dun & bradstreet

Dun & Bradstreet

RESPONSE TO:

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE

REQUEST FOR COMMENT:

DEVELOPING THE ADMINISTRATION'S APPROACH TO CONSUMER PRIVACY

OCTOBER 29, 2018

DOCKET NUMBER:

180821780-8780-01

PREPARED BY:

Allison Schwartz
Global Government Relations Leader
Dun & Bradstreet
11710 Plaza America Drive, Suite 900
Reston, VA 20190
703.807.5065
schwartza@dnb.com

Dun & Bradstreet is pleased to respond to the National Telecommunications and Information Administration (NTIA), request for information on Developing the Administration's Approach to Consumer Privacy.

Dun & Bradstreet commends NTIA for their balanced approach to consumer privacy and appreciates the opportunity to provide opinions on how to create a principles-based policy which balances the needs for privacy with needed protections to help encourage prosperity and innovation. We additionally appreciate the Administration's approach to ensuring the policy is viewed in the lens of operationalizing as increased foreign governments, domestic states and localities are all addressing privacy concerns in sometimes incongruent ways, and multi-national corporations' compliance structures can be confusing in their attempts to comply with the various jurisdictions.

ABOUT DUN & BRADSTREET

For over 178 years, Dun & Bradstreet has been dedicated to growing valuable business relationships through the collection, curation, and analysis of business data. For 90 years, Dun & Bradstreet has partnered with federal, state, local and provincial organizations to co-develop innovative solutions that fulfill mission objectives. Moreover, nearly 90% of Fortune 500 companies, and small and medium enterprises, Dun & Bradstreet partners with customers in every facet of business and government – providing timely and critical information, insight and analysis to drive business and economic growth in all sectors of the economy, improve operations, identify supply chain risk, support national security, and reduce fraud, waste, and abuse.

With more than 300 million global company records, we have the largest commercial database in the world, and we collect data from more than 30,000 global sources. Dun & Bradstreet prides itself as an industry leader in data quality and governance, and we believe that our commitment to fundamental Privacy Principles and effective compliance greatly improves the value of our data. To this end, we submit our response in the hopes of aiding the NTIA achieve federal outcomes that create privacy protections for the individual and enable American businesses to continue succeeding in an increasingly data-driven and global economy.

PROTECTING BUSINESS INFORMATION COLLECTION

The request focuses on federal outcomes and goals related to consumer-privacy protections in the private space[1]. Consumer-privacy protections should be thoughtfully defined[2] to apply, as it does today in the United States, to protecting information about individuals when they are acting in their personal, family or household capacity but not in their business capacity[3].

An individual's reasonable expectations of privacy rights in their personal capacity is different from those expectations in their business role. Businesses and individuals are afforded similar but not exactly the same rights to liberty, privacy, and property. Both are recognized in the Constitution and jurisprudence. However, business data, and data on individuals in their business capacity, should be seen in a different light than individual information that, for example, someone posts on their own social media site.

Individuals should have a choice to protect their privacy on personal activities, but business data should be viewed with a different lens. The public has a right to know about, and should have trust in business risk assessments, so they can make informed decisions on whether a business is carrying out its activity in a risky

[1] See RFC, Part II. B; andC.3.
[2] See id, Part II.D.1.
[3] See e.g. U.C.C. § 9-102(22)-(26).

manner. To deter fraud, bad actors, and poor business information, we should encourage transparent access to business data and information. Moreover, we should recognize that an individual's information in their business capacity is distinctly different from other consumer information which should have privacy protections options provided. The public and businesses have a legitimate interest in this information, and any policy framework created. As small and micro businesses continue to grow in the United States, and across the globe, we encourage regulators to recognize and explicitly ensure a distinction between consumer information on the one hand, and information collected about an individual in their business capacity on the other. Information about an individual's shopping preferences should not be seen in the same light as a person's history of committing business fraud or acting as a front for illegal activity and any framework should be explicit to not allow business information crucial for the public's legitimate business interest in making informed decisions to be confused with privacy protections designed to protect individual consumers or children.

In some legislative initiatives the distinction is not explicit. For example, California's Consumer Privacy Act defines "consumer" so broadly that it could include individuals even in their business activities. Any unconditional right to opt out or delete information for individuals' information about their business activity would provide nefarious individuals and businesses tools to abuse these mechanisms to delete or otherwise hide their fraudulent pasts, defraud unsuspecting victims, and preclude third party due diligence which are required by many jurisdictions and various international laws. Strong privacy protections are important to protect consumers and individual, but we must carefully craft them to protect citizens, and not allow disreputable individuals and companies to use the new laws as a pretense to hide their dangerous business behavior from legitimate business interests.

Today's economy is increasingly global. Businesses can go to their community bank or a non-traditional lender to get a small business loan. Businesses could be brick and mortar stores or an online presence only. Customers could be within their local community or across the world. The infrastructure of businesses has changed and will continue to evolve. Technological innovations now permit a small American business to hire a graphic designer for their website on the other side of the world or find a customer to ship their goods to another state or country. More and more businesses are navigating the global business environment with people they have never met in person, or only via a video chat. In this respect, having the right information and tools to verify the legitimacy of organizations and persons that we interact with in a business capacity must be protected to prevent increased victimization.

As such, Dun & Bradstreet strongly recommends that NTIA clearly delineate the difference between personal information and data which is collected when an individual who is acting in their business capacity. Information on credit fraud and publicly available data including suits, liens and judgments, for examples, should not be included in any opt-out provision contemplated by the Administration, as these are crucial data points in third party compliance due diligence reviews, and they are absolutely necessary to ensure an accurate risk assessment can be conducted to protect individuals and businesses with needed protections against nefarious actors.

PROTECTIONS OF PUBLICLY AVAILABLE DATA

Although public record information and information available to the general public have traditionally been excluded from data protection and privacy bills, they are too narrowly excluded under the California privacy law. Public information such as court proceedings, real estate transaction, death certificates, and other similar sources should be available to all, including insurance companies, credit bureaus and others, to accomplish various important public purposes necessary for legitimate business interests such as third-party due diligence programs,

and engage in activity protected by the First Amendment.

Much of this information is necessary for third-party due diligence programs and limiting its availability and usage would do more harm. Any Federal framework or legislative initiative must ensure that all legitimate publicly available information is exempted from opt out or deletion standards.

ABILITY TO CORRECT SHOULD BE BALANCED WITH NEED FOR ACCURACY

Some information collected may include inaccuracies and individuals and businesses alike should have a path to have their information corrected. However, some disreputable actors and criminal enterprises may ask for information to be "corrected" but when reviewed is proven to be accurate. For example, a business or individual seeking a loan, may wish to have a default payment removed from the credit score that was in fact accurate. Removal of an accurate default could cause a community bank to make a risky loan because they were not able to make a financial risk assessment with all available facts.

Any Federal effort should incorporate a process for individuals and businesses to offer their responses to inaccurate and faulty data which has been collected. We urge insertion of language to clarify this point by adding in the words "should not interfere with the public's right to know legitimate information including information necessary to prevent fraud and illegal activity" under any language relating to access and correction frameworks and legislation.

There is also a responsibility on companies to ensure accuracy of their data. Therefore Dun & Bradstreet believes that the right to delete or correct should not be an unqualified and overriding factor, but instead should trigger an internal process by companies to validate their data for accuracy and corrections should be made when the information cannot be validated or if the inaccuracy is proven to be true.

HARMONIZING REGULATORY LANDSCAPE

Dun & Bradstreet complies with the laws and regulations in which we operate, but the ever-growing divergence of privacy laws creates a confusing patchwork where compliance with one law may be seen as non-compliance in another jurisdiction. For example, the European data protection law's (GDPR) "right to be forgotten" is not unlimited. European regulators understood that they did not wish to give criminals additional ammunition to defraud someone else and therefore considered the collection of this type of data within the scope of "legitimate interest "where the right to be forgotten cannot be invoked so long as the data is correct because it is "necessary [and] relevant." The California law, however, does not include the same consideration of collection of this type of data. Moreover, localities are also moving their own consumer privacy bills at different levels of compliance burdens. Without the ability to track individuals in the business capacity, whether they be officers, directors or shareholders/principals, a company will not be able to determine with certainty whether it is doing business with a legitimate business person or a criminal or fraudster.

Dun & Bradstreet recommends that the any federal framework or legislation exclude from the definition of personal information about individuals in the context of business. Moreover, any right to delete or opt out should be subject to an exclusion for data relevant to any determination related to potential business fraud or illegal activity. Moreover, we urge a federal privacy framework and law, which includes state pre-emption clauses. Without a federal framework, businesses will have a difficulty with compliance of a patchwork of state and local privacy requirements.

We also urge the Administration to continue including protections of cross border data of personal information, at

least as it related to persons acting in their business capacity, within trade negotiations to ensure continued growth of global markets and to permit American companies to be assured that they there are trading with legitimate foreign businesses. Failure to do so could have significant blockages of cross border data flow in the business space which would negatively harm global business growth, preventing U.S. businesses from finding a trusted partner to export their goods and services to another jurisdiction (whether they be across state lines or across a country border). Dun & Bradstreet recommends that any Federal privacy policy ensures that sharing business information be permissible and allows for protection of cross-border data flows in the case of individuals in the context of their business dealings. Such protections should be included in all trade negotiations and protected in federal data policies.

DEFINITIONAL CLARITY

Dun & Bradstreet strongly urges that some key terms are defined by the Administration's framework to help ensure definitional clarity for compliance. In addition to the definition of "consumer" discussed above, clarity of a definition of Personal Information would be recommended. Dun & Bradstreet suggested that Personal Information should be defined as "information about an identified or identifiable living individual. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records and information voluntarily made public by an individual." Clarifying not only what is included, but also what isn't included would help companies better understand their compliance burdens and also provide needed differentiations around data segments.

REGULATORY AUTHORITY

Federal privacy laws and regulations should be harmonized under one federal regulatory body to protect against compliance confusion. Dun & Bradstreet supports the Federal Trade Commission (FTC) serving in the role as the chief regulator on federal privacy laws. The FTC has a long history as the chief federal agency on privacy policy and enforcement. Since the 1970's they have continued to review the privacy policies and enforcement and modernize them to ensure new technological innovations are continuously review as to how they impact consumer privacy protections.

CONCLUSION

Dun & Bradstreet's long history in supporting global business growth and for providing analysis to allow for trusted relationships to be created between entities who may only interact via an innovative technology. While consumer privacy is critically important, and we applaud the federal government for taking on this important issue, frameworks and legislation should explicitly distinguish from individual consumer protection and where individuals are acting in a business capacity. Commercial data privacy-related issues should be balanced against the public and legitimate business interest to know information with whom they do business. Lastly, protections for publicly available data should be included to ensure accurate and public data are able to be presented in the appropriate capacities.

We welcome the opportunity to work with the Administration to ensure any and all privacy laws, rules, and regulations have a balanced approach to strong privacy protections which also support innovation and increased economic growth in the global economy.