CITIZENS AGAINST GOVERNMENT WASTE

Thomas A. Schatz, *President*
1100 Connecticut Ave., N.W., Suite 650
Washington, D.C. 20036
cagw.org

November 8, 2018

Mr. David Redl
Administrator
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Attn: Privacy RFC
Washington, D.C. 20230

Re: Comments on Developing the Administration's Approach to Consumer Privacy (Docket Number: 18021780-8780-01)

Dear Administrator Redl,

On behalf of the more than one million members and supporters of Citizens Against Government Waste, I offer the following comments and recommendations on ways to advance consumer privacy while protecting prosperity and innovation in response to the Request for Comments on Developing the Administration's Approach to Consumer Privacy (Docket Number: 180821780-8780-01).

Policymakers and individual Americans have become increasingly concerned about the amount of personal information held by online platforms, e-commerce sites, internet service providers (ISPs), banking institutions, retailers and many others, and how such information is being used for data analytics, online advertising, and targeted messaging without adequate transparency or consumer choice by social media companies and online search engines. This concern was underscored after the 2016 elections when it was revealed that Cambridge Analytica used ill-gotten personal data for targeted political ads.

Furthermore, new technologies, including automated license plate readers, event data recorders in vehicles, and radio frequency identification, are making it easier to track, collect, access, and repurpose or manipulate personal information.

The United States has enacted several laws that contain provisions governing how personal information should be protected using an industry-by-industry approach, including the Communications Act of 1934, the Electronic Communications Privacy Act, the Children's Online Privacy Protection Act, the Driver Privacy Act, the Family Educational Rights and Privacy Act, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, the Wire Act, and

the Video Privacy Protection Act. There is no single law or federal agency for protecting consumer privacy. The most prominent agency entrusted with protecting consumer privacy are the Federal Trade Commission (FTC).

On April 14, 2016, the European Parliament adopted the General Data Protection Regulation (GDPR). The GDPR entered into force on May 24, 2016, and its provisions became directly applicable to all member states on May 25, 2018. The GDPR imposes requirements for data protection by businesses or other entities that process the personal data of individuals in the member states of the European Union, regardless of where the data processing takes place.[1] This includes U.S. companies conducting business in the E.U. These U.S. companies need to be able to rely on a U.S. framework that facilitates trade and data transfer around the world, including with Europe.

On June 28, 2018, the California Consumer Privacy Act was signed into law by Governor Jerry Brown. The bill, which was rushed through the legislature in a few days, imposes extremely onerous requirements on how companies must store and provide access to consumers' personal information, as well as harsh restrictions on the types of product and service options and discounts companies may offer to their customers. Other states have enacted or are reviewing laws that would purportedly protect personal information, covering issues such as children's online privacy, website privacy policies, and monitoring employee e-mail communications. There is an overriding concern that without the adoption of a consistent national privacy protection regime that preempts state and local laws, more states will follow California's example, further complicating the privacy regulatory environment that companies, large and small, must negotiate.

CAGW offers the following recommendations for consumer-based privacy:

1. National Privacy Framework: Because of the unique nature of the internet ecosystem and its presence beyond state borders, a clear and concise national data privacy framework is necessary to provide consistency and certainty for businesses and consumers alike.
2. Consumer Choice and Control: Businesses should provide consumers with easy-to-understand privacy choices based on the sensitivity of their personal data and how it will be used or disclosed, consistent with the FTC's privacy enforcement guidance. Businesses should provide consumers with an opt-out choice to use their non-sensitive customer information for personalized third-party marketing. Businesses should be able to continue to rely on implied consent to use customer information for activities such as service fulfillment and support, fraud prevention,

[1] Roslyn Layton, "The GDPR: What It Really Does and How the U.S. Can Chart a Better Course," Federalist Society Review, Volume 19, October 29, 2018, https://fedsoc.org/commentary/publications/the-gdpr-what-it-really-does-and-how-the-u-s-can-chart-a-better-course.

market research, product development, network management and security, compliance with the law, and first-party marketing.

3. Transparency: Consumers should be provided with clear, comprehensible, accurate, and continuously available privacy notices by businesses collecting, using, or sharing consumer data that describe in detail the information being collected, how that information will be used, and whether the information will be sold or shared with third parties. Should customer information be sold or shared with a third party, customers must be notified about the types of third parties to whom their information has been given and for what purpose.
4. Data Minimization and Contextuality: Consumers should expect reasonable limits on the amount of personal data that organizations will collect, use, and disclose, consistent with the context in which that data is provided. Every effort should be made to de-identify and delete data as promptly as possible when it is no longer necessary.
5. Flexibility: Different types of data require separate methods and standards of protection. For example, sensitive health care data and financial data require a higher level of security than a social media account or a computer's IP address. Therefore, policies must be consistent with the type of data being collected and how it is to be used.
6. Data Security and Breach Notification: Consumers should expect that the personal data they share with other entities is maintained in a secure environment. Information technology systems are under constant attack; breaches have and will continue to occur. In the event of a data breach in which there is a reasonable likelihood of misuse and consumer harm, consumers should expect timely notification of the event, and an offer by the entity breached as to the remedies available to make the consumer as whole as possible, including credit protection services, fraud alerts, and credit monitoring through credit reporting agencies.

We appreciate the opportunity to provide you with our views and recommendations. If you have any questions or concerns, please feel free to contact either myself, or CAGW Technology and Telecommunications Policy Director Deborah Collier at (202) 467-5300. Thank you.

Sincerely,

Tom Schatz