



Etienne Sanz de Acedo
Chief Executive Officer

655 Third Avenue, 10th Floor, New York, NY 10017-5646, USA
t: +1-212-642-1776 | f: +1-212-768-7796
inta.org | esanzdeacedo@inta.org

Via email: privacyrfc2018@ntia.doc.gov

November 9, 2018

Mr. Travis Hall
Telecommunications Policy Analyst
Office of Policy Analysis and Development
National Telecommunications & Information Administration
U.S. Department of Commerce
1401 Constitution Ave., N.W.
Washington, D.C. 20230

Dear Mr. Hall:

The International Trademark Association (“INTA”) appreciates this opportunity to provide comments in response to the NTIA’s Request for Public Comment (“RFC”) on Developing the Administration’s Approach to Consumer Privacy published on 26 September 2018. We are pleased to provide comments directed at the proffered Privacy Outcomes in Section A and the proposed High-Level Goals for Federal Action in Section B. Our comments focus on Security, Accountability, Harmonization and Enforcement.

INTA's views on this topic are informed by its mission as an association "dedicated to supporting trademarks in order to protect consumers, and to promote fair and effective commerce."¹ Brands have always acted as shortcuts for consumers and other businesses to identify goods and services with the reputation of their provider. This has often been encapsulated in a trademark and has grown to include trade dress and more. Reputations for trustworthy goods and services extend to many business decisions captured in both non-financial and financial reporting. A reputation for securely handling customer data in understandable and transparent ways has rapidly developed into an integral part of the trust that a brand represents – especially in the area of connected devices and online services.

¹ <http://www.inta.org/About/Pages/Overview.aspx>.

INTA believes that consumer trust will only be enhanced if a voluntary Privacy Framework incorporates privacy-enhancing measures and assurances of reasonable security standards. On the other hand, consumer trust is likely to be eroded by a continued non-alignment of privacy laws and rules within the United States.

The high-level goal should be to encourage reasonably uniform data privacy rules across the United States that enable American businesses to engage in the provision of inter-state services with confidence that they are complying with a clear legal framework. As the Austrian data protection commissioner said in her evidence on 10 October, providing a single legal regime with consistent enforcement for the continent of Europe was a key driver for GDPR following the fragmentation that had grown up under the previous directive. As a result, the U.S. should be well placed both to continue to export digital services and to benefit from the receipt of services from beyond its borders.

These comments are generally organized in accordance with NTIA's 2017 survey regarding Major Concerns Related to Online Privacy and Security Risks footnoted in the RFC (the "2017 Survey"), and address Balance of Privacy Versus Security, Accountability of Data Owners and Processors, Harmonization Across Jurisdictions, and Enforcement of Regulations.

1. Privacy Versus Security

INTA prefers the term "data protection" to encompass both "privacy concerns" and the consequential "security concerns." While privacy concerns address whether data should be collected at all and who is entitled to collect what types of data, security focuses on how that data is protected after it is collected.

For brand owners to retain their customers' trust, it is important that collection and use of data be transparent and that common security standards be employed by both data owners and processors. Determining what data will be regulated by a federal standard is the first step toward determining the appropriate constraints that should be placed on the collection and securing of such data.

Published, understandable procedures around the collection and storage of personally identifiable and sensitive data are important for maintaining transparency and trust of consumers about how their data is handled. Consumers should not be surprised about what data is collected and how it is processed and used, even if they have not read a detailed privacy policy.

Certainty is also a critical factor for supporting investment in development and innovation. A Privacy Framework that makes clear distinctions between the data of individuals and that of legal entities would reduce the costs and complexity of compliance considerably. As well as excluding data related to legal entities, excluding anonymized data about user preferences which can then be used in recommendation engines and other applications will support innovations that provide “a valuable service” to the consumer.²

Regardless of what data is collected and how it is collected, consumer concerns escalate when that data is not properly secured and thus is improperly (intentionally or unintentionally) released or exposed to others. When security fails in this manner, consumers become dis-incentivized to continue providing their data for otherwise legitimate and useful purposes.

In summary, INTA believes it will be critical to properly define the types of “personal data” that will be subject to a Privacy Framework (the “Protected Data”), and consequently the types of data not subject to it. Standards and protocols must be developed to ensure it is clear to consumers when and how Protected Data is being collected and who will have access to their Protected Data and for what purposes. INTA believes that a Privacy Framework should focus on establishing and implementing state-of-the-art security protocols for collection, storage, use and transmission of Protected Data in the United States. Determining what those security protocols will be, when they require updating and how they will be implemented to maintain reasonable inter-operability with other countries and to keep up with technical advancements, will require that ongoing funding be devoted to research in this data security space.

2. Harmonization Across Jurisdictions

Turning to harmonization, brands and trademarks are used across the country and across the world by small and large businesses alike. INTA members have significant experience of engaging with customers in legal jurisdictions beyond their place of establishment. The explosion of ecommerce via the Internet and online platforms promises much greater reach for all brands if new data rules are kept aligned

As stated in our introductory remarks, INTA believes that a comprehensive, uniform approach to privacy within the United States is desirable. The recent enactment of the California Consumer Privacy Act of 2018 (“CCPA”) and the pending privacy legislation in some 26 other states risks

² <https://www.commerce.senate.gov/public/index.cfm/hearings?ID=2FF829A8-2172-44B8-BAF8-5E2062418F31>

putting the U.S. in the position of Europe before EU General Data Protection Regulation (GDPR). Instead of making the rules more predictable and easier for the consumer and businesses to follow, this fragmented approach will do the exact opposite. Further, a perhaps unintended consequence of the failure to develop a harmonizing Privacy Framework for data privacy regulation will be to restrict the free flow of data in U.S. commerce, as data which might be freely usable in one state is restricted from use in another. Issues of restricted data flow are already arising across international borders as U.S. companies continue to evolve as they undertake to comply with the EU GDPR.

With the CCPA set to go into effect in 2020, and laws pending in several other states will have various effective and enforcement dates, now is the time for a voluntary Privacy Framework. The focus must be on the need to cultivate consumer trust in organizations with whom they do business, but also on the need to ensure minimal friction in foreign trade, giving due consideration to data regulations already in place or currently being implemented around the world.

However, INTA believes that while a voluntary Privacy Framework is essential, a one-size-fits-all is not appropriate, either from an organization or data type perspective. We note that Federal and state regulations already exist for personal health information and for financial information. Consideration must be given as to how those existing regulatory schemes will integrate with any newly adopted Privacy Framework, and it should not be necessary to completely over-haul the existing protection protocols in these industries.

Similarly, consideration must be given to how any adopted regulations emanating from a Privacy Framework would be implemented and enforced among organizations of varying sizes and resources. As intellectual property practitioners, we are privileged to advise business of all sizes, from Fortune 100 companies to start-ups and entrepreneurs. The demands on these businesses, and the resources available to them, vary dramatically. While it may be economically viable for a large, multi-national firm to implement strict security protocols for safeguarding its data, compliance with those same protocols could cripple a start-up or a local “mom and pop” business. The latter may find the incentives to comply with a rigorous framework to be outweighed entirely by its ability to be in business at all. Proportionality needs to be achieved in this respect.

If small businesses and entrepreneurs, who are a critical component to the American workforce, are unable to devote the necessary resources to comply with the regulatory framework, these businesses may simply disappear entirely, or not even form in the first place, and as a result

innovation will suffer. Therefore, INTA believes any regulatory framework must consider the size of the business being regulated, the kinds of data that business is seeking to collect from a user and for what purpose, and the reasonableness of the security requirements imposed in that context.

3. Accountability and Enforcement

Once the data protection regulations and security protocols are adopted based on the Privacy Framework, penalties for violations must not only be available but also enforced. Data owners and processors must be properly incentivized to comply with the regulations, and a comprehensive, but manageable scheme for enforcing the regulations is necessary to achieve that incentivization. INTA looks forward to further engagement on how a scalable and consistent enforcement regime can be achieved.

Based on the experience of INTA members following horizontal data protection measures elsewhere, there are a few areas directly related to the registration and enforcement of IP rights that need to be kept in mind as the Privacy Framework is developed.

Attribution. The rule of law relies on the ability to identify and hold to account before the courts those that harm others. The very trust consumers place in brands requires brands to be policed to prevent frauds, fakes and misleading diversions based on the misuse of the brand. In this respect, justice delayed is often justice denied if effective means to rapidly identify infringers is omitted.

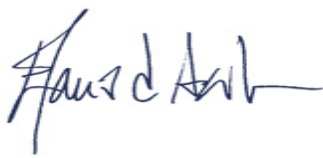
Registers of ownership of tangible and intangible property should remain public. Accountability comes from transparency, especially for individuals and entities who offer foods or services in commerce or are otherwise engaged in commercial activities. This is particularly true in the domain name system where the masking of registrant information data hinders law enforcement, cybersecurity research, consumer protection and Intellectual Property enforcement efforts.

Legal discovery processes. Rules regarding access to personal data need to be viewed alongside general rules of legal discovery, to ensure that checks and balances in one system are not undone by rules developed in another context.

Multi-stakeholderism. Since Tunis and WSIS, Internet governance has generally been left to processes that are not built on statutes, but often community standards or contracts. These need to be carefully accounted for in developing national legislation.

INTA thanks NTIA for its consideration of this submission. For more information about INTA and its policies, you may contact Lori Schulman, Senior Director for Internet Policy, lschulman@inta.org.

Sincerely,

A handwritten signature in blue ink, appearing to read "Etienne Sanz De Acedo". The signature is fluid and cursive, with a long horizontal stroke at the end.

Etienne Sanz De Acedo
Chief Executive Officer

About INTA

Founded in 1848, INTA is a global not-for-profit association with more than 7,200 member organizations from over 191 countries. One of INTA's goals is the promotion and protection of trademarks as a primary means for consumers to make informed choices regarding the products and services they purchase. During the last two decades, INTA has also been the leading voice of trademark owners within the Internet community, serving as a founding member of the Intellectual Property Constituency of the Internet Corporation for Assigned Names and Numbers (ICANN). INTA's Internet Committee is a group of over 150 trademark owners and professionals from around the world charged with evaluating treaties, laws, regulations and procedures relating to domain name assignment, use of trademarks on the Internet, and unfair competition on the Internet, whose mission is to advance the balanced protection of trademarks on the Internet.