SUMMARY OF WHITE HOUSE PRIVACY FRAMEWORK

Consumer Data Privacy in a Networked World:
A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy

OVERVIEW

The White House, in conjunction with the Department of Commerce and Federal Trade Commission, released its long-awaited white paper on consumer data privacy in a digital age. The centerpiece of the paper is a Consumer Privacy Bill of Rights. The Privacy Bill of Rights consists of seven principles:

- ***Individual control*** over what data is collected from consumers and how it is used.
- ***Transparency*** regarding privacy and security practices.
- Treat personal data in a manner consistent with the ***context*** in which it is provided by consumers.
- ***Security*** concerning handling of personal data.
- ***Access*** rights to ensure accuracy of personal data maintained on consumers.
- ***Focused collection*** that limits the personal data that companies collect and retain.
- ***Accountability*** to ensure that personal data is handled in accordance with the Bill of Rights.

Later this year, the Administration will convene a multi-stakeholder process to implement the Bill of Rights through codes of conduct that would be enforceable by the Federal Trade Commission and State Attorneys General.

The Administration will also work with Congress to implement these rights through legislation, also enforceable by the FTC and State Attorneys General, which would include a safe harbor for compliance with codes of conduct that embody the Privacy Bill of Rights. "Inconsistent" State laws would be preempted. The Administration also supports enactment of a national uniform breach notification standard.

As contemplated by the Administration, the legislation would generally preserve existing Federal sector-specific privacy laws, such as those applicable to education, credit reporting, financial services, health care, and children's personal data. On the other hand, existing Federal laws that create "inconsistent or confusing" requirements – such as the current privacy laws governing communications common carriers, cable operators, and satellite carriers – would be "simplif[ied] and "clarif[ied]." Left unstated is precisely the extent to which the new legislation would replace or supplement these latter statutes. Even within sectors subject to existing privacy laws, however, activities that do not fall under those laws would be covered by the proposed legislation.

The paper also addresses increasing global interoperability between the U.S. consumer data privacy framework and other countries' frameworks.

SUMMARY

Consumer Privacy Bill of Rights

The Consumer Privacy Bill of Rights applies to commercial uses of "personal data."

Definition of Personal Data. Any data, *including aggregations of data, which is linkable to a specific individual*. Personal data may include data that is linked to a specific computer or other device (*e.g.*, an identifier on a smartphone or family computer that is used to build a usage profile is personal data).

1. Individual Control. Consumers have a right to exercise control over what personal data companies collect from them and how they use it.

Control Over Personal Data. A company that deals directly with consumers should give them appropriate choices about what personal data the company collects, irrespective of whether the company uses the data itself or discloses it to third parties. Consumer-facing companies that contract with third parties that gather personal information directly from consumers (as is the case with online advertising) should diligently inquire about how those third parties use personal data and if they provide consumers with appropriate choices about collection, use, and disclosure.

Companies should act as stewards of personal data that they and their business partners collect from consumers. Consumer-facing companies should recognize consumer choices through mechanisms that are simple, persistent, and scalable from the consumer's perspective. Third parties should offer choices about personal data collection appropriate for the scale, scope, and sensitivity of the data collected.

Data and Third Parties. The ultimate uses of personal data that third parties, such as ad networks, collect affect the privacy interests at stake. Innovative technology can help to expand the range of user control.

Do Not Track. "Privacy-enhancing" technologies such as the "Do Not Track" mechanism allow consumers to exercise some control over how third parties use personal data or whether they receive it at all. The online advertising industry developed self-regulatory principles that provide a common interface to alert consumers of the presence of third party ads and to direct them to more information about the relevant ad network, and allow them to opt out of targeted advertising by individual ad networks. These examples are promising but require further development.

In the interim, data brokers and other companies that collect personal data without direct consumer interactions or a reasonably detectable presence in consumer-facing activities should seek innovative ways to provide consumers with effective *Individual Control*. If it is impractical to provide *Individual Control*, these companies should ensure that they implement other elements of the Consumer Privacy Bill of Rights in ways that adequately protect consumers' privacy.

Withdrawing Consent. Companies should provide means of withdrawing consent that are on equal footing with ways they obtain consent. A company must also have a way to effect a withdrawal of consent even if it has limited contact with that individual. *Data that a company cannot reasonably associate with an individual is not subject to the right to withdraw consent*. The withdrawal of consent obligation only extends to data that the company has under its control. Companies do not have to permit withdrawal of consent for personal data that they collected before implementing the Consumer Privacy Bill of Rights, unless they made such a commitment at the time of collection.

2. Transparency. At times and in places that are most useful to enabling consumers to gain a meaningful understanding of privacy risks and the ability to exercise *Individual Control*, companies should provide clear descriptions of what personal data they collect, why they need the data, how they will use it, when they will delete the data or de-identify it from consumers, and whether and for what purposes they may share personal data with third parties.

Plain Language Statements. Companies should make plain language statements about personal data collection, use, disclosure, and retention, visible to consumers when they are most relevant to understanding privacy risks and easily accessible when called for.

Personal Data Use Statement. Personal data uses that are not consistent with the context of a company-to-consumer transaction or relationship must be more prominently disclosed than uses that are integral to or commonly accepted in that context.

Device Notices. Companies should provide notice in a form that is easy to read on the devices that consumers use, and should present mobile consumers with the most relevant information in a manner that takes into account mobile device characteristics.

Companies That Do Not Interact Directly With Consumers. Companies that do not interact directly with consumers, such as data brokers, should make available explicit explanations of how they acquire, use, and disclose personal data; such disclosures could be made on their websites or other publicly accessible locations. Companies that have first-party relationships with consumers should disclose specifically the purpose(s) for which they provide personal data to third parties, help consumers to understand the nature of those third parties' activities, and whether those third parties are bound to limit their use of the data to achieving those purposes. First parties could create greater transparency by disclosing the types of personal data obtained from third parties, who the third parties are, and how they use this data.

3. Respect for Context. Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data. Companies should limit their use and disclosure of personal data to those purposes that are consistent with both the relationship that they have with consumers and the context in which consumers originally disclosed the data, unless required by law to do otherwise. While this principle emphasizes the importance of the relationship between a consumer and a company at the time the consumer discloses data, it also recognizes that the relationship may change over time in ways not foreseeable at the time of collection. The company-to-consumer relationship should guide companies' decisions about which uses of personal data they will make most prominent in privacy notices.

Respect for Context does not foreclose any particular ad-based business models. Rather, the principle requires companies to recognize that different business models based on different personal data raise different privacy risks. Thus, a company should clearly inform consumers of what they are getting in exchange for the personal data they provide.

Heightened Notice for Data Used for Other Purposes. If a company will use or disclose personal data for other purposes, it should provide heightened *Transparency* and *Individual Choice* by disclosing these other purposes in a manner that is prominent and easily actionable by consumers at the time of data collection. Such heightened notice is not, however, required for data practices that are common and integral to the company's operations.

Companies May Infer Consent To Use Personal Data To Conduct Marketing in the Context of Most First-Party Relationships. Companies may also collect and use personal data for purposes that are common (*e.g.*, preventing fraud, complying with law enforcement orders and other legal obligations, and protecting intellectual property), even if they may not be well known to consumers. If, subsequent to collection, companies decide to use or disclose personal data for purposes that are inconsistent with the context in which the data was disclosed, they must provide heightened measures of *Transparency* and *Individual Choice.*

Companies should fulfill the obligations under this principle in ways that are appropriate for the age and sophistication of consumers (*e.g.*, apply greater protections for personal data obtained from children and teens). Companies engaged in online advertising should refrain from collecting, using, or disclosing personal data that may be used to make decisions regarding employment, credit, and insurance eligibility or similar matters that may have significant adverse consequences to consumers.

4. Security. Companies should assess the privacy and security risks associated with their personal data

practices and maintain reasonable safeguards to control risks such as loss; unauthorized access, use, destruction, or modification; and improper disclosure.

5. Access and Accuracy. Companies should use reasonable measures to ensure they maintain accurate personal data. Companies should provide consumers with reasonable access to personal data that they collect or maintain about them, as well as the appropriate means and opportunity to correct inaccurate data or request its deletion or use limitation. To help consumers make more informed choices, companies should make personal data available in useful formats to the properly authenticated individuals over the Internet.

6. Focused Collection. Consumers have a right to reasonable limits on the personal data that companies collect and retain. Companies should collect only as much personal data as they need to accomplish purposes specified under the *Respect for Context* principle, however, wide-ranging data collection may be essential for some familiar and socially beneficial Internet services and applications (search engines are one example). Companies should securely dispose of or de-identify personal data once it is no longer needed, unless they are under a legal obligation to do otherwise. This principle does not relieve companies of any independent legal obligations that require them to retain personal data.

7. Accountability. Companies should be accountable to enforcement authorities and consumers for adhering to these principles and should hold employees responsible for adhering to these principles. Companies should train their employees to handle personal data consistent with these principles and regularly evaluate their performance in this regard. Companies that disclose personal data to third parties should at a minimum ensure that the recipients are under enforceable contractual obligations to adhere to the principles, unless they are required by law to do otherwise.

Companies should link evaluations to the enforcement of pre-established internal expectations. Audits, whether conducted by the company or by an independent third party, may be appropriate under some circumstances, but are not required to satisfy the accountability principle. If a company transfers personal data to a third party, it remains accountable and should hold the recipient accountable (*e.g.*, through contracts) for using and disclosing the data in ways that are consistent with the Consumer Privacy Bill of Rights.

Implementing the Consumer Privacy Bill of Rights

Multi-Stakeholder Process. Individual companies, industry groups, privacy advocates, consumer groups, crime victims, academics, international partners, State Attorneys General, Federal civil and criminal law enforcement representatives, and other relevant groups should participate in multi-stakeholder processes to develop codes of conduct that implement the general principles. Even without legislation, the Administration intends to convene and facilitate a multi-stakeholder process to produce enforceable codes of conduct that implement the Consumer Privacy Bill of Rights. National Telecommunications and Information Administration (NTIA) will serve as the convener.

Adoption of the Code. Once a code of conduct is complete, companies to which the code is relevant may choose to adopt it. The Administration expects that a company's public commitment to adhere to a code of conduct will be enforceable under the FTC's authority to prevent deceptive acts or practices, just as a company is bound today to follow its privacy statements.

Evolution. Stakeholders may decide at any time that a code of conduct no longer provides effective consumer data privacy protections, in light of technological or market changes. NTIA might also draw this conclusion and seek to re-convene stakeholders. The Federal Government would not revise a code of conduct; rather, stakeholder groups will make these changes with Federal Government input. Under the legislative safe harbor framework (see below), Congress could prescribe a renewal period for codes of conduct, so that the FTC periodically reviews

codes that are the basis of enforcement safe harbors.

Building on the FTC's Enforcement Expertise

With or without consumer data privacy legislation, the FTC should provide assistance and advice regarding development of enforceable codes of conduct. In the absence of legislation, the FTC, Federal civil and criminal law enforcement representatives, and States should participate in the multi-stakeholder deliberations. Once stakeholders have developed a code, a company may voluntarily adhere to the code. Companies may choose to adopt multiple codes of conduct to cover different lines of business; the common baseline of the Consumer Privacy Bill of Rights should help ensure that the codes are consistent. In any investigation or enforcement action, the FTC should consider the company's adherence to the codes favorably.

International Interoperability

The United States is committed to engaging with its international partners to increase interoperability in privacy laws by pursuing mutual recognition, the development of codes of conduct through multi-stakeholder processes, and enforcement cooperation. The Safe Harbor Frameworks that the United States developed with the EU and Switzerland are early examples of global interoperability that have had a meaningful impact on transatlantic data flows.

Enacting Consumer Data Privacy Legislation

Congress should codify the Consumer Privacy Bill of Rights. The legislation should state companies' obligations under the Bill of Rights with greater specificity than provided in the white paper. Legislation should avoid duplicative or overly burdensome rules; prescribing technology-specific means of compliance; or precluding new business models.

The legislation should include the following elements:

Enforcement Authority. Congress should authorize the FTC to enforce each element of the statutory Consumer Privacy Bill of Rights. Congress should grant the same authority to State Attorneys General.

Flexible Standards. Congress should adopt flexible standards rather than tailoring them to specific technologies or practices. It is important that a baseline statute provide a level playing field for companies, a consistent set of expectations for consumers, and greater clarity and transparency in the basis for FTC enforcement actions.

Safe Harbor. The FTC should be authorized to grant a "safe harbor"—forbearance from enforcement of the statutory Consumer Privacy Bill of Rights—to companies that follow a code of conduct that the FTC has reviewed and approved. Companies that decline to adopt a code of conduct, or choose not to seek FTC review of a code that they do adopt, would simply be subject to the general obligations of the legislatively adopted Consumer Privacy Bill of Rights.

Preemption/Role of the States. Congress should preempt State laws to the extent they are inconsistent with the Consumer Privacy Bill of Rights as enacted and applied. Congress should also provide forbearance from enforcement of State laws against companies that adopt and comply with FTC-approved codes of conduct. States would participate in the multi-stakeholder process, however, and State Attorneys General would have the authority to enforce the Consumer Privacy Bill of Rights. The Administration will also work with Congress, States, the private sector, and other stakeholders to determine whether there are specific sectors in which States could enact laws that would not disrupt Federal law.

As a General Matter, Preserve Existing Federal Data Privacy Laws. Consumer data privacy legislation should preserve existing sector-specific Federal laws that effectively protect personal data and provide consumers with a clear sense of what protections they have and who enforces them. Examples include the data privacy laws applicable to education, credit reporting, financial services, health care, and children's personal data. Activities that do not fall under an existing data privacy law would be covered by the proposed legislation, however.

Communications Providers Should Be Subject to FTC Enforcement of Privacy Bill of Rights. Because existing Federal laws treat similar technologies within the communications sector differently, the Administration supports simplifying and clarifying the legal landscape and making the FTC responsible for enforcing the Consumer Privacy Bill of Rights against communications providers.

National Standard for Security Breach Notification. As part of its comprehensive cybersecurity legislative package, the Administration recommended creating a national standard for notifying consumers in the event that there are unauthorized disclosures of certain types of personal data. This national standard would replace the various State standards that exist today and preempt future State legislation in this area.