	These principles aim to... promote innovation, in both digital services and privacy protection.
Google	Governments can support these goals by rewarding research, best practices, and open-source frameworks. Creating incentives for organizations to advance the state of the art in privacy protection promotes responsible data collection and use.
IA	N/A
Intel	Not later than one year after the date of enactment of this Act, and at least annually thereafter, the Commission shall publish… a report to Congress on recommendation… for government funding for the research of privacy enhancing technologies.
ITI	The purpose of this framework is to inform the development of legislation or the promulgation of rules that enhance personal data protection, further the trust relationship between companies and their customers, and enable innovation while also avoiding regulatory fragmentation that undermines all three goals.
US Chamber	Incorporating privacy considerations into product and service design plays an important role and benefits all consumers. A national privacy framework should encourage stakeholders to recognize the importance of consumer privacy at every stage of the development of goods and services.

RISK-BASED ENFORCEMENT	*What types of violations should regulators focus on?*
BRT	Enforcement actions and fines should be informed by the harm directly caused by, and severity of, an organization's conduct as well as any actions taken by the organization to avoid and mitigate the harm, the degree of intentionality or negligence involved, degree of cooperation, and the organization's previous conduct involving personal data privacy and security.
BSA	Where the processing of data poses risks to the privacy of consumers, privacy frameworks should implement a risk-based approach that tailors protections to circumstances that are likely to lead to substantial harm.
CCIA	Policy should account for and be proportionate to the risk of harm.
Google	Regulators should encourage the design of products to avoid harm to individuals and communities. Enforcement and remedies should be proportional to the potential harms involved in the violation. Innovative uses of data shouldn't be presumptively unlawful just because they are unprecedented, but organizations must account for and mitigate potential harms. This includes taking particular care with sensitive information that can pose a significant risk. To enable organizations to develop effective mitigations, regulators should be clear about what constitutes a harm.
IA	A national privacy framework should be grounded in a risk-based approach, based on the sensitivity of the personal information, the context of its collection and use, and the risk of tangible harm for its misuse or unauthorized access. Consistent with FTC data security order provisions and the FTC's unfairness standard, companies should identify and address reasonably foreseeable risks to the privacy and the security of personal information where the result of failing to address the risk would cause, or be likely to cause, tangible consumer harm.
Intel	The FTC shall issue a final rule in accordance with this section to provide more guidance on potential adverse consequences that would fall underneath this definition. The term "privacy risk" means potential adverse consequences to individuals and society arising from the processing of personal data, including, but not limited to: 1) Direct or indirect financial loss or economic harm; (2) Physical harm…
ITI	N/A
US Chamber	Enforcement provisions of a federal data privacy law should only apply where there is concrete harm to individuals.

DATA QUALITY	*How can regulation support the maintenance of accurate, complete, and necessary information?*
BRT	Personal data should be relevant to the purpose for which it is used and, to the extent necessary for those purposes, should be accurate, complete, and current.
BSA	Personal data should be relevant to the purpose for which it is used and, to the extent necessary for those purposes, should be accurate, complete, and current.
CCIA	Personal information should be accurate, current, and complete to the extent possible for the purpose for which the covered organization maintains the data.
Google	Organizations should make reasonable efforts to keep personal information accurate, complete, and up-to-date to the extent relevant for the purposes for which it is maintained. Data access and correction tools, as mentioned below, can assist organizations in meeting this obligation.
IA	N/A
Intel	A covered entity shall only process personal data that is relevant to the purposes for which they are to be processed, and, to the extent necessary for those purposes. To the extent reasonable for the purpose of the processing, the data should be complete, accurate, and should be updated by the covered entity as necessary to maintain accuracy."
ITI	Companies should ensure that personal data under their control is adequate (sufficient to properly fulfill the stated purpose), relevant (has a rational link to that purpose), limited to what is appropriate in relation to the purposes for which the data is used, and used only for purposes compatible with the context.
US Chamber	N/A