Prepared Remarks of Jordan Francis, Senior Policy Counsel, Future of Privacy Forum

Joint Hearing of the House Committee on Commerce and Economic Development and the Senate Committee on Economic Development, Housing, and General Affairs
"An Educational Hearing on the Core Pillars of Privacy"

February 4, 2026

Good morning. Thank you to the members of the House Committee on Commerce and Economic Development and the Senate Committee on Economic Development, Housing, and General Affairs, for the invitation to be here today.

For a quick word about myself, my name is Jordan Francis. I am a senior policy counsel on the U.S. legislation team at the Future of Privacy Forum. FPF is a global non-profit organization that advances principled and pragmatic data protection, AI and digital governance practices. We convene leaders across industry, academia, and the public sector to provide expert analysis, benchmarking, and best practices that support responsible innovation and regulatory compliance.[1]

In my role I support expert, independent analysis of federal, state, and local consumer privacy legislation and regulation. My work focuses on tracking consumer privacy legislation, specifically comprehensive consumer privacy bills, and doing comparative analysis to help stakeholders make sense of the legislative landscape and trends.

10 minutes is far too little time to cover a complex topic like data minimization, but I hope that my testimony will provide a balanced and nuanced overview of data minimization requirements as they have historically been understood and integrated into privacy and data protection frameworks, as well as some emerging legislative trends. For more in-depth coverage of this issue, please refer to my data minimization report published last June on the FPF website.

Background on Data Minimization

With all of that said, let's get into "what is data minimization." Part of what makes it difficult to talk about data minimization is that when this topic comes up in debates around privacy legislation these days, people are usually talking not about data minimization but about a broader set of interrelated concepts.

Modern information privacy law and data protection is primarily based on a set of principles developed in the 70s and early 80s known as the Fair Information Practice Principles, or the FIPPs. These are a set of core principles and baseline rules for the collection and use of personal information that have proven extremely influential over the decades. Among those principles are collection limitation, purpose specification, and purpose limitation. These ideas are fairly straight forward. To generalize—

[1] The opinions expressed herein do not necessarily reflect the views of FPF's supporters or Advisory Board.

- You should not collect or retain personal information beyond what is in some sense necessary for your purpose;
- You have to notify someone of the purpose for using their personal information when you collect that information; and
- You have to get that person's consent to use their information for reasons that are incompatible with the purposes you disclosed to them at the time of collection.

That is data minimization in a nutshell: Do not collect more data than necessary to accomplish your identified purpose, and it connects back to these other principles. This is beneficial to consumers because it protects them from excessive, purpose-less data collection; it also helps businesses by reducing their risk exposure.

Different articulations of these principles have appeared in a variety of data protection frameworks across the globe in the last 50 years. Just to highlight a few international examples:

- The OECD's privacy guidelines, which developed in 1980 to support cross-border data flows, include these principles.
- So too does the Asia-Pacific Economic Co-operation Privacy Framework from 2015.
- The European General Data Protection Regulation includes data minimization as one of many core principles under the law. The GDPR provides that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

I want to emphasize today that while this all may sound very straightforward, a lot of significant compliance work has to happen behind the scenes to make any of this work. Data minimization is an ongoing process that requires mature data governance, including audits, mapping, and oversight. In practice, organizations must maintain current inventories of the personal data they collect, use, retain, and share, and continuously assess whether that data remains adequate, relevant, and reasonably necessary for specific, disclosed processing purposes. This process also requires data mapping to identify the systems that process personal data, document internal and external data flows, and support accountability through documentation of processing purposes, retention schedules, data classification by sensitivity, and conducting impact assessments to identify and weigh risks. Minimization also extends to vendor relationships, where controllers must ensure through contracts and oversight that vendors process data only as instructed and do not retain or repurpose it beyond what is necessary.

Technical safeguards, too, play a role. Some people might tell you that privacy means just collecting less data. But responsible data use benefits many people, and data minimization is fundamentally about whether the collection, use, retention of data extends beyond what is necessary to accomplish a legitimate purpose. There are a number of technical safeguards that can factor into that calculus in different contexts, including differential privacy, synthetic data, homomorphic encryption, or anonymization, pseudonymization and deidentification.

In short, data minimization is a continuous, behind-the-scenes accountability process—one that must remain responsive to evolving technologies, business practices, and shifting privacy risk.

Overview of Data Minimization in U.S. State Privacy Laws

Looking now specifically at the states, data minimization has become a hot topic in privacy legislative debates in recent years. To generalize both sides of these debates—I think that if you are someone who is a privacy advocate, data minimization is a natural rallying cry because data minimization means less data collection. That's very intuitive. If you are on the opposite end of the spectrum, however, and concerned about disrupting innovation and economic activity, it may sound like a threat to longstanding business practices.

I am here to provide a nuanced analysis that contrasts the different proposals floating around so that hopefully you are better equipped to understand data minimization's role in privacy if and when people come to you in support of one framework or another. This is an interesting and developing area of state privacy law, so I'll be covering how states are approaching this issue and what are the most pressing questions raised. Since 2018, nineteen states have enacted comprehensive privacy laws and this has led to what I would argue are three distinct data minimization standards across those laws.

First up we have what most states have done. It is worth noting that several states, including Iowa, Rhode Island, and Utah, do not have general data minimization requirements in their comprehensive privacy laws. But fourteen states have enacted some version of the rule that I have on the slide now: A controller must limit its collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which that data is processed, as disclosed to the consumer.

That language is actually very similar to what we saw earlier in the GDPR. The operative requirement here is a disclosed purpose—what you can collect is based on what you're telling the consumer. I call this standard procedural data minimization because it is more about the steps the controller has taken than it is about the data or the purpose itself. For data controllers, this standard provides a lot of certainty and control—if a type of data processing is necessary for your business, you can collect and process it as long as you are adequately disclosing it. This standard has come under some criticism as being less privacy protective, however, because there isn't a substantive backstop preventing a controller from overdisclosing and collecting data that a consumer may not expect. There are some natural checks and balances to that, but I won't dig deep in the interest of time.

California has taken a slightly different approach. The statutory language under the California Consumer Privacy Act is actually fairly similar to what I just described, but I would like to move right into the CCPA regulations that were published in 2023. Under the regulations, a business's collection and use of personal information has to be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed. That sounds like data minimization as it has been understood and applied for decades—be consistent with your stated purpose at collection.

But the regulations further provide that the purposes for which personal information was collected or processed must be consistent with consumer's reasonable expectations. How do you figure out what a consumer would expect? The regulations provide a handful of factors, including the relationship between the consumer and the business, the type, nature, and amount of personal information in question, the sources of the personal information, disclosures made to the consumer, and the degree to which a consumer would be aware of involvement by other parties such as service providers.

This is distinct from the procedural data minimization standard I shared a few slides ago because the disclosures that a business makes to a consumer are relevant but not dispositive. There is also an inquiry into the nature of the data itself, the relationship, and what the consumer would perceive. That is an interesting evolution of data minimization, in my opinion, and it was interpreted for the first time in an enforcement action last year.

Moving on to our final data minimization framework, Maryland added yet another data minimization standard when the Maryland Online Data Privacy Act was enacted in 2024. That law shifts the data minimization requirements from focusing on the disclosures being made to the consumer and instead looks at the nature of the product or service being offered: A controller must limit their collection of personal data to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains. For sensitive data, this is even stricter: A controller has to limit not just its collection, but also its processing and sharing of sensitive data to what is strictly necessary to provide or maintain a specific product or service requested by the consumer.

Depending on how these requirements are interpreted, this could be a significant departure from what the majority of states have done so far. Like with California's "reasonable expectations" standard, it appears to be an intentional shift towards a privacy framework that tries to align data collection more with consumer expectations than with a controller's disclosure and notice. This is very different than how I think data minimization has been understood historically, because this requirement tells you the purposes for which you can collect personal data. I call this Maryland-style rule "substantive data minimization" for that reason—the key consideration in applying the rule is the substantive purpose for which the data will be used. The labels "procedural data minimization" and "substantive data minimization" are not meant to be a value judgement on their relative strength or protectiveness. Rather, those labels are meant to describe how the rule functions.

Maryland's law takes a novel approach to data minimization, which introduces a number of important questions. When is personal data reasonably necessary to provide a product or service? What about strictly necessary? How much deference does a controller get to define its product or service and assert what it believes to be necessary? Does necessary mean that it must be essential? Does it account for business need, like profitability? What makes a product or service requested? Does clicking an "I agree" consent box count? How does this affect advertising? Product development and research? AI Model development? My data minimization report from last June unpacks those questions.

Recently, the Maryland Attorney General's released FAQs on the law, and it included a question about how to interpret these requirements. Their answer is that this will be based on the expectations of the reasonable consumer about how the data that is collected will be used. While that is not a significant clarification, it does suggest that Maryland's approach might be converging with California's, or that you can at least try to approach them similarly in compliance.

Finally, I think it is important that I clarify that Maryland is not the only law to include this kind of requirement. There are similar requirements, for example, in Washington state's My Health My Data Act and in the New York Child Data Protection Act. None of these laws, however, have been enforced yet, so we are still awaiting more detailed guidance from a regulator on how they are interpreting "necessity" in practice.

In conclusion, data minimization is a decades old concept that is common to privacy and data protection frameworks, but may mean different things to different people. Three distinct models have emerged in the states, and they all offer distinct tradeoffs. Each adds a layer or protection for consumers and each is subject to potential criticism. Hopefully after my presentation today, when stakeholders come to you to discuss data minimization you can ask them for specifics on what model they prefer, why, and how that requirement will fit in with the rest of the statutory framework, for whatever privacy legislation you consider.