February 24, 2023

TO: Members, Subcommittee on Innovation, Data, and Commerce
FROM: Committee Majority Staff
RE: Hearing Entitled "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy"

I. INTRODUCTION

The Subcommittee on Innovation, Data, and Commerce will hold a hearing on Wednesday, March 1, 2023, at 8:30 AM in Rayburn 2123. The hearing is entitled "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy."

II. WITNESSES

- Alexandra Reeve Givens, President and CEO, Center for Democracy & Technology
- Graham Mudd, Founder and Chief Product Officer, Anonym
- Jessica Rich, Of Counsel and Senior Policy Advisor for Consumer Protection, Kelley Drye & Warren, LLP

III. BACKGROUND

A. LEGISLATIVE ACTION AROUND THE WORLD

Data is central to commerce in the 21st century economy. It provides opportunities for businesses to make informed decisions and develop products responsive to customer feedback. Due to the digitization of our society, data has become more readily available to collect and use, and as a result more difficult for the individual whose data is collected and used to ultimately track. As a result, countries across the globe have enacted privacy and data security legislation dictating how businesses and entities can collect, use, and transfer data as well as providing their citizens with more control over their data.

In 1970, a German state enacted the world's first Data Protection Act and other states followed suit, creating the impetus for the first German Federal Data Protection Act in 1978.[1] Forty years later, the European Union enacted the General Data Protection Regulation (GDPR),

[1] Germany has given rise to two political systems in which the surveillance of its own people played a fundamental part in their control, manipulation and oppression – this history has made data privacy critically important for Germans. *See*, Olga Stepanova et. al, *The Privacy, Data Protection and Cybersecurity Law Review: Germany*, The Law Reviews (October 27, 2022).

which became the leading model for the world.[2] As of 2021, 137 out of 194 countries have put in place legislation to secure the protection of data and privacy within the bounds of their country.[3]

While other countries have led to provide protections for their citizens' data privacy, the United States has failed to enact the same broad protections.[4] While Congress has enacted sectoral laws for specific industries, for instance, the Gramm Leach Bliley Act (GLBA), which regulates financial institutions,[5] many of these sectoral laws are limited to notices on how user data is used and grant limited opportunities for consumers to opt out. In the absence of Federal action on comprehensive privacy and data security legislation, five States have enacted broad privacy and data security laws that vary in scope, protections, obligations, and enforcement mechanisms.[6] To ensure all Americans receive strong privacy and data security protections, and all businesses have clear rules of the road to operate within, the U.S. must enact a comprehensive and preemptive privacy and data security law so that it can maintain its leadership on the world stage.

This hearing will examine how personal data is currently treated and handled in today's digital ecosystem and the dangers facing the U.S. if Congressional inaction continues.

B. THE PROBLEM

Without a comprehensive federal standard governing how companies can collect, process, and transfer data, Americans find it challenging to know which entities have their data and how their data is being used, in many cases, for purposes beyond what they expect. With each passing year, privacy policies have become so convoluted and extensive that the average American may not fully comprehend what they are agreeing to or even take the time to read. Additionally, without a comprehensive federal standard, there are insufficient limits to what types of data companies may collect, process, and transfer.

This problem is exacerbated when companies provide or sell data to data brokers.[7] Data brokers are companies whose primary business is collecting personal data from various sources ranging from traffic tickets to property data to purchase history. They process, aggregate and analyze the personal data to make inferences about specific consumers. These consumer insights are then sold or licensed to individuals or companies for purposes such as marketing products or verifying an individual's identity.[8] Significantly, data brokers do all this without interacting with

[2] Bahrain, Israel, Qatar, Turkey, Kenya, Mauritius, Nigeria, South Africa, Uganda, Japan, New Zealand, South Korea, Argentina, Brazil, Uruguay, and Canada have all enacted national legislation similar to GDPR. *See*, Mike Woodward, *16 Countries with GDPR-like Data Privacy Laws*, Security Scorecard (July 8, 2021). *See also*, *Adequacy decisions*, European Commission (Accessed February 17, 2023).
[3] *Data Protection and Privacy Legislation Worldwide*, UNCTAD (December 14, 2021).
[4] The French data privacy regulator, the CNIL, labeled the U.S. as a country that does not ensure an adequate level of data protection recognized by the EU. *See*, *Data protection around the world*, CNIL (November 15, 2022).
[5] Gramm-Leach-Bliley Act, available at: https://www.congress.gov/bill/106th-congress/senate-bill/900
[6] Rajesh De et. al, *Connecticut Passes Comprehensive Privacy Law: Comparing to Other States*, Mayer Brown (May 11, 2022).
[7] Yael Grauer, *What are 'Data Brokers,' and Why Are They Scooping Up Information About You?*, Vice (March 27, 2018).
[8] Edith Ramirez et. al, *Data Brokers A Call for Transparency and Accountability*, Federal Trade Commission (May 2014).

the consumer directly. Therefore, consumers have little awareness of the marketplace for their personal data.[9]

The data broker industry is a multibillion-dollar economy selling consumers' data with virtually no restrictions or oversight.[10] The biggest brokers tout the details of their data on millions or even billions of people,[11] which powers their ability to create remarkably specific and rich consumer profiles with enough information to link sensitive data to real people. Numerous websites populate the internet where someone may go to purchase this data, without any regard to the verification on how they may use the information.

C. DATA SECURITY

For the last decade, Americans have been flooded by reports and breaking news related to ransomware attacks perpetrated by both private entities and state sponsored entities. When American's data is in the hands of nefarious actors it can be used for a variety of harmful purposes. For example, consumer data can be used to steal someone's identity. Identity theft can allow nefarious actors to gain access to a consumer's secure accounts, set up credit cards using the consumers name, or otherwise use the victim's identity to benefit themselves and wreak havoc on the consumer's life.[12] Nefarious actors can also sell consumer data on black market websites where data is illegally bought and sold.[13] This data can be bought by cybercriminals or state actors and government entities.[14]

To protect American's data effectively, any comprehensive federal standard must include rigorous data security protections and privacy by design requirements for businesses to consider how they are collecting, processing, and transferring personal data. Data minimization requirements can also assure that companies are not collecting more information than they need, which guarantee less personal information is available for cybercriminals to breach.

D. DIGITAL ADVERTISING ECOSYSTEM

American's data in the hands of companies can be used for a variety of purposes. As advertising has given birth to innovation in support of new business models, companies can use consumer data to make products better by incorporating user behaviors into product design to make the consumer experience better.[15] Conversely, companies can use the data they collect to

---

[9] Apple ran a commercial that does a good job presenting the mostly invisible consumer data marketplace. *See*, *Privacy on iPhone | Data Auction*, Apple via YouTube (May 18, 2022).
[10] Justin Sherman, *Data Brokers Are a Threat to Democracy*, Wired (April 13, 2021).
[11] For example, CoreLogic advertises its real estate and property information contains 99.9% of the U.S. population. *See*, *Property Data Solutions*, CoreLogic (Accessed February 17, 2023).
[12] *What is data theft and how to prevent it*, Kaspersky.
[13] Robert Elgart, *The Data Black Market: Where Hackers Take Stolen Data*, Turn-Key Technologies (August 5, 2019).
[14] Senator Wyden has been investigating the U.S. government's purchase of American's data without judicial authorization for several years. *See*, Ron Wyden, *Letter to Inspector Generals of DHS, DOJ & DOD*, United States Senate (September 21, 2022).
[15] Anne Taylor, 4 ways to create better customer experiences with data, CIO (August 1, 2022).

monetize their customers as an additional revenue stream, or for companies that operate a "freemium" business model, [16] monetizing consumer data can be their primary revenue stream.

Companies primarily monetize American's data through digital advertising, utilizing two main categories of digital advertisements. The first method companies may use is contextual advertising, a technique which creates and ensures the content on an advertisement depends on or relates to the content on a webpage.[17] The second method is targeted advertising, a practice which involves the use of previously collected data on a consumer, whether that be from historical online activity or real world interactions, to deliver specific advertisements.[18] With no regulation to disincentivize what information a company can collect, they have been able to collect vast amounts of data on Americans.

In 2006, the digital advertising ecosystem transformed through the advent of social media, which provided advertisers looking to reach specific demographics and users with a rich data profile and method to do so. This led to the current digital advertising ecosystem and online environment where consumers receive more targeted advertisements as opposed to the traditional contextual advertisements. [19] The more data collected from Americans translated directly to the increase in hyper specialized ads, which to many Americans, felt like an invasion of privacy.[20]

This invasion feels worse when the same targeted ad follows you around the internet in a practice known as retargeting – a form of targeted advertising that serves ads to people who have already visited a website or are in a company's database. There are two main types of retargeting: pixel-based and list-based.[21] The pixel-based retargeting practice starts when a consumer enters a website, a cookie is added to the consumer's browser to remember which pages the consumer has viewed.[22] When the consumer leaves the website to surf the web, that cookie notifies retargeting platforms to serve specific ads based on the specific pages the consumer visited on other websites, allowing ads to retarget consumers immediately after they leave the original website, giving the consumer a feeling that they are being followed. A company will upload a list of email addresses or phone numbers to a retargeting campaign, usually on a social network, and the platform will identify users on that network who have the same email address or phone number and serve retargeting ads just to them.

Advertising in the digital age has prompted Americans to question how their information is collected, processed, and transferred. Many Americans certainly appreciate the ease of shopping online that comes with different advertising practices. However, the American people deserve more transparency into the ways in which theses targeted advertising practices exploit their data and should be granted more autonomy to decide how they want to participate in the digital advertising ecosystem.

---

[16] "Freemium" is a combination of "free" and "premium". It has become the dominant business model among internet start-ups and smartphone app developers. Users get basic features at no cost and can access richer functionality for a subscription fee. *See*, Vineet Kumar*, Making "Freemium" Work*, Harvard Business Review (May 2014).
[17] *Contextual vs Behavioral vs Audience Targeting: A Full Comparison*, AdButler (July 25, 2022).
[18] Id.
[19] Karla Hesterberg, *A brief History of Online Advertising*, HubSpot (November 29, 2021).
[20] *New Survey Reveals that Consumers want Digital Ads to Carry a "Privacy Guaranteed" Seal*, Businesswire (December 15, 2021).
[21] Dan Hecht, *What Is Retargeting? How To Set Up an Ad Retargeting Campaign*, HubSpot (August 5, 2021).
[22] Katie Broida, *What Is Cookie Tracking*?, HubSpot (May 9, 2018).

E. AMERICANS SUPPORT DATA PRIVACY LEGISLATION

Despite not having a complete understanding of all the ways in which digital devices and services track consumers,[23] a majority of Americans still believe their online and offline activities are being tracked and monitored by companies and the government with some regularity.[24] It is such a common condition of modern life that roughly six-in-ten U.S. adults say they do not think it is possible to go through daily life without having data collected about them by companies or the government.[25]

Due to the ubiquitous, insidious, and pervasive nature of data collection and Americans' increasing awareness of these practices, data privacy and security has become a major concern. A recent study reveals that nearly all Americans surveyed (92%) believe it is important for Congress to pass new legislation to protect consumers' personal data, and 4-in-5 voters (81%) support a national standard that outright prohibits harmful ways of collecting, using and sharing personal data.[26]

F. PRIVACY ENHANCING TECHNOLOGIES

In a world where Americans value their privacy and data security, businesses need to explore new and innovative technologies that can both provide value for their business in addition to protecting the privacy of their customers and users. Previously this proposition was a trade-off that needed to be made but with the advent of privacy enhancing technologies (PETs) companies can do both - extract value from American's data while maintaining their privacy.
PETs are a growing suite of tools that can help maximize a company's use of data by reducing risks inherent to data use, especially data related to consumers. Some PETs provide new tools for anonymization, while others enable collaborative analysis on privately held datasets, allowing data to be used without disclosing copies of data.[27] PETs can play an important role in privacy by design approaches to data governance and are already being used in a variety of commercial applications.

G. RELEVANT COMMITTEE ACTION AND PREVIOUS LEGISLATION

THE AMERICAN DATA PRIVACY AND PROTECTION ACT

Reps. Pallone (D-NJ), Rodgers (R-WA), Schakowsky (D-IL), and Bilirakis (R-FL) introduced H.R. 8152, the "American Data Privacy and Protection Act" (ADPPA) on June 21, 2022, and subsequently passed it out of Committee by a 53-2 vote. ADPPA is the first bipartisan, bicameral national comprehensive privacy and data security proposal with support from leaders on the House Energy and Commerce Committee and the Senate Commerce, Science, and Transportation Committee.

---

[23] Natasha Singer et. al, *Americans Flunked This Test on Online Privacy*, The New York Times (February 7, 2023).
[24] Brooke Auxier et. al, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (November 15, 2019).
[25] Ibid.
[26] *New Data Reveals Americans' Overwhelming and Bipartisan Support for Federal Privacy Legislation*, Privacy for America (November 18, 2021).
[27] Alison Noble, *From Privacy to Partnership – the role of privacy enhancing technologies in data governance and collaborative analysis*, The Royal Society (January 2023).

The legislation establishes a preemptive national consumer privacy and data security framework built around limitations for collecting, processing, and transferring individuals' information, obligations for covered entities and service providers, and providing individuals with control with respect to their personal information. Certain covered data is considered sensitive and subject to additional restrictions and there are further protections for Americans under 17 years old. Covered entities may not use covered data in any manner that discriminates or makes unavailable the equal enjoyment of goods or services on the basis of protected classes. Large businesses are subject to additional requirements, while small and midsize businesses are exempted from certain provisions and eligible to participate in certain technical compliance programs. H.R. 8152 provides for federal, state, and private enforcement.

H. ISSUES

- How will the emerging patchwork of state data privacy laws impact business that operate in the digital economy?
- Should a federal standard preempt state laws that would not be covered within such standard?
- What is the difference between a company using first party data for advertising and transferring such data to a third party for advertising?
- Why are safe harbors important for complying with federal law?
- What aspects of other countries data privacy laws are too restrictive?
- Why should Congress enact legislation that would establish comprehensive privacy and data security protections as opposed to rulemakings, or a continued state by state approach?

STAFF CONTACTS

- Tim Kurth, Chief Counsel
- Teddy Tanzer, Senior Counsel
- Brannon Rains, Professional Staff Member
- Michael Cameron, Professional Staff Member
- Lacey Strahm, Technology Fellow
- Jessica Herron, Clerk