

John Paul Tomaszewski
700 Milam Street, Suite 1400
Houston, Texas
(713) 860-0088
Skizyx1969@gmail.com

**RE: Department of Commerce, National Telecommunications and
Information Administration Docket No. 180821780-8780-01**

The National Telecommunications and Information Administration published its Request for Comments (RFC) “Developing the Administration’s Approach to Consumer Privacy” with a request for feedback by 11:59 pm, November 9, 2018.

This approach is intended to advance consumer privacy while protecting prosperity and innovation and is divided into two parts:

- 1) A set of user-centric privacy outcomes that are underpinned by the protections that should be produced by any Federal consumer-privacy policy actions;
- 2) Identifying the direction the Federal action should take to provide these protections, considering the goals the Administration wants to achieve.

As an attorney who has been practicing international data protection for the better part of the last 20 years, I have seen the evolution of data protection across cultures and legal systems. As part of the US delegation to APEC, I was one of the primary drafters of the Cross Border Privacy Rules (“CBPR”) system. As the General Counsel of TRUSTe (now TrustArc), I helped develop and support self-regulatory privacy systems which operated across borders and cultures. Also, as a Chief Privacy Officer for a financial services company, I have built compliance systems to ensure the privacy of consumers in the financial ecosystem is respected.

The Administration’s stated goals and approach are laudable. However, I would respectfully submit that there are some additional elements which need to be explored for any legislation to achieve the dual goals of enhancing individual privacy and supporting technological and cultural innovation.

I. Desired Outcomes

The current approach understands that legislation should be outcome oriented. However, the stated outcomes in the current approach seem not to be outcomes, but controls which can be used to achieve outcomes. At the highest level, any US federal privacy legislation needs to adhere to the following approach:

- Technology Neutrality
- Risk and context sensitivity
- Outcome-oriented
- Interoperable with other systems

- Reduction in administrative burdens for compliance

This approach supports the ultimate outcomes necessary for any data protection system:

- Enhancing trust in the information ecosystem
- Scalability (both domestically and globally)
- Supporting innovation

Privacy is a state which supports trust in the ecosystem. Privacy isn't an "end state" or a goal, it is a mechanism by which the end state of trust is achieved. As such, policy decisions which are made solely for the purpose of fostering privacy may not actually end up having the result of fostering trust in the ecosystem. They may also damage the scalability and innovation outcomes which need to be valued as well.

II. Regulatory Structure

The US has precedent around how to structure regulatory systems around privacy. The passage of the Gramm-Leach-Bliley Act ("GLB") is a good example of how a consistent set of privacy and security rules can be implemented across multiple different regulatory domains. The existing banking regulators maintained their statutory authority and the Federal Trade Commission ("FTC") was used as the default regulator for those entities not directly regulated by the other banking regulators.

It will be important for any new legislation to take advantage of the learnings the US has developed in the sectoral approach to privacy law. As such, the regulatory structure a new privacy law should maintain should have the following components:

- FTC jurisdiction and rulemaking authority
- Compliance safe harbors
- Interoperability with existing federal law (the existing "rules of the road" for regulated industries should not change)
- Preemption of State law
- Risk-based and outcome-oriented approach to enforcement

With this structure, the actual privacy controls which may be mandated by an omnibus privacy law should avoid negative unintended consequences.

III. Privacy Controls

Privacy-specific controls which support trust have been a part of the US legal landscape for many years. The Fair Information Practice Principles ("FIPPs") created by the US in the 1970's went on to be the foundation of the OECD privacy principles - which is the basic set of principles underpinning every privacy system in the world today. It is important to maintain the use of these principles when legislating privacy controls. As such, the practical approach for drafting such legislation should include each of the FIPPs.

Transparency: Awareness of an entity’s data handling practices is an important component to fair and lawful processing. Fortunately, the Federal Trade Commission (FTC), through its compliance guidance and advice provisions related to other privacy laws in the US, has already promulgated approaches which serve the need to describe how to achieve transparency. The FTC should be able to use guidance to provide a foundation for “how to do transparency”. This concept is taken directly from the FTC’s work under GLB. The goal here is to provide a level of flexibility necessary to achieve the goal of balancing the use of private information with user-centric privacy, all the while enhancing trust in the ecosystem.

Control: Control as a concept within the approach presented should be carefully applied based on context, and based on the desired outcome of trust. In some circumstances, the individual data subject’s exercise of control around data processing may be inappropriate (e.g. disclosure of personal data in a public record related to real estate holdings). In other circumstances, the individual may prefer convenience over control. Under other privacy systems, control is not as important as “fair and lawful” processing. This is the position that the EU General data Protection Regulation (“GDPR”) has taken. Consequently, control (or “consent”) should be viewed as a fairly limited mechanism by which individual privacy rights can be supported. Additionally, an over-reliance on control will also stifle innovation and reduce scalability.

A more useful approach may be to articulate what constitutes “fair and lawful” processing. The precedent for this concept under US law is the Fair Credit Reporting Act (“FCRA”). Under the FCRA, if an “adverse action” is taken against a consumer, the consumer is then given rights to exert “control” around the processing. However, such control isn’t necessary where there is no adverse action taken. Similarly, the exercise of control may only be needed when an “adverse” action is taken against the individual’s interests. Under the GDPR, this is known as the “right to object”.

Reasonable Minimization: Minimization is tied to the concept of “purpose for collection”. Data processing should only use the necessary amount (and type) of data for the purpose articulated under the Transparency control. However, minimization requirements should follow the same concept of avoiding “adverse action. The EU approach to minimization will likely stifle innovation, and doesn’t necessarily foster trust in the information ecosystem. If there is a requirement to minimize the collection of data, it should be reasonable based on not just the original purpose for collection, but also any reasonably related purpose.

Security: Security is the foundation upon which trust in the information ecosystem is based. Reasonable security is already mandatory in many other state and federal privacy laws. However, like was done in the HIPAA Security Rule, security should be risk and context sensitive. Requiring military grade security for grandma’s cookie recipe isn’t necessary and will increase the administrative cost to comply without any corresponding benefit or reduction of risk. Specifics of this approach should be developed by regulation, and not by the law itself.

Access and Correction: Similar to the control concept, Access and Correction rights exist in other US privacy laws. The FCRA has access and correction rights. Similarly to the comments around control, access and correction rights should be present, but they should also be balanced by other, similarly important policy objectives (e.g. reliability of records systems). In this area,

the approach would be well informed by the analogous provisions of the GDPR and other omnibus privacy laws in how they balance competing interests in personal data.

Risk Management (RM): The risk management provision of the approach is central to the success of any legislation. Since one of the outcomes is the enhancement of trust, inserting a control where there is no risk achieves nothing. Further, it damages the other objectives of the legislation related to decreasing administrative burdens, and supporting innovation. As noted earlier, a risk-based approach was taken with HIPAA's Privacy and Security Rules.

Accountability: One of the lessons the EU took from the US in drafting the GDPR was the concept of accountability. Additionally the APEC CBPR systems also uses accountability as a component of their system. However, the aspect of accountability which is important for the US isn't the introduction of the concept, but the development of mechanisms which motivate good behavior - as opposed to just punishing bad behavior. In the US we have seen the use of safe harbors (e.g. under the Children's On-Line Privacy Protection Act), self-regulatory certification marks (e.g. BBB and TrustArc), and similar mechanisms which give organizations to inject reliability into their compliance programs. Any new omnibus federal privacy law should include such tools. It should be noted that the GDPR also includes these concepts in the provisions around certification marks and codes of conduct. The FTC is the appropriate vehicle to approve such mechanisms including, but not limited to, minimum standards with guidelines and parameters an organization must be within, depending on various criteria.

II. High-Level Goals for Federal Action

Harmonizing the Regulatory Landscape: While privacy is a basic right, as interpreted through the U.S. Constitution and myriad state constitutions, there is very real differentiation around how that right is perceived and enforced at both the state and federal level (California has over 60 different laws which contain privacy implications). An omnibus federal privacy law can provide a consistent baseline of regulation throughout the nation, as well as the opportunity to scale and interoperate with other privacy systems, such as the GDPR, Brazil's omnibus privacy law, the UK's Data Protection Act of 2018 (DPA), Canada's PIPEDA (and its Provincial enactments), Mexico's data protection law, and the various data protection laws in Asia (including China, Japan, and Korea). This law must be drafted in a technology neutral manner, allowing it to address advances in technology without requiring amendment. Finally, it must federally preempt inconsistent state and local laws impacting individual privacy, while still retaining the current "rules of the road" for the already regulated industries (e.g. FCRA, HIPAA, GLB).

Legal Clarity While Maintaining the Flexibility to Innovate. FTC rulemaking authority through the omnibus privacy law will support a reasoned and bipartisan (due to the FTC's structure) approach which should improve the chances of achieving all the stated policy objectives. It will also support clarity and order to the law's enforcement while enabling flexibility for novel business models and technologies.

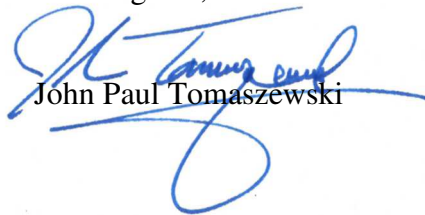
Comprehensive Application. The baseline of the law and its implementing regulation should mandate the controls around data practices be similar to the context in which data is used. Such an approach will necessarily require preemption or repeal of inconsistent laws as well as promulgation of an omnibus privacy law authorizing the FTC to adopt specific rules.

Incentivize Privacy Research. In this aspect the Administration’s approach lacks specificity. More research does need to be conducted related to the privacy expectations of individuals. Additionally, development of products and services that improve privacy protections is also needed. Similarly to the way that money was set aside under HIPAA/HITECH for research and innovation, it would be prudent to explore this aspect as well. Federal encouragement could be made in the form of monetary grants and other compensatory incentives to educational and other institutions. The state of Texas is in the process of developing a tri-part initiative between government, education and the private sector to address information sharing. There is no reason why something analogous to this could not be formed to address overall privacy policy.

FTC Enforcement. The omnibus law must specifically grant the FTC rulemaking authority, as well as the authority and budget to work with other regulators who have privacy as part of their mandate (e.g. FCC, CFPB, OCC, etc.) to ensure consistency across the information ecosystem. (FTC). This rulemaking must be tempered, via statute, to allow flexibility to any organization in how it complies. Additionally safe harbors, or other mechanisms for “deeming compliance” should be included. This will also provide greater flexibility for industry to develop innovative and novel solutions to support compliance.

Thank you for accepting these comments in response to the Administration’s Request for Comments.

Kind regards,



John Paul Tomaszewski