A Consumer-Focused National Data Privacy Framework

April 7, 2025

Rep. Brett Guthrie (KY-02), Chairman
Rep. John Joyce, Vice Chairman
House Committee on Energy and Commerce
Rayburn House Office Building, 2125,
Washington, DC 20515

Response to the Request for Information for a Data Privacy and Security Framework

The **Consumer Choice Center** is an independent, non-partisan consumer advocacy group championing the benefits of freedom of choice, innovation, and abundance in everyday life. We champion smart policies that are fit for growth, promote lifestyle choice, and defend technological innovation.

Herein, we will offer our comments on a future data privacy and security, albeit from a consumer-focused perspective.

The APRA

The previous attempt at comprehensive privacy legislation, the **American Privacy Rights Act**, was flawed for several reasons.

While this privacy bill addressed important principles, such as **requiring transparency of data collected**, the ability for consumers to have **portable access** to their information, and mechanisms for **punishing bad actors**, it went too far in granting government agencies power over private contracts and business models while exempting any agency from those same privacy rules.

The particular provision creating a new **private right of action**, unheard of in any other global privacy bill, inevitably would have created a quagmire that would litter our justice system with bogus and outrageous claims, all the while empowering politically connected trial attorneys who stand the most to gain. This would only further increase the $500 billion "lawfare liability" tax on our economy. This ultimately would have degraded the quality and raised the prices of goods and services that consumers depend on and would do nothing to safeguard user privacy.

712 H St NE PMB 94982
Washington, DC 20002
Golden Cross House, 8 Duncannon Street
London, WC2N 4JF, UK
Rond Point Schuman 6, Box 5
Brussels, 1040, Belgium
Block D, Platinum Sentral, Jalan Stesen Sentral 2, Level 3 – 5
Kuala Lumpur, 50470, Malaysia

OUR RECOMMENDATIONS:

- Champion Innovation
- Defend Portability
- Allow Interoperability
- Embrace Technological Neutrality
- Avoid patchwork legislation
- Promote and allow strong encryption

WHAT TO AVOID

In California, the Consumer Privacy Act of 2018 requires that companies calculate the value of individual data, provide opt-outs, require companies to inform consumers if their data is being sold, allow consumers to request data be deleted (right to be forgotten), and allow consumers access to the data collected by said firms in readable formats.

Vermont's privacy law requires companies to inform consumers of data breaches directly, and also prohibits some forms of targeted advertising specifically when it comes to students.

Both of these laws contain elements of the EU's GDPR, which has now been in effect for close to 9 years. As has been noted by several analysts, the enormous compliance costs and efforts have meant a significant reduction in both investment and market activity from small and medium-sized firms that relate to data. What's more, European users have since been cut-off or blocked from using many services outside EU jurisdiction as firms are avoiding running afoul of the strict regulation. That has resulted in fewer products and services available to European citizens.

These previous attempts at privacy laws are flawed for the following reasons:

First, many parts of these laws stymie and prevent innovation. By making it more difficult and costly for firms to handle consumer data, companies are less incentivized to invest resources in innovative consumer services and offerings, resulting in less consumer choice and a higher barrier of entry for new competitors.

Second, at least in the cases of Vermont and California, these laws create a patchwork of regulation that makes compliance difficult or nearly impossible for firms operating in both the national and global marketplace, thereby driving up

712 H St NE PMB 94982
Washington, DC 20002
Golden Cross House, 8 Duncannon Street
London, WC2N 4JF, UK
Rond Point Schuman 6, Box 5
Brussels, 1040, Belgium
Block D, Platinum Sentral, Jalan Stesen Sentral 2, Level 3 – 5
Kuala Lumpur, 50470, Malaysia

costs and depriving consumers of these firms' services irrespective of which state they reside in. A national law or widely adopted (and ideally global) industry self-regulation, which protects consumer privacy and also champions innovation, would be preferred.

Third, calculating data value for each and every firm's customer and detailing every aspect of how that data is used is nearly impossible, vastly increasing costs for services that will inevitably be passed on to consumers.

Fourth, these laws do not take into consideration existing business practices that already provide adequate consumer and data protection, and have thus been used as industry standards. They also thwart innovation practices such as targeted advertising, geo-targeting, and personalization, which consumers prefer.

Last, each of these privacy laws further emboldens litigiousness, sparking new lawsuits and trials that would serve to vastly increase the cost of normal consumer products and services.

CHAMPION INNOVATION

Considering that thousands of firms have both safeguarded and used consumer data responsibly, lawmakers should seek to create clear and uniform rules that respect current standards, allow innovation, and provide clarity to both firms and consumers. Privacy rules that place an undue burden on companies following the law, rather than target the most blatant examples of data breaches and impropriety, will end up raising the cost of doing business and thus raise prices for consumers.

There should be recognition that consumers willingly give data to firms in order to receive a final service or goods that will be useful to them. As long as proper procedures are followed, and no data is leaked or changes hands without authorization, there should be no additional regulatory requirements that would serve to complicate a consumer's voluntary relationship with a firm.

DEFEND PORTABILITY

Consumer-friendly data portability should be a reasonable standard applied to most firms that complete data transactions. Most of today's firms allow personal data to be exported for review, but should also remain confidential and secure to avoid potential exploitation. If portability standards are kept too lax, this would be an

712 H St NE PMB 94982
Washington, DC 20002
Golden Cross House, 8 Duncannon Street
London, WC2N 4JF, UK
Rond Point Schuman 6, Box 5
Brussels, 1040, Belgium
Block D, Platinum Sentral, Jalan Stesen Sentral 2, Level 3 – 5
Kuala Lumpur, 50470, Malaysia

invitation to hackers and pirates looking to profit from identity or intellectual property theft.

Given the fast pace this environment changes, industry standards might be a more agile way of enforcing portability as compared to regulation.

ALLOW INTEROPERABILITY

Where necessary, firms should be incentivized to maintain open data standards that can be used between platforms where necessary. However, considering the fast-moving nature of data structures and standards, lawmakers should avoid favoring a particular method of data collection or export, whether that be JSON, HTML, or otherwise.

Rather, a broad principle of "*technological neutrality*" would allow the best standards to naturally evolve rather than be arbitrarily determined by regulatory bodies. Enforcement of interoperability standards would therefore be agreed to by firms handling data, and not necessarily determined by law. Consumers should ultimately decide if they want a service or product that either allows interoperability or not. The wide acceptance of apps and standards such as Apple CarPlay shows that most companies favor such standards that allow consumers to benefit by "plugging in".

EMBRACE TECHNOLOGICAL NEUTRALITY

Because standards and technologies change so quickly, lawmakers should avoid legislation that favors a particular method or technology in data privacy rules. Applying a uniform rule on the format or process of technology would serve to limit the amount of innovation and natural evolution that currently defines our existing tech sector.

In all cases, legislation should embrace and encourage competition and consumer preference to determine the best technology. Technology changes too quickly and too much regulation might limit new technologies and standards from emerging as fast as they could within a more flexible framework.

AVOID PATCHWORK LEGISLATION

Due to the ever-growing consumer base across both state lines and international borders, state-by-state regulations that would impose different rules on different

712 H St NE PMB 94982
Washington, DC 20002
Golden Cross House, 8 Duncannon Street
London, WC2N 4JF, UK
Rond Point Schuman 6, Box 5
Brussels, 1040, Belgium
Block D, Platinum Sentral, Jalan Stesen Sentral 2, Level 3 – 5
Kuala Lumpur, 50470, Malaysia

residents should be avoided. This patchwork of legislation would increase the cost of delivering services in an efficient manner, and would likely stunt the availability of various products or services to consumers in various jurisdictions. As such, a broad and agile uniform standard should be agreed to at the federal level, rather than individual states or municipalities.

PROTECT AND ALLOW STRONG ENCRYPTION

The use of encryption by both individuals and firms is essential to our digital rights online. Many legislative proposals since the 1990s have attempted to outlaw cryptographic methods of securing and encrypting data. Most of these proposals have been justified on national security and law enforcement grounds. That said, existing laws on judicial warrants and Fourth Amendment protections apply to firms, and there is no reason to believe that a ban on encryption would make this easier or more productive.

Lawmakers should recognize citizens' rights to encrypt and protect information and should extend this to the proprietary encryption methods that firms and companies use that serve their customers. Protecting rights to encryption is a safe and effective method to ensure consumer and data privacy can be upheld, whether that be medical data, personally-identifiable information, or financial data.

CONCLUSION

As we have outlined, there are examples of existing laws on data and consumer privacy that go far beyond the scope of consumer protection. Often, these laws serve to thwart innovation and slow down the progress that firms and companies can deliver to their customers.

What's more, a regulatory approach that is far too restrictive or cumbersome will serve large incumbent players that can afford the additional costs while locking out start-ups and new competitors.

While we cheer the focus on data and privacy framework that would benefit consumers, we hope these recommendations are taken into account.

Yaël Ossowski
Deputy Director
Consumer Choice Center
yael@consumerchoicecenter.org

712 H St NE PMB 94982
Washington, DC 20002

Golden Cross House, 8 Duncannon Street
London, WC2N 4JF, UK

Rond Point Schuman 6, Box 5
Brussels, 1040, Belgium

Block D, Platinum Sentral, Jalan Stesen Sentral 2, Level 3 – 5
Kuala Lumpur, 50470, Malaysia