April 7, 2025

Chairman Brett Guthrie
Vice-Chairman John Joyce
House Energy & Commerce Committee

PrivacyWorkingGroup@mail.house.gov

Re: Comments on House E&C Committee Privacy Working Group RFI

The Insights Association (IA), the leading nonprofit association for the market research and analytics industry (also known as the insights industry), appreciates the opportunity to respond to the House Energy & Commerce Committee Privacy Working Group's Request for Information (RFI) "to explore the parameters of a federal comprehensive data privacy and security framework."[1]

IA supports a comprehensive federal consumer data privacy law that will respect and protect consumers, facilitate compliance in the private sector, preempt the patchwork of conflicting state laws, centralize enforcement at the Federal Trade Commission (FTC) and state Attorneys General (AGs), and continue to allow for the informed decision-making provided by insights services.

While we were glad to be able to participate in the committee's process with the ADPPA in 2022 and APRA in 2024, both bills were awkward, stitching together conflicting pieces that made for confusing and unsatisfying products. Both bills also ultimately failed to effectively preempt state laws. Every sought-after improvement in one area came with two steps back in another area.

IA salutes you for taking a blank slate approach, instead of trying to resurrect the ADPPA and APRA, and embracing a more open and engaged process involving stakeholder input.

The committee can build a viable legislative framework from provisions in state privacy laws like those in Texas and Kentucky (with additional language as recommended). This can shift the burden away from consumers and toward a common set of privacy norms backed by strong enforcement to incentivize and ensure accountability by the businesses and organizations that use data every day.

Below, we will explain who we are, explain why harmonizing with Europe is a fool's errand, set out the basics of a legislative framework, and highlight some key issues in privacy legislation that you may need to address: preemption; enforcement; sensitive personal data; profiling; and terms of art.

The insights industry: who we are

IA's more than 9,600 members are the world's leading producers of intelligence, analytics and insights defining the needs, attitudes and behaviors of consumers, organizations and their employees, students and citizens. With that essential understanding, leaders can make intelligent

[1] https://d1dth6e84htgma.cloudfront.net/02_21_2025_PWG_Request_for_Info_2_e1753e1356.pdf

decisions and deploy strategies and tactics to build trust, inspire innovation, realize the full potential of individuals and teams, and successfully create and promote products, services and ideas.

We are involved in the scientific process of collection and analysis of data regarding opinions, needs, awareness, knowledge, views, experiences, and behaviors of a population, through the development and administration of surveys, interviews, focus groups, polls, observation, analytics, or other research modes and methodologies.

The insights industry studies individuals and their personal data in order to understand the opinions, preferences, and potential actions of larger, representative groups.

Our working definition of "**market research**" is:

> "***the collection, use, maintenance, or transfer of personal information as reasonably necessary to investigate the market for or marketing of products, services, or ideas, where the information is not: (i) integrated into any product or service; (ii) otherwise used to contact any particular individual or device; or (iii) used to advertise or market to any particular individual or device.***"[2]

A form of market research, **audience measurement**, is usually carved out of state law definitions of targeted/personalized advertising, to make sure that it is not inadvertently restricted: "***processing personal information solely for delivering, measuring, or reporting advertising or content, performance, reach, or frequency, including independent measurement***."

Advertisers, for example, pay based on the number of "impressions" for online ads, and independent measurement in particular verifies that the number of impressions is accurate. Many businesses and organizations would bear the burden of elevated costs for every impression inaccurately added to the count. Independent measurement also allows content creators to know their actual viewership in relation to the marketplace, thus allowing for accurate programming and publishing decisions.

We urge the committee to follow suit, and clarify that audience measurement is not included.

Harmonizing with Europe would be a mistake

When it comes to a legislative approach, many activist groups and some of the largest multinational corporations have urged the harmonizing of American law to European law, namely the EU's General Data Protection Regulation (GDPR). However, this should *not* be the goal.

1. The biggest companies would potentially benefit from it from a comparative advantage standpoint, since they already are GDPR-compliant and can afford all the extra bureaucratic red tape and investment, but mid-sized and small businesses would be ruined.
2. More importantly, EU policymakers have made clear for decades that one of the primary motivators of their lawmaking was competition against the U.S., and American businesses. Even if the committee were to replicate GDPR wholesale, along with its arcane enforcement

[2] While the ADPPA and APRA adopted this definition of market research, and the APRA made it a permissible purpose, the APRA also shoe-horned in an affirmative consent requirement to collect, process, retain or transfer data for such purposes, which could have eliminated a majority of market research in the U.S. That would have chilled innovation and hindered businesses/organizations from making improvements.

regime, the EU will still refuse to designate the U.S. as providing "adequate" data protection and would still discriminate against U.S. businesses.

3. Finally, even the Europeans are recognizing they went too far with their privacy law. The European Commission will be proposing "to cut back" GDPR "in the next couple of weeks," according to *Politico*. Danish Digital Minister Caroline Stage Olsen commented that, "we don't need to regulate in a stupid way. We need to make it easy for businesses… to comply."[3]

Building a legislative framework

The base model of privacy legislation, drawing from the state models, would revolve around consumers and businesses/organizations (covering data controllers, data processors, and third-parties, with delineated responsibilities). It would:

- cover both for-profit and nonprofit companies;
- avoid overly-restrictive prohibitions on businesses/organizations, while requiring contracts (with built-in oversight) between data-sharing partners to ensure that consumers are protected and responsibilities are clear;
- require transparency from businesses/organizations and put consumers in control as much as feasible;
- limit responsibilities for businesses that collect, process, or share minimal amounts of personal data, rather than simply carving out small businesses;
- require the establishment, implementation, and maintenance of reasonable administrative, technical, and physical data security practices that suit the size and nature of personal data in question, and prioritize general outcomes rather than specific technologies or prescriptive requirements;
- prohibit specifically-defined unreasonable data practices, such as: using personal data to determine ineligibility for employment, credit, insurance, health care, financial aid, or housing (discrimination); charging a consumer a higher price for products/services based on personal data relating to the consumer's race, ethnicity, religion, national origin, sexual orientation or gender identity (except as permitted by existing laws applicable to the business/organization); impersonation for collection of personal data or obtaining access to a consumer's accounts, for purposes of fraud; misrepresenting/mischaracterizing products/services to induce disclosure of a consumer's personal data; using personal information to defraud a consumer; using personal data in pursuit of criminal activity; or retaliating against a consumer for exercising their privacy rights;
- include the privacy rights commonly found in state laws -- notice, access, deletion, correction, portability, and opt-out -- with reasonable verification requirements;
- require privacy notices, made available in a clear and conspicuous manner, that explain what personal data will be collected, processed, and disclosed, the categories of entities that may receive data, and for what purposes data will be processed and disclosed;

[3] "Europe's GDPR privacy law is headed for red tape bonfire within 'weeks'." Politico. April 3, 2025. https://www.politico.eu/article/eu-gdpr-privacy-law-europe-president-ursula-von-der-leyen/

- define personal data as "any information that is linked or reasonably linkable to an identified or identifiable individual," but exclude aggregated, de-identified, and publicly available data;
- demand consent for personal data that is truly "sensitive";
- make exceptions in certain circumstances, such as for pseudonymous data,[4] and for customer fulfillment, and other routine and essential data practices;
- require assessments of business/organization data practices, and risk assessments, which should weigh if the costs to the consumer's privacy interests would be outweighed by the countervailing benefits to the consumer or to competition, including determining significant risk of harm to consumers, benefits provided, the impact on a business/organization's practices, the reasonable expectations of consumers, and whether risk is being mitigated; and
- facilitate FTC-approved self-regulatory compliance programs and industry standards, such as ISO, to help police the marketplace, support compliance with specific parts of the committee's legislative framework, and encourage responsible data uses (with participants in good standing getting the benefits of some protections from enforcement action).

Preemption

The U.S. needs a uniform national privacy standard. Both consumers and businesses need regulatory certainty and constistency in privacy protection, and should not have to contest with a confusing, conflicting patchwork of 20 state privacy laws.

Businesses have had to invest heavily in legal and compliance consulting and extra staff just to figure out if they are covered by certain laws, let alone how to actually deal with such laws and ensure their practices, policies and contracts concord. Even while one *general* approach is followed by a majority of the state privacy laws, the *details* can vary dramatically. A 2022 study estimated that the state patchwork (which included a lot fewer states at the time) "could impose out-of-state costs of between $98 billion and $112 billion annually," with $20–23 billion falling specifically on small businesses.[5]

Therefore, legislation from the committee should fully preempt state laws related to data privacy and security.

While that preemption should have appropriate carveouts for general consumer protection laws and specific industries, the committee should be careful to avoid loopholes, such as too-broadly carving out state health privacy laws. As happened in the 2024 APRA draft, this would mistakenly allow the continuation of the Washington My Health My Data Act, a Washington state law that is *presented* as only about health care data, but that is *written and defined so broadly that it is effectively just another conflicting comprehensive state privacy law*.

---

[4] "**Pseudonymous data**" means "personal information that cannot be attributed to a specific natural individual without the use of additional personal information, provided that such additional personal information is kept separately and is subject to appropriate technical and organizational measures to ensure that the pseudonymous data is not attributed to an identified individual."

[5] "The Looming Cost of a Patchwork of State Privacy Laws." ITIF. January 24, 2022. https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/

However, most other federal privacy laws need to be respected. The committee's framework should exclude from coverage personal data that is covered by and collected, processed, etc., in compliance with several other federal privacy laws, such as Gramm Leach Bliley, FCRA, HIPAA, COPPA, TCPA, DPPA, and more.

Enforcement

The FTC has decades of experience in consumer data privacy and security issues with a designated focus on consumer protection and a sizeable staff with expertise, so the FTC should be the primary federal regulator/enforcer of this comprehensive federal privacy legislation. Other federal agencies could provide assistance with setting standards as necessary. State AGs (or privacy enforcement authorities) would also be able to enforce the law.

Both the FTC and state authorities would punish violations with injunctive relief and civil penalties. Private rights of action would be prohibited.

While the legislation should take effect immediately upon passage into law, enforcement should be delayed a year to provide covered businesses and organizations (and enforcing authorities) a chance to prepare.

Sensitive personal data

The committee's privacy framework should require opt in consent for collecting, processing, maintaining or transferring sensitive personal data collected from a consumer. As a result, it needs to be carefully defined.

Federal bills have frequently tried to avoid definition and just defer to agencies like the FTC. The end result would always have been an extremely broad reach, since the FTC has, at least since the late 2000s, considered most personal data to be sensitive. That would not be workable.

This is also an area where state privacy laws have frequently missed the mark by capturing common demographic data -- some so common they are asked by the decennial census and the American Community Survey (ACS), such as race, ethnicity and sex – as "sensitive" personal data. Such common data are essential elements in market research, particularly for segmentation and ensuring that a study covers a statistically-representative sample of a given population. Considering this common demographic data to be sensitive and subjecting it to opt in consent requirements for sharing would limit individuals from uses of covered data that benefit them and society.

Properly defined, sensitive personal data should be narrowly focused on the actual risk associated with the data, covering such areas as:

- personal data used to identify a past, present, or future physical or mental health diagnosis of an individual;
- financial account numbers and related access information and credentials;
- government-issued identifiers;
- biometric data processed to uniquely identify the specific consumer to whom that data pertains;
- genetic data;
- neural data;

- precise geolocation data;
- phone call details;
- personal data collected from minors (13-16 year olds) when the controller has actual knowledge or willfully disregards knowledge of the consumer's age;
- video content viewing data (except for purposes of audience measurement); and
- intimate or sexually-explicit images/content that the controller actually knows pertains to an identifiable consumer.

Profiling

An increasing number of state privacy laws offer an opt out from the "profiling" of a consumer.

IA recommends defining profiling as "*any form of automated processing performed on personal information to evaluate, analyze, or predict personal aspects related to an identified or identifiable consumer's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.*"

However, to ensure that audience measurement and market research are not mistakenly construed as "profiling" (since they involve the study of individuals in order to understand groups), a caveat needs to be added to the definition: "***This term does not include profiling for purposes of market research, provided that the controller conducting the market research requires, in the applicable contracts required under this Act, all processors and third parties that will have access to the personal data to maintain and process it only for purposes of market research***."

Terms of art

Privacy laws in the U.S., Europe and elsewhere use a cacophony of generally synonymous terms: "covered data", "personal data", and "personal information"; "sensitive covered data", "sensitive data" , "special categories of personal data", and "sensitive personal information"; "covered entity", "service provider", "controller", and "processor"; and "consumer" and "individual."

Crafting a privacy policy and notices for companies that do business across multiple jurisdictions, in addition to contracts, can be a compliance nightmare as companies struggle to decide on the appropriate nomenclature. IA recommends an "interpretation clause" in the committee's legislative framework, such that referring to a term of art also captures the other synonymous terms of art in other jurisdictions:

"*Privacy policies, privacy notices and contracts may use terminology from other jurisdictions that are functionally the same as the terms in this Act, as determined by the Commission.*"

Conclusion

By clearly and consistently prohibiting the exploitation of personal data, a federal comprehensive approach to privacy regulation can directly and explicitly alleviate consumer concerns, and facilitate the compliance of businesses and organizations.

Getting the committee's legislative framework for consumer data privacy and security is critical. Getting it wrong could lead to higher costs for insights services -- costs which would be passed on to the consumers you are trying to protect, in the form of: higher prices for goods and services; lengthier time before new or better goods and services are brought to the marketplace; delayed

introduction of new or better public policies. This would all come from a decrease in the amount and quality of market research and analytics by businesses and organizations, whose decision-making capabilities would be impaired. These challenges would also pose a threat to the American economy, with U.S. companies and organizations weakened in the global marketplace by attempts to use intuition and guess-work in place of tested scientific methods.

We look forward to engaging with the Working Group, and the whole committee, to make sure that consumers are protected and respected, and businesses and organizations can continue to provide consumers the benefits of informed decision-making and innovation.

Sincerely,

Howard Fienberg
Senior VP, Advocacy
Insights Association

CC: Reps. Morgan Griffith (R-VA-09), Troy Balderson (R-OH-12), Jay Obernolte (R-CA-23), Russell Fry (R-SC-07), Nick Langworthy (R-NY-23), Tom Kean (R-NJ-07), Craig Goldman (R-TX-12), and Julie Fedorchak (R-ND).