November 9, 2018

David J. Redl
Assistant Secretary for Communications & Information
National Telecommunications & Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Washington, D.C. 20230

Re: Response of The National Association of Professional Background Screeners ("NAPBS") to Request For Information Regarding Developing the Administration's Approach to Consumer Privacy – Docket No. 180821780–8780–01

Dear Mr. Redl:

Thank you for the opportunity to provide information regarding the development of the Administration's approach to consumer privacy. As the representative of a highly-regulated industry, the National Association of Professional Background Screeners ("NAPBS") encourages the Administration to work with stakeholders to develop a universal disclosure and consent process to reduce unnecessary paperwork and confusion among consumers related to the background screening process.

Additionally, NAPBS recommends the Administration focus on preempting contradictory or competing data privacy laws, in general, and breach notification requirements, specifically. This approach would establish a clear regulatory baseline that protects consumer data while protecting private-sector prosperity and innovation.

About NAPBS

The National Association of Professional Background Screeners ("NAPBS") is an international trade association of over 900 member companies. Its members provide employment and tenant background screening and related services to virtually every industry around the globe. The reports prepared by NAPBS's background screening members are used by employers and property managers every day to ensure that workplaces and residential communities are safe for all who work, reside or visit there.

NAPBS members range from large background screening companies to individually-owned businesses, each of which must comply with applicable law, including when they obtain, handle, or use public record and private data. NAPBS members also include suppliers of background screening information such as court-record retrieval services and companies that provide access to public record data to background screeners.

110 Horizon Drive, Suite 210 • Raleigh, NC 27615
Phone: 919.459.2082 • Fax: 919.459.2075 • Email: info@napbs.com

The majority of NAPBS's members are consumer reporting agencies ("CRAs") who provide consumer reports (also known as background checks) for employment or tenant screening purposes to employers and property managers.

Regulation of Background Screening and Recommendation for Universal Consent in the Context of Background Screening

NAPBS members work within a well-defined, highly regulated arena with respect to user data privacy. Most importantly, pursuant to the Fair Credit Reporting Act (FCRA) and various state laws, all consumer reporting agencies (whether NAPBS members or not) must obtain a consumer's consent before preparing a consumer report. In most cases, consumers provide their personal information directly to the agency for preparation of the report.

NAPBS members use the provided information to obtain public record and other database information and gather additional information, all of which is evaluated and compiled into a consumer report within the limited scope as defined by their client. Consumers are entitled to a copy of the report upon request, and are provided the opportunity to dispute the completeness or accuracy of the report.

During this entire process, NAPBS members adhere to statutory and industry standards regulating the use and storage of personal information such as the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act. It is from this unique, experienced perspective that NAPBS respectfully submits its comments on developing the Administration's approach to user data privacy.

Within the context of employment screening, NAPBS members receive certifications from their clients, potential employers, that the employers have both disclosed and received authorization from potential employees to access both public record information and private information for legitimate public safety reasons. A potential employee will authorize a prospective employer to contract with a background screening company to prepare a consumer report by accessing both public record information, such as criminal history, and private information, such as credit reports. The information is then compiled into a consumer report and shared with the prospective employer as authorized by the consumer.

As noted in the Request for Comment, the "desired outcome," in this type of situation and countless others, is "a reasonably informed consumer," aware of who is accessing and sharing their information, how it is protected, and for what purpose. Such situations present a unique challenge, especially given the vertical sharing of information – consumer to prospective employer to background screening company – and horizontal access, specifically the laws and regulations governing data in various jurisdictions and across different databases.

The result, as noted in the Request for Comment, is "long, legal, regulator-focused privacy policies and check boxes" that confuse the consumer and place expensive burdens on companies. This inherent nature of data access and sharing, among multiple parties and across various jurisdictions, elicits a front-end, single consent solution for the collection, use, storage, and sharing of personal information over an appropriate and contextual life-cycle.

In the context of background screening, this "outcome-based approach" would provide consumers with a universal consent form informing them of the who, what, and how when authorizing access to their personal information without requiring burdensome consent at every data-exchange point. A consolidated, unitary approach to consent with respect to data privacy serves consumers and companies as well.

First, consumers subjected to multiple consent forms, and exhaustive terms of conditions, may actually result in a less-informed authorizer than one with a front-end overview of the access, sharing, and storage of their data. NAPBS envisions a brief, universal consent form at the outset of the background screening process.

This consent form would provide a high-level overview of which companies are accessing certain data, why such access is necessary, and how they share and protect the data across the entire vertical and horizontal data spectrums. Moreover, the consent form would still comply with existing statutory and regulatory notification requirements by including necessary information such as terms and conditions, providing detailed, actionable information for consumers who wish to learn the details of data use and privacy.

Second, a universal consent form would reduce the regulatory burden on companies which are already held to statutory and industry standards. Without having to worry about technical violations of consent at every stage in the data life-cycle process, companies could reorient their focus and resources to the continued protection of consumer data.

Recommendation for a Harmonized Approach:

The issue of data-use consent across various jurisdictions lies within the broader context of which governmental entities should regulate data privacy, a field that inherently does not lend itself to jurisdiction-by-jurisdiction laws. Given the nature of personal data collection, use, storage, and sharing, NAPBS believes that it should be the province of the federal government and its agencies, not states or counties, to "harmonize the regulatory landscape."

Take, for example, data breach notification requirements. A state-by-state regulatory environment concerning data breaches unduly burdens consumers and companies. With separate definitions and requirements from each state, a consumer could conceivably receive multiple data breach notifications for the same data, resulting in potentially conflicting and confusing of information.

Moreover, companies required to abide by state requirements necessarily devote resources to compliance rather than investing those resources in further data protection above and beyond what is legally required.

With any regulatory regime comes necessary enforcement mechanisms. NAPBS recognizes the purpose and need for consequences for companies and individuals who disregard a consumer's right to data privacy. However, NAPBS recommends the Administration adopt a high-level goal of adopting a harm-based, injunctive enforcement regime rather than the current approach of private rights of action over technical violations of privacy laws.

napbs
National Association of Professional Background Screeners
The Voice of Screening Professionals

The current enforcement regime provides perverse incentives for private individuals to sue companies over technical violations of privacy laws. This regime stifles innovation and flexibility, and distracts business resources from the ultimate purpose of privacy laws – the prevention of actual harm to users as a result of data breaches or misuses. A minefield of potential technical violations, especially jurisdiction by jurisdiction, coupled with a perversely-incentivized private cause of action for punitive damages, slows, or even blocks, the road to innovative use and safe storage of private personal data.

In this environment, private prophylactics impose unnecessary cost on businesses, which could otherwise be invested in pursuing the ultimate purpose of such privacy laws – the protection and appropriate use of personal data. A shift to focusing on injunctive remedies for actual harm, as opposed to statutorily-created legal harm, would provide meaningful data privacy protection without driving up the cost of business unnecessarily.

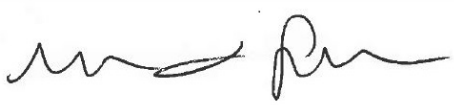
For example, data privacy under the FCRA would be served by enforcement through equitable relief, rather than private punitive remedies. Such a shift in the Administration's enforcement focus would promote innovation and flexibility within personal data industries, while providing for appropriate remedies to consumers actually harmed in certain situations.

Conclusion:

NAPBS thanks NTIA for the opportunity to share its comments, and sincerely hopes its comments are beneficial to the development of the Administration's approach to consumer data privacy. NAPBS and its members are available and prepared to discuss any questions regarding our industry or the aforementioned concerns.

Thank you for accepting our comments and we look forward to working with you further.

Sincerely,



Melissa Sorenson, Esq.
Executive Director

110 Horizon Drive, Suite 210 • Raleigh, NC 27615
Phone: 919.459.2082 • Fax: 919.459.2075 • Email: info@napbs.com