April 7, 2025

Congressman Brett Guthrie (R-KY)
Chairman
House Committee on Energy and Commerce

Congressman John Joyce, M.D. (R-PA)
Vice Chairman
House Committee on Energy and Commerce

2125 Rayburn House Office Building
Washington, DC 20515

Re: Privacy Working Group Request for Information

Dear Chairman Guthrie and Vice Chairman Joyce:

My name is Ryan Nabil, and I serve as the Director of Technology Policy at the National Taxpayers Union Foundation in Washington, DC, where my research focuses on U.S. and international technology policy issues of interest to U.S. taxpayers.

We welcome the House Energy and Commerce Committee's continued commitment to establishing an innovation-friendly and balanced federal data privacy framework, and appreciate the opportunity to submit comments on the request for information on data privacy and security.

The attached document contains our responses to the Privacy Working Group's request for information. We hope that these insights prove useful as the Committee develops proposals for well-designed U.S. federal privacy legislation.

Respectfully,
Ryan

Ryan Nabil
Director and Senior Fellow, Technology Policy
National Taxpayers Union Foundation
122 C Street NW
Washington, DC 20001

I. Roles and Responsibilities

The digital economy includes a wide range of business models, including entities that collect information directly from consumers, those that process personal information on another business's behalf, and others that collate and sell personal information.

A. How can a federal comprehensive data privacy and security law account for different roles in the digital economy (e.g., controllers, processors, and third parties) in a way that effectively protects consumers?

A well-designed comprehensive data privacy and security law must recognize and define different actors in the data privacy landscape and specify rights and responsibilities for each actor. In this context, Congress would benefit from evaluating how such roles are distinguished in other leading privacy frameworks like the EU and UK's General Data Protection Regulation, Japan's Act on the Protection of Personal Information (APPI), and Canada's Consumer Privacy Protection Act (CPPA). Congress would benefit from a comparative understanding of how different U.S. state privacy legislation defines and distinguishes between different actors. While the precise definition should be set by Congress based on a more detailed analysis, such a framework should, at a minimum, include the following roles: data controllers, processors, sub-processors, brokers, joint controllers, data recipients, and data subjects.

It is worth noting that certain data privacy laws introduce unique terms that are uncommon in other frameworks, while others may define the same term in varying ways. For example, the term "service provider" is specific to the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA)—and does not appear in many other privacy legislation. Likewise, Japan's APPI introduces the term "Personal Information Collector (PIC)"—which doesn't exist in the GDPR—covering entities that collect personal information for business purposes.[1] The U.S. data privacy and security law does not have to follow the precise template of any existing privacy legislation at the national or state level. However, if it does introduce new categories—it must be backed with important policy and legal rationale and defined clearly to avoid uncertainties.

Special consideration is also necessary in understanding possible interaction between different actors within the digital economy and whether such interactions necessitate the creation of a legally defined category or role under the proposed data privacy law. For example, a sub-processor, which processes personal data on behalf of another processor, could be one such category.[2] Distinguishing between these roles and establishing clear responsibilities, expectations, and rights for each type of actor will be key to the long-term success of the U.S. data privacy framework.

---

[1] Formally translated as "Business Operator Handling Personal Information." Act on the Protection of Personal Information, Act No. 57 of 2003, Art. 2, Para. 3 (Japan), amended by Act No. 32 of 2020.
[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Article 28, OJ L 119, 4.5.2016, pp. 48–50.

B. What are appropriate obligations for different regulated entities, and what are the practical and legal limitations associated with each type of entity?

Obligations must be carefully calibrated to different actors according to the scope and scope of their data collection and processing activities within the digital ecosystem. The most extensive set of obligations should apply to controllers—as they have a direct relationship with data subjects and have the highest level of decision-making authority over how user data is collected and processed.[3]

For example, controllers must provide data subjects with a clear and easily understandable privacy notice that explains why, how, and for how long their data will be collected, processed, and stored. Such data should then only be processed for the specified, explicit, and legitimate purposes that were disclosed to data subjects at the point of data collection. Well-designed privacy laws typically include data minimization and scoping requirements, meaning that only data necessary for the pre-specified purpose should be collected. Likewise, controllers typically have the primary responsibility for ensuring that data subjects can exercise any applicable rights (e.g., objection to processing and the right to rectify or erase collected data). Additionally, controllers should have obligations to implement adequate safeguards to ensure data security and should be required to notify the relevant regulator and affected individuals in the event of a data breach.[4]

Another set of calibrated responsibilities and obligations should apply to processors and sub-processors—who lack a direct relationship with users but act on behalf of controllers and follow their instructions to process user data.[5] The U.S. privacy framework should include calibrated laws and regulations to implement safeguards personal data, maintain detailed record of data processing activities, and assist data controllers in compliance assistance, such as responding to data subject requests and data protection impact assessments, where appropriate. In the case of a data breach, data processors should be required to notify data controllers promptly, who can then inform the relevant regulators and affected individuals.[6]

Data brokers—which are entities that collect, aggregate, and resell personal data from public and non-public sources without directly interacting with data subjects—warrant a distinct regulatory approach.[7] Although data brokers do not typically initiate data collection, their role in determining how personal data is aggregated, analyzed, and sold requires the need for additional obligations.

---

[3] GDPR, Article 4(7).
[4] GDPR, Articles 5, 12, 13, 15–22, 32–34.
[5] GDPR, Articles 4(8), 28(2), and 28(4).
[6] GDPR, Articles 33(1), 33(2), and 34(1); 45 CFR § 164 (HIPAA).
[7] There does not appear to be a consensus among existing legislation and regulators on the definition of data brokers. For the Federal Trade Commission's approach, see FTC, "FTC to Study Data Broker Industry's Collection and Use of Consumer Data," December 18, 2022, https://www.ftc.gov/news-events/news/press-releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data.

A hybrid approach can be particularly beneficial in this context.[8] Data brokers and third parties that merely process data on behalf of other entities—without independently determining the purpose and means of processing data—should be subject to the same obligations as processors. That would be the case, for example, when a broker provides services such as data storage and analytics under the instructions of a data controller or processor. However, data brokers and third parties that i) exercise decision-making authority over how personal data is collected, aggregated, and analyzed, ii) sell or share data for commercial purposes, and/or iii) build its own commercial analytics should be considered controllers for the purposes of U.S. privacy law and subject to the same set of legal obligations and responsibilities.[9]

C. Should a comprehensive data privacy and security law take into consideration an entity's size, and any accompanying protections, exclusions, or obligations?

A two-pronged approach can help the United States promote steps to protecting data privacy and security without disproportionately burdening smaller and medium-sized businesses. There has to be a baseline level of privacy regulations that applies to all entities processing personal data, including small businesses and government entities. Such baseline regulations should cover, among others, requirements related to data minimization and transparency requirements. Beyond this baseline, more restrictive measures can apply on the basis of the size of the company and the scope and extent of data processing. Such scaled-requirements could include the requirement to appoint data protection officers and conduct impact assessments. While smaller entities with low-risk processing activities might be exempt from these requirements, they must still comply with the baseline requirements that apply to all firms irrespective of size.

II. Personal Information, Transparency, and Consumer Rights

A federal comprehensive data privacy and security law should apply to personally identifiable information and provide consumers with clear disclosures and rights to their personal information.

A. Please describe the appropriate scope of such a law, including definitions of "personal information" and "sensitive personal information."

A comprehensive U.S. data privacy and security law should provide a clear definition of both "personal information" and "sensitive personal information." "Personal information" should encompass any information related to an already identified or identifiable individual, whether through direct means (e.g., name and Social Security number) or indirect means (e.g., online identifiers and geolocation data).[10]

---

[8] GDPR, Articles 4(7), 4(8), 28; CCPA, Sections 1798.140(c), (j), (v); CPRA, Sections 1798.140(d), (ag).
[9] See the note above.
[10] While the GDPR's definition of "personal data"—which is comparable to "personal information" under potential U.S. federal privacy legislation—may not be well-suited to the U.S. legal context, it can provide an additional frame of reference for defining the term, alongside privacy legislation of other advanced economies and U.S. states. The GDPR defines personal data as "Any information relating to an identified or identifiable

Meanwhile, "sensitive personal information" should be recognized as a separate category that requires more restrictive regulations due to the higher risk associated with such data. Such data should include, as examples, a person's Social Security number, genetic data, and more broadly, personal educational, financial, and medical records.[11] Such an approach would be consistent with leading data privacy frameworks, which recognize sensitive personal information as a special category of data for which a more restrictive set of regulations would apply. Congress would also benefit from a comparative overview of how leading international privacy frameworks define these terms, and ensure that the U.S. definitions of such terms are consistent with internationally recognized standards.

B. What disclosures should consumers be provided with regard to the collection, processing, and transfer of their personal information and sensitive personal information?

Under U.S. federal privacy legislation, consumers should be provided easily understandable, accessible, and comprehensive disclosures informing them of how their data is being collected and used and the precise reasons for such collection. These disclosures should also specify the category of data being collected, whether they will be shared with third parties, the purposes for such sharing, and how long the data will be retained. The disclosures should include a description of consumer rights and provide clear mechanisms on how consumers can exercise those rights.[12] Finally, any privacy notices should be periodically updated to ensure that they reflect any material changes in the data collection and processing practices of the relevant entities.

C. Please identify consumer protections that should be included in a comprehensive data privacy and security law. What considerations are relevant to how consumers enforce these protections and how businesses comply with related requirements?

The comprehensive data privacy and security law may benefit from the inclusion of the following consumer protections:

---

natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." (GDPR Article 4(1)).

[11] While the GDPR's definition of "special categories of personal data" and associated rules may not necessarily align with the U.S. context, it can provide a frame of reference for how other jurisdictions define personal data with a higher level of risk. Under the GDPR, "special categories of personal data" are defined as data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation" (GDPR Article 9(1)). The Committee may also benefit from comparison with the definition of "sensitive personal information" under the California Consumer Privacy Act (CCPA, § 1798.140(ae), as amended by CPRA), and "sensitive data" under the Consumer Data Protection Act (VCDPA, § 59.1-575).

[12] See GDPR, Articles 5(1)(a), 12, 13; American Data Privacy Protection Act, H.R.8152, 117th Congress (2021-2022).

1) **Right to be informed**. Data subjects should have the right to be informed about the collection and use of their personal data. The information should include the purposes of data collection and use, data retention periods, third-party sharing, and mechanisms to exercise any applicable consumer rights.
2) **Right to consent**. While the level of consent should vary depending on the type of data, explicit and informed consent is particularly important for the collection and processing of highly sensitive personal data.
3) **Right to access**. Consumers should have the right to access the personal data collected about them and know how their data were used, subject to certain conditions.
4) **Right to rectification**. Data subjects should have the right to rectify inaccurate personal data.
5) **Right to erasure.** Individuals should have the right to request the deletion of personal data under certain conditions. That could be the case when the data is no longer necessary for the original purpose of data collection or when data processing violated any applicable consumer privacy laws.
6) **Right to restrict processing**. Consumers should have the request to restrict the processing of their personal data under certain circumstances–a right that is especially important for certain categories of data.
7) **Right to data portability**. The right to request personal data in machine-readable format and transmit it to another provider, where technically feasible, could help protect rights and promote digital competition.
8) **Right to object or opt out.** Consumers should have the right to opt out of certain data collection and processing practices (e.g., the sale of personal data), the conditions of which should be specified in the privacy law.
9) **Right to redress**. While the U.S. privacy law should not have a private right of action, it should include mechanisms by which affected individuals can lodge complaints with the designated data protection authority and seek redress.[13]

D. What heightened protections should attach to the collection, processing, and transfer of sensitive personal information?

U.S. privacy law would benefit from heightened protections related to the collection, processing, and transfer of sensitive personal information. Such protections could include:

1) **More extensive consent requirements**. The collection of sensitive personal data, such as genetic data and financial records, should be subject to more explicit consent requirements than is the case for less sensitive categories of personal data.

[13] This list, which is not exhaustive, has been developed based on a comparative evaluation of major foreign and state level U.S. privacy legislation. The Committee may also benefit from paying closer attention to existing U.S. and international privacy frameworks to ensure that consumer rights in any U.S. federal privacy legislation is consistent with those provided for by well-designed privacy legislation in other advanced economies.

2) **Enhanced data minimization and purpose limitations**. Stricter data minimization and purpose requirements can help ensure that only the minimum level of data that is required for the specified purpose is collected. Stricter purpose limitations would help ensure that the collected sensitive data (e.g., genetic information) is used exclusively for the stated purpose and not for any other use not disclosed to consumers at the point of data collection.
3) **Stricter and more extensive security measures and operational safeguards**. A particular challenge in relation to highly sensitive personal data is data security. The collection, processing, and transfer of such data should be subject to stricter and more extensive security measures to ensure their security.
4) **Impact assessment and auditing requirements**. While impact assessments and auditing requirements carry higher compliance costs than many other data protection regulations, the collection and processing of highly sensitive data means that such impact assessments and auditing requirements might be necessary to ensure data security.
5) **Enhanced data breach notification requirements**. Due to the highly sensitive nature of such data, the collection, processing, and transfer of sensitive personal data should be subject to more stringent data breach notification requirements.
6) **Restrictions on cross-border transfer of sensitive data**. There should be additional safeguards to ensure that sensitive personal data is not transferred to third countries that do not ensure a similarly high level of data protection.[14]

[14] Please see the footnote above.