April 7, 2025

Submitted in Word and PDF to PrivacyWorkingGroup@mail.house.gov

Honorable Brett Guthrie
United States House of Representatives
Washington, D.C. 20515

Honorable John Joyce
United States House of Representatives
Washington, D.C. 20515

RE: House Energy & Commerce Committee Data Privacy Working Group Request for Information

Dear Chairman Guthrie and Vice Chairman Joyce:

On behalf of the National Association of Professional Insurance Agents (PIA)[1], thank you for issuing the recent Request for Information (RFI), which invited members of the public to share their perspectives with the House Energy & Commerce Committee's Data Privacy Working Group (Working Group) as it considers the development of a federal data privacy and security framework.

I. Introduction. PIA's members are independent insurance agencies, many of which are small businesses whose resources would be strained or depleted by a requirement that they adhere to rules applicable to international insurance companies. PIA appreciates the Committee's recognition of the various ways business entities use consumer data and the differences in the obligations that correspond to those uses.

That said, PIA strongly supports the state-based regulation of insurance, including the array of state-based efforts to protect the misuse of insurance consumers' data. PIA's priorities are ensuring that consumer data is protected; that consumers know how their data is being used; that they have the right to limit the sharing of their data, other than for insurance-related purposes; and that they are aware of that right and given a chance to exercise it. Empowering consumers to limit the circumstances in which their data may be exploited is valuable, especially as insurance consumer data may be particularly susceptible to exploitation because of the extent to which the purchase of insurance products requires the transmission of potentially sensitive personal information. Those priorities are most meaningfully fulfilled by state insurance departments. For that reason, **PIA would oppose any federal law or regulation that would override the existing authority of the states to manage the insurance industry's use of consumer data.**

[1] PIA is a national trade association founded in 1931, which represents member insurance agents in all 50 states, Puerto Rico, Guam, and the District of Columbia. PIA members are small business owners and insurance professionals.

National Association of Professional Insurance Agents
419 N. Lee Street, Alexandria, VA 22314 ■ *main*: 703-836-9340 ■ *fax*: 703-836-1279 ■ *e-mail*: info@pianational.org ■ *web*: www.pianational.org

II. Responses to RFI Questions

a. Roles and Responsibilities. The Working Group need not produce a "federal comprehensive data privacy and security law," unless, at a minimum, such a law includes an exemption for insurance entities licensed and regulated by state insurance departments. As the RFI acknowledges, such entities are already subject to comprehensive state data privacy and security laws. Consumers are well protected by state insurance regulators; PIA urges Congress not to provide a federal agency with expansive new authority over insurance entities in violation of the McCarran-Ferguson Act, which, more than 75 years ago, codified Congressional delegation of insurance regulation to the states. In fact, the states have been the primary source of insurance regulation for over a century; McCarran-Ferguson merely formalized Congress's longstanding practice of exempting insurance regulation from most federal oversight. Current federal and state law requires Congress to yield to states' existing regulatory oversight roles. Irrespective of whether the Working Group exempts insurance licensees from such a law, it should consider the size of subject entities to avoid imposing cost-prohibitive restraints on small businesses. The definition of "small" entities could include, among other options, a threshold annual gross revenue level or a threshold number of consumers whose data is being used.

b. Personal Information, Transparency, and Consumer Rights.

i. Definitions. "Personal information" (PI) may be defined as "individually identifiable information from which judgments can be made about an individual's character, habits, finances, occupation, credit, health, or other significant personal characteristic," where such a definition would include a person's name and medical records, for example, but would not include privileged or publicly available information.[2] "Sensitive personal information" (SPI) may include race, ethnicity, religious beliefs, mental or physical health diagnoses, sexual orientation, citizenship or immigration status, or health data.[3]

ii. Disclosures. As mentioned above, state-licensed and regulated entities like insurance agents should be exempt from any federal data privacy and security law because they are comprehensively regulated by their state insurance departments. The disclosures described here should apply to federally regulated entities, which should be required to provide consumers with an electronic notification of the privacy policy governing the internal collection and/or processing of consumer information, as well as the transfer of consumer PI or SPI from one covered entity to another. Consumers should receive subsequent electronic notifications when entities' privacy policies are changed, but they need not receive more than one identical electronic notification.

---

[2] Adapted as modified from the definition of "personal information" contained in the National Association of Insurance Commissioners (NAIC) Insurance Information and Privacy Protection Model Act, Model Law #670, located at https://content.naic.org/sites/default/files/model-law-670.pdf (last viewed April 4, 2025).

[3] Adapted as modified from the definition of "sensitive personal information" contained in the Virginia Consumer Data Protection Act, located at https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/ (last viewed April 4, 2025).

III. Existing Privacy Frameworks & Protections.

a. **Existing comprehensive data privacy and security laws.** Insurance laws/regulations are most efficacious when they are developed by state insurance regulators. Every state has well-developed data privacy laws and strong consumer data protections, and states are constantly testing and strengthening those regimes. The federal passage of a statutory data privacy regimen would be, at best, confusing, burdensome, and duplicative. Like all insurance industry licensees, independent agents are regulated by their domiciliary state insurance departments[4], and their use and protection of consumer data is governed by a framework of state and federal authorities, including but not limited to applicable state regulations, the Fair Credit Reporting Act (FCRA), the 1996 Health Insurance Portability and Accountability Act (HIPAA), the 1998 Children's Online Privacy Protection Act (COPPA), and the 1999 Gramm-Leach-Bliley Act (GLBA).[5] While the state regulatory regime inevitably yields some inconsistencies around the country, the proliferation of related NAIC model laws and regulations has minimized those inconsistences, because states almost always begin their examination of these issues by referring to applicable NAIC model(s) and striving to maintain uniformity, to the extent doing so is reasonable considering their state-specific issues.

b. **Accounting for existing federal and state law.** State laws governing insurance should not be preempted by federal law on insurance data privacy and security. PIA recommends that entities subject to existing federal law addressing these same issues should not also be compelled to adhere to a redundant federal data privacy and security law. Entities that are already subject to FCRA, HIPAA, COPPA, and GLBA compliance should be deemed to be complying with any new, duplicative federal law. Such a clause would also limit the burden on state-regulated entities, as NAIC Model Law #672 was promulgated in response to the passage of GLBA and quickly generated corresponding laws and/or regulations in every single state. State-regulated entities are already required to comply with GLBA-adjacent state-level laws and regulations. Subjecting state-regulated insurance entities to a new and redundant federal law could create significant conflicts with the established insurance consumer data privacy and protection regimes governing the insurance industry pursuant to GLBA and related state laws. The state-based insurance regulatory regime provides extensive regulation of insurance licensees. Additionally, subjecting insurance

---

[4] When it passed McCarran-Ferguson, Congress delegated the task of regulating insurance entities to the states, and, since then, it has reinforced that position repeatedly. The century-plus of state-based insurance oversight has worked well for regulators, consumers, and members of the industry, in part because state insurance regulators have, comparatively, greater familiarity with and flexibility to address their residents' specific geographic and economic insurance needs.

[5] GLBA included an ultimatum that threatened the insurance industry with federal regulation of consumer data if state regulators did not develop sufficient protections within a prescribed timeframe. To facilitate the states' compliance with their new GLBA regulatory obligations, in response, the NAIC passed its Privacy of Consumer Financial and Health Information Regulation model (Model #672). As a result, all 50 states promptly developed strong insurance consumer data privacy oversight regimes that remain the law in every state. Since then, the NAIC has continued to update and modify its model law regime, and those efforts are ongoing.

Because the NAIC represents state insurance commissioners, it is better positioned than Congress to recommend insurance-specific laws and regulations, which states can customize to meet the needs of their stakeholders.

agencies to a new and redundant federal data privacy and security law would violate McCarran-Ferguson's delegation of insurance regulation to the states.

IV. **Data Security.** Congress should exempt insurance industry licensees from the requirements imposed by any bill establishing a federal data security standard. Consumers' data security will not be improved by subjecting insurance industry licensees to a new and duplicative federal data security regime, because their data is already amply secured via the state-based system of insurance regulation.

a. **Federal preemption of state law.** State laws governing insurance should not be preempted by federal law on insurance data privacy and security, irrespective of whether Congress exempts insurance licensees. Such preemption would produce a particularly unfavorable public policy for states in which existing law is more rigorous than a redundant federal law. The alternative would encourage covered businesses to "shop" between federal and state law for the most favorable treatment.
b. **Enforcement.** In developing an insurance-exempt, federal data security regime, Congress should delegate enforcement to state attorneys general. If such a regime is applicable to state insurance licensees, enforcement should be delegated to state insurance commissioners.

V. Artificial Intelligence (AI). A comprehensive federal data privacy and security law should yield to state-level AI frameworks, including the oversight of automated decision-making. Any "comprehensive data privacy and security law" will necessarily be sprawling and complex and potentially duplicative of existing law. A federal law governing the use of AI should be considered and passed independently from one governing data privacy and security.

VI. Accountability & Enforcement. Any comprehensive federal data privacy and security law should include an exemption for state regulated entities like independent insurance agencies. Covered entities could be subject to enforcement by state attorneys general and, if state licensees are not exempt, state insurance departments. Such an enforcement regime would task a state agency already overseeing state regulated licensees with the oversight of their compliance with a duplicative federal law, further illustrating the need for a state licensee exemption. In enforcing a federal law applicable to entities not already regulated by state insurance regulators, state attorneys general could consult with other state regulators for enforcement expertise and available resources.

VII. Additional Information. Even though insurance is already well-regulated by the states, Congress has spent considerable time over the past several years attempting to recreate the dependable state data privacy and security regime at the federal level. Such proposals would impose new and burdensome federal requirements on insurance agents.

a. **Ongoing concerns: federal preemption of state law and private right of action.** PIA is most concerned with provisions that would explicitly preempt existing state law and those that would grant consumers a private right of action.
b. **Persistent pursuit of federal preemption in recent Congresses.** In just the past five years, Congress has considered the American Data Privacy and Protection Act (ADPPA), which was passed by the Energy and Commerce Committee during the

117th Congress; the Data Privacy Act, which was passed by the House Financial Services Committee during the 118th Congress; and the American Privacy Rights Act (APRA), which was marked up by a subcommittee of House Energy and Commerce, also during the 118th Congress. The Data Privacy Act would have imposed unsuitably burdensome requirements on insurance agencies. Both it and the ADPPA would have improperly preempted state law on the topic of data protection, undermining the authority of existing state laws and regulations.

c. **Private right of action.** The ADPPA and several other proposals over the years have included a new and superfluous private right of action that would dramatically expand the reach of the nation's existing privacy frameworks, particularly as applied to the insurance industry. A private right of action could drastically increase litigation, choke the court system with frivolous suits, lead to higher costs for consumers, and destroy small businesses struggling to comply with increasingly duplicative, complex, draconian federal and state laws.
d. **Safe harbor.** Entities that are already required to comply with the FCRA, HIPAA, COPPA, and GLBA should be granted safe harbor from independent compliance with any new, similar law. Such a clause would limit the burden on state-regulated entities; NAIC Model Law #672 was promulgated in response to the passage of GLBA and quickly generated corresponding laws and/or regulations in every single state; as a result, state-regulated entities already effectively comply with GLBA and its state counterparts.

VIII. **Conclusion.** Because every state already has a legislative and/or regulatory regime governing the protection of consumer data, and because the NAIC is presently modernizing its GLBA model, PIA opposes the development of a prescriptive, duplicative federal structure that would improperly encroach upon state regulatory authority. Insurance is unique among the financial services in that state laws and regulations already provide robust consumer data protection, and the industry should therefore be exempted from any comprehensive federal data privacy and security law resulting from the Working Group's examination of this significant issue.

Thank you for your consideration of these important issues. We welcome the opportunity to engage in further conversation with the Working Group as its work continues.

Sincerely,

Mike Skiados

Mike Skiados
CEO
National Association of Professional Insurance Agents