PRIVACY FOR AMERICA: Creating a Strong New Paradigm for Privacy and Responsible Data Use

Americans deserve to have strong and effective privacy protections to prevent companies from using their data in ways that are unexpected and harmful. They should not be forced to choose between protecting their privacy and enjoying the many benefits we have all come to expect – benefits like access to a wide array of online content and mobile services and discounts on goods and services that matter to users. And they deserve to have the same high level of privacy protections no matter where they live in the country.

To meet this challenge, the United States needs a strong new paradigm for ensuring consumer data privacy protection. Privacy for America will support enactment of federal legislation that would clearly define prohibited data practices that make personal data vulnerable to breach or misuse, while preserving the benefits that come from the responsible use of data. The framework would set forth comprehensive, clear and enforceable privacy rules for the entire nation. This framework would create new national protections for consumers backed by enforcement and strict penalties for those who do not comply. The legislation would shift the burden from consumers by allowing them to depend on these strong national standards without having to rely on reading hundreds of lengthy privacy policies in order to protect themselves.

We support legislation that would:

1. **Protect Consumers Nationwide.** The new law will provide, for the very first time, broad-based privacy rules for the entire U.S. marketplace. To date, privacy in the U.S. has been addressed through a patchwork of state and federal laws and industry self-regulation that leave gaps in consumer protection.

2. Establish New Prohibitions on Certain Data Practices. Rather than asking consumers to read the "fine print" in order to protect themselves, the new law would ban outright a wide range of harmful and unexpected data practices, including:

- ✓ *Eligibility* – Using a person's data to turn them down or set unfavorable terms for a job, credit, insurance, healthcare, education, or housing, unless specifically permitted under existing federal and state laws governing such benefits.

- ✓ *Discrimination* – Using personal characteristics such as race, color, or religion to discriminate against a consumer in setting prices or determining eligibility for products and services.

- ✓ *Assisting and facilitating fraud* – Sharing consumer data with another company with reason to know that it will be used to defraud a consumer.

✓ ***Sensitive data*** – Collecting or using sensitive data – including medical, financial, biometric, and precise geolocation data, as well as email communications and private recordings – without the permission of the consumer to whom the data relates, with limited exceptions.

✓ ***Vendor and third party oversight*** – Sharing consumer data with vendors or third parties without entering into enforceable contracts ensuring their lawful use of the data.

3. Create a New Data Protection Bureau to Strengthen Privacy Oversight and Enforcement. The new law would significantly strengthen privacy oversight and enforcement by creating a new Data Protection Bureau at the Federal Trade Commission (FTC), in order to enhance the FTC's longstanding expertise in overseeing privacy issues. In addition, the FTC will be provided with additional privacy staff and resources and privacy jurisdiction over common carriers and nonprofits.

4. Grant Enhanced Rulemaking Authority to the FTC. Recognizing that new data practices will arise over time, the new law would set forth specific criteria for the FTC to identify and prohibit additional data practices through rulemaking.

5. Ensure Responsible Advertising Practices. Many consumers welcome information about products and services they enjoy, but some are concerned about the scope of data collected and the risk that such data could be misused. The new law would impose significant restrictions on data use for advertising – including banning certain types of data from being collected and used for advertising, limiting the purposes for which advertising data may be used, and allowing consumers to identify their preferences regarding what advertising they do or do not wish to receive.

6. Require Strong Data Security Protections. Currently, despite the massive data breaches that have occurred over the last decade, data security laws in this country still apply to only a few sectors of the economy. The new law would impose, for the very first time, robust security requirements, including the adoption of required security mechanisms, on virtually every company in this nation. Our goal is to make universal the adoption of automatic mechanisms that will have the impact that seat belts and air bags had on auto safety.

7. Authorize Strict Penalties for Violations. Currently, the FTC's authority to obtain penalties for privacy and data security violations is too limited. The new law would authorize both the FTC and State Attorneys General to seek in some cases new penalties against companies that violate it.

Next Steps:
In the coming weeks and months we will call on Americans and all companies and sectors of the U.S. economy to join with us in support of a new law that furthers these goals.

We will work with the Congress, the FTC, the Department of Commerce, the White House, consumers, and other stakeholders to drive the consensus necessary for enactment of the law.