The American Privacy Rights Act of 2024 ("APRA")

OVERVIEW

I am thrilled to delve into a transformative piece of legislation that aims to reshape how consumer data is handled in the United States—the American Privacy Rights Act of 2024. This measure is designed to establish comprehensive national consumer data privacy rights and set rigorous standards for data security, ensuring that individuals have greater control over their personal information in an increasingly digital world.

At its core, the Act mandates transparency from covered entities, requiring them to clearly disclose how they collect, use, and share consumer data. This transparency is crucial in building trust between consumers and companies, as it allows individuals to make informed decisions about their data.

One of the key features of this legislation is the empowerment of consumers with specific rights over their data. Consumers will have the right to access their data, correct inaccuracies, delete information they no longer want to be shared, and even export their data for use elsewhere. Additionally, they can opt out of targeted advertising and data transfers, giving them more control over how their personal information is used.

The Act also emphasizes data minimization, a principle that ensures companies collect and use only the data necessary for specific purposes. This means no more excessive data collection—companies must limit their data practices to what is essential for providing services or fulfilling legal obligations. Furthermore, the Act prohibits the transfer of sensitive data to third parties without the consumer's explicit consent, safeguarding personal information from unauthorized use.

Importantly, the legislation addresses the potential for discrimination through data use. It explicitly prohibits the use of covered data to discriminate against consumers, ensuring that all individuals are treated fairly and equitably, regardless of their personal data.

Enforcement of these provisions is robust, with multiple avenues for accountability. The Federal Trade Commission (FTC) plays a central role in enforcing the Act, alongside state attorneys general and consumers themselves, who can take legal action against violations. This multi-layered enforcement approach ensures that companies are held accountable and that consumer rights are protected.

The American Privacy Rights Act of 2024 represents a significant step forward in consumer data protection, aligning the United States with global privacy standards and addressing the growing concerns about data security and privacy in the digital age. By setting clear guidelines and empowering consumers, this legislation aims to create a safer, more transparent environment for all data transactions.

This expanded overview provides a detailed explanation of the Act's goals, key features, and the impact it aims to have on consumer data privacy and security.

The APRA was introduced by Representative Cathy McMorris Rodgers (R-WA) on June 25, 2024.

DEFINITIONS

Let's dive into some key definitions that form the foundation of this Act:

- Covered entity: This includes any entity determining the purpose and means of handling covered data, subject to the FTC Act, including common carriers and certain nonprofits. Notably, small businesses, governments, and specific non-profits are excluded from some obligations.
- Covered data: This refers to information that identifies or is linkable to an individual or device, excluding de-identified data, employee data, and publicly available information.
- Sensitive covered data: This is a subset of covered data, encompassing government identifiers, health and biometric information, financial data, and more, with specific protections in place.
- Large data holder: Defined as entities with significant revenue and data handling responsibilities, impacting millions of individuals or devices.
- Small business: These are businesses with limited revenue and data handling, exempt from many requirements of the Act.
- Targeted advertising: This involves displaying ads based on individual preferences but excludes first-party and contextual advertising.

DATA MINIMIZATION

The Act enforces strict data minimization principles, ensuring entities only collect and use data necessary for providing requested services or communications. Notably, biometric and genetic data require explicit consent for collection and transfer. The FTC will guide what constitutes reasonable data minimization, ensuring First Amendment freedoms remain intact.

TRANSPARENCY

Transparency is a cornerstone of this Act. Covered entities must maintain publicly accessible privacy policies detailing their data practices. These policies must be clear, multilingual, and accessible to individuals with disabilities. Any material changes to policies require advance notice and the option for consumers to opt out.

CONSUMER CONTROLS OVER COVERED DATA

Consumers are empowered to control their data. Upon request, they can access, correct, delete, or export their data. Entities must comply within set timeframes, ensuring accessibility for individuals with disabilities. The FTC will issue guidance on these controls, with specific exceptions outlined for denying requests.

OPT-OUT RIGHTS AND CENTRALIZED OPT-OUT MECHANISM

Consumers have the right to opt out of data transfers and targeted advertising. A centralized mechanism will facilitate these opt-outs, ensuring seamless consumer experience.

INTERFERENCE WITH CONSUMER RIGHTS

The Act prohibits using dark patterns to mislead consumers or impair their rights. It ensures that rights are exercised without misleading statements or representations.

PROHIBITION ON DENIAL OF SERVICE AND WAIVER OF RIGHTS

Entities cannot retaliate against consumers for exercising their rights. Loyalty programs are allowed, but participation requires explicit consent.

DATA SECURITY AND PROTECTION OF COVERED DATA

Entities must establish data security practices proportionate to their size and data sensitivity. The FTC, in consultation with the Department of Commerce, will interpret these requirements.

EXECUTIVE RESPONSIBILITY

Covered entities must appoint privacy or data security officers, with large data holders facing additional reporting and assessment requirements.

SERVICE PROVIDERS AND THIRD PARTIES

Service providers must adhere to covered entity instructions and maintain data security, with due diligence required for selecting providers.

DATA BROKERS

Data brokers must maintain a public website and are prohibited from misusing data. The FTC will establish a data broker registry to enhance transparency.

CIVIL RIGHTS AND ALGORITHMS

The Act prohibits discrimination through data use, with specific requirements for large data holders using algorithms.

OPT-OUT RIGHTS FOR CONSEQUENTIAL DECISIONS

Consumers can opt out of algorithmic decisions affecting critical areas like housing and employment.

COMMISSION-APPROVED COMPLIANCE GUIDELINES

The FTC will approve compliance guidelines, offering entities a rebuttable presumption of compliance.

PRIVACY-ENHANCING AUDITS PILOT PROGRAM

A pilot program encourages the use of privacy-enhancing technologies, with entities gaining compliance presumptions.

ENFORCEMENT BY THE FEDERAL TRADE COMMISSION

The FTC will enforce the Act, establishing a new bureau and a relief fund for consumers.

ENFORCEMENT BY STATES ATTORNEYS GENERAL

State attorneys general can enforce the Act, seeking various forms of relief.

ENFORCEMENT BY INDIVIDUALS

Consumers can file lawsuits for privacy violations, with specific provisions for damages and arbitration.

PREEMPTION

The Act preempts certain state laws, preserving others, and aligns with federal privacy laws.

COPPA

The Act does not alter obligations under the Children's Online Privacy Protection Act.

This summary provides a comprehensive overview of the American Privacy Rights Act of 2024, highlighting its key components and implications for consumer data privacy and security.

TEXT OF BILL

A complete text of the APRA may be found at: https://www.congress.gov/bill/118th-congress/house-bill/8818/text.

CONCLUSION

As we wrap up this paper on the American Privacy Rights Act of 2024, it is clear that this legislation marks a pivotal moment in the evolution of data privacy and security in the United States. By establishing comprehensive consumer data privacy rights, the Act empowers individuals with greater control over their personal information, ensuring that their data is handled with transparency and respect.

Key takeaways from this legislation include:

- Empowerment of Consumers: The Act grants consumers the right to access, correct, delete, and export their data, as well as opt out of targeted advertising and data transfers. These rights put individuals in the driver's seat, allowing them to make informed decisions about their personal information.
- Data Minimization and Security: By enforcing data minimization principles, the Act ensures that companies collect only what is necessary and protect sensitive data with stringent security measures. This approach reduces the risk of data breaches and unauthorized use.
- Prohibition of Discrimination: The Act prohibits the use of data to discriminate against consumers, promoting fairness and equality in data practices across all sectors.
- Robust Enforcement: With enforcement by the FTC, state attorneys general, and consumers, the Act provides multiple layers of accountability, ensuring that violations are addressed promptly and effectively.
- Alignment with Global Standards: By aligning with international privacy standards, the Act positions the United States as a leader in data privacy, fostering trust and confidence in the digital economy.

In conclusion, the American Privacy Rights Act of 2024 is a forward-thinking piece of legislation that addresses the challenges of the digital age. It balances the needs of businesses with the rights of consumers, creating a framework that enhances privacy, security, and trust. As we move forward, it will be essential for all stakeholders to engage with these new standards, ensuring that the benefits of digital innovation are realized without compromising individual privacy.

Walt Green
walt.green@phelps.com
Phelps Dunbar LLP