U.S. based callers: 1-888-376-1079
Callers from outside U.S.: +1-617-398-7067
www.verasafe.com

VeraSafe's Response to Request for Comments Regarding Developing the National Telecommunications and Information Administration's Approach to Consumer Privacy

[Docket No. 180821780–8780–01]
RIN 0660–XC043
November 9, 2018

VeraSafe appreciates the opportunity to respond to the Request for Comments Regarding Developing the National Telecommunications and Information Administration's Approach to Consumer Privacy. VeraSafe's privacy, data protection, and cybersecurity team is comprised of attorneys as well as privacy and cybersecurity experts dedicated to advising clients across various geographies and industry sectors. VeraSafe can be contacted as follows:

Web: https://www.verasafe.com

Phone: +1 (617) 398-7067

Mail: VeraSafe, 22 Essex Way, Essex Vermont 05452, USA

II.A.1. Are there other outcomes that should be included, or outcomes that should be expanded upon as separate items?

Limits on Changes to the Purposes of Processing of Personal Data

As an extension of the principle of *Transparency* identified in the RFC, VeraSafe proposes that organizations should be limited to processing personal data only for the purposes that are disclosed to individuals when their data is collected, and for other purposes only insofar as those purposes have an

USA: VeraSafe | P.O. Box 8203 | Essex, VT 05451 | USA

EU: VeraSafe | Zahradníčkova 1220/20A | Prague 15000 | Czech Republic

obvious connection to the ones originally disclosed. In VeraSafe's opinion, the norm in the U.S. private sector is for personal data to be processed for nearly any purpose an organization chooses—at its sole discretion—and that those purposes are prone to change at any time after collection. While likely incorrect, the common presumption is that an organization merely needs to update its privacy policy before using personal data for new purposes. Even taking into account federal unfair and deceptive acts and practices legislation, a clear obligation to affirmatively notify the individual and seek his consent for new purposes for which the previously collected personal data will be used, would be an improvement. VeraSafe believes that to ensure the right of self-determination regarding the processing of one's personal data, such personal data should not be used for new, unrelated purposes without genuine transparency and choice for the individual.

Notice and Choice for Transfers of Personal Data to Third Parties Other Than Those Acting as Vendors and Service Providers for the Controller

In the course of business, organizations commonly sell, share, and otherwise transfer personal data to a third party for uses that are determined by that third party. In this case, the receiving party is not acting in the capacity of a vendor or service provider for the disclosing party. However, where an organization receives personal data from another organization, the *Transparency* principle should require that individuals are informed of (1) such recipients of their personal data, (2) the purposes for which the personal data will be used by the recipient, and (3) the means by which individuals may exercise choice with respect to such use of their personal data.

II.B.3. Are there any risks that accompany the list of goals, or the general approach taken by the Department?

Allocation of Responsibilities and Rights is Essential

The outcome-based approach taken by the Department sets high-level goals drawn from important privacy principles and which seek to address common privacy risks. This focus on the outcomes is laudable, as it emphasizes the impact on the individual consumer. VeraSafe believes that in order for this approach to be most effective, the Department should consider going even further by allocating responsibilities and rights among the relevant parties more explicitly.

For example, the description of the outcome "*Control*" states:

> Users should be able to exercise reasonable control over the collection, use, storage, and disclosure of the personal information they provide to organizations. However, which controls to offer, when to offer them, and how they are offered should depend on context, taking into consideration factors such as a user's expectations and the sensitivity of the information.

This description raises several questions. Who determines whether a user has been allowed to exercise reasonable control? Will the organization have discretion to determine what overall level of control, what types of control to offer, and how to offer them—or will there be an established baseline? It isn't difficult to imagine problems that might arise if organizations are granted too much discretion.

USA: VeraSafe | P.O. Box 8203 | Essex, VT 05451 | USA

EU: VeraSafe | Zahradníčkova 1220/20A | Prague 15000 | Czech Republic

Additionally, VeraSafe believes that the following related questions (among others) should be answered in order to achieve the minimal level of specificity required to make the outcome-based approach successful:

- Which party is ultimately responsible for each of the outcomes?
- How will the outcomes be enforced?
- Are individuals being granted new actionable rights?

More clearly defining the roles of privacy stakeholders—including individuals and the organizations processing their personal data—will result in a stronger foundation on which to build a congruous and equitable privacy solution at the federal level.

Harmonization of the Regulatory Landscape

Harmonization of the privacy regulatory landscape is overdue and VeraSafe commends the Department for pursuing this as a high-level goal. However, if federal preemption of state privacy laws is intended, this may result in some consumers having less privacy protection than they currently enjoy. This would be counterproductive. To that end, we echo and amplify the point made by the Department that the regulatory landscape should remain "strong" in addition to "flexible," "predictable," and "harmonized." This point counsels in favor of adopting a federal floor for privacy standards, rather than a ceiling. Establishing such a minimum privacy standard would allow states to exceed the standards set by the Department, at least in certain designated areas.

Interoperability as an Opportunity

As noted under the heading "*High-Level Goals for Federal Action*," interoperability with international privacy norms, frameworks, and laws is a necessary goal for any future federal action related to privacy.

Privacy is an increasingly important issue to governments around the world—a fact most recently demonstrated by the EU's adoption of the General Data Protection Regulation (otherwise known as the "GDPR"), which is viewed as the international benchmark regulation for privacy and data protection. Therefore, the creation of a federal privacy solution in the near term presents a unique opportunity for interoperability with European privacy law. The benefits of such a solution cannot be overstated, given the importance of the European marketplace to U.S. organizations.

If any future federal privacy law in the U.S. were to be harmonized with the tenets of the GDPR, the U.S. would be well-positioned to seek an "adequacy decision" from the European Commission. Receiving an adequacy decision would enable cross-border data flows between the EU and the U.S. without the need for additional safeguards like the EU-U.S. Privacy Shield Framework or the Standard Contractual Clauses. This would be an immensely valuable outcome for U.S. organizations.

Furthermore, because many U.S. organizations are already subject to the GDPR due to the regulation's

USA: VeraSafe | P.O. Box 8203 | Essex, VT 05451 | USA

EU: VeraSafe | Zahradníčkova 1220/20A | Prague 15000 | Czech Republic

extraterritorial scope, harmonization of U.S. federal privacy law with European law would likely pay dividends down the road, in terms of helping to avoid or mitigate European enforcement actions against U.S. organizations that are unaware of the GDPR's applicability to their operations.

II.C.2. Should the Department convene people and organizations to further explore additional commercial data privacy-related issues? If so, what is the recommended focus and desired outcomes?

As a leader in privacy compliance and risk management advisory services tailored to small and medium-sized organizations, VeraSafe would welcome the opportunity to, in conjunction with the Department, further explore data privacy-related issues that impact these organizations. In particular, VeraSafe believes the following questions should be answered:

- How can federal privacy regulation be constructed so that business stakeholders easily understand their obligations under the law?

- How can the Department and the FTC foster the development of a standardized approach for organizations to contract with their service providers (who process personal data on their behalf), in a way that creates genuine accountability but also simplifies and streamlines the contracting process?

- How can federal privacy regulation provide structure for organizations to identify, rank, and manage privacy risks, without introducing burdensome complexity into the regulation?

II.D. The Department understands that some of the most important work in establishing privacy protections lies within the definitions of key terms, and seeks comments on the definitions. In particular:

1. Do any terms used in this document require more precise definitions?

VeraSafe believes the following terms and phrases require more precise definitions:

- "*Collecting, storing, using, and sharing personal information*"; and

- "*Vendors and servicers*".

2. Are there suggestions on how to better define these terms?

- The notion of "*collecting, storing, using, and sharing personal information*" is not sufficiently broad to encapsulate all of the activities performed on personal data that may create risk to the privacy of the individuals involved. Using the term "processing" is preferable, and should be construed to include any activity performed on personal data.

- The concept of "vendors and servicers" could be simplified but also broadened.

USA: VeraSafe | P.O. Box 8203 | Essex, VT 05451 | USA

EU: VeraSafe | Zahradníčkova 1220/20A | Prague 15000 | Czech Republic

Conclusion

VeraSafe values the opportunity to provide these comments to the Department. Furthermore, VeraSafe appreciates the Department's outreach on this important issue and would welcome the opportunity to work with the Department as it explores how to provide a harmonized, clear, comprehensive, risk-based, and interoperable approach to federal privacy regulation.

Sincerely yours,

Matthew Joseph, CIPP/E, CIPP/US
Head of Privacy, Data Protection, and Cybersecurity Practice

USA: VeraSafe | P.O. Box 8203 | Essex, VT 05451 | USA

EU: VeraSafe | Zahradníčkova 1220/20A | Prague 15000 | Czech Republic