Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 31 • NUMBER 2 • FEBRUARY 2019

# NTIA Receives Comments on a Flexible Risk-Based Approach to Consumer Privacy

**By Stephanie M. Phillipps, Maureen R. Jeffreys, Nancy L. Perkins, and Vernon G. Ross**

Several months ago, the National Telecommunications and Information Administration (NTIA), an agency within the U.S. Department of Commerce, published a Request for Comment (RFC) on how the Administration should "advance consumer privacy while protecting prosperity and innovation."The RFC sought comments on a risk-based approach that is divided into two parts:

(1) "user-centric privacy outcomes that underpin the protections that should be produced" by federal privacy policy, and

(2) "high-level goals that outline the ecosystem that should be created to provide those protections."

**Stephanie M. Phillipps** (*stephanie.phillipps@arnoldporter.com*) is a partner at Arnold & Porter representing clients in administrative proceedings and litigation on telecommunications issues. **Maureen R. Jeffreys** (*maureen.jeffreys@arnoldporter.com*) is a partner at the firm and chair of the firm's Telecommunications, Internet, and Media practice. **Nancy L. Perkins** (*nancy.perkins@arnoldporter.com*) is counsel at the firm focusing her practice on litigation, regulatory compliance, and consulting on data privacy and security matters. **Vernon G. Ross** (*vernon.ross@arnoldporter.com*) is an associate at the firm counseling communications and technology clients on policy, regulatory, and competition issues.

NTIA received over 200 comments, including from the Federal Trade Commission (FTC), technology companies, telecommunications carriers, business groups, equipment manufacturers, cable operators, copyright owners, public interest groups, software providers, trade associations representing various interests, and academic groups.[2]

**The RFC proposed that consumer privacy "refocus on the outcomes of organizational practices, rather than on dictating what those practices should be."**

While the RFC stopped short of specifically calling for federal privacy legislation, one of the high-level goals identified in the RFC was to harmonize consumer privacy regulation, and the RFC asked for comment on whether legislation is needed to achieve federal goals. The RFC noted that it is not proposing any changes to current consumer privacy "sectoral laws," including:

- The Children's Online Privacy and Protection Act;
- Gramm-Leach-Bliley Act;

- The Health Insurance Portability and Accountability Act (HIPPA); and

- The Fair Credit Reporting Act.

This RFC comes at a time when there is a new wave of interest in federal privacy legislation, which has been controversial to date. Recently, representatives of a number of leading technology companies and others testified before Congress in favor of such legislation. Their position reflects recognition that U.S. companies may be better off with uniform standards rather than attempting to juggle the different standards set by various state privacy laws.

## Privacy Outcomes

The RFC proposed that consumer privacy "refocus on the outcomes of organizational practices, rather than on dictating what those practices should be." The collection, use, storage, and sharing of information, as well as user transparency, control and access, should be "reasonable" and "appropriate to the context." The RFC emphasized balancing flexibility with the need for legal clarity and strong consumer protections. Thus, the RFC proposed a risk-management approach that "affords organizations flexibility and innovation in how to achieve" the privacy outcomes listed below.

**The RFC pointed out that lengthy privacy notices in many cases do not lead to adequate user understanding.**

- *Transparency*. Users should be able to easily understand how an organization collects, stores, uses, and shares their personal information. The RFC pointed out that lengthy privacy notices in many cases do not lead to adequate user understanding.

- *Control*. Users should be able to exercise reasonable control over the collection, use, storage, and disclosure of the personal information they provide to organizations.

- *Reasonable minimization*. "Data collection, storage length, use, and sharing should be minimized in a manner and to an extent reasonable and appropriate to the context and risk of privacy harm."

- *Security*. Organizations should employ security safeguards to protect personal information they collect, store, use, or share.

- *Access and correction*. Users should have reasonable access to their personal data and the ability to amend or delete that data, given the context of the data flow and risk of privacy harm.

- *Risk management*. "Users should expect organizations to take steps to manage and/or mitigate the risk of harmful uses or exposure of personal data."

- *Accountability*. "Organizations should be accountable externally and within their own processes for the use of personal information" they or their third-party vendors collect, maintain and use in their systems.

## High-Level Goals for Federal Action

The RFC described the goals below as a nonexhaustive and nonprioritized list of the Administration's priorities.

- *Harmonize the regulatory landscape*. The RFC noted that there is a need to avoid duplicative and contradictory privacy-related obligations placed on organizations.

- *Legal clarity while maintaining the flexibility to innovate*. This goal would ensure organizations have clear rules, while providing flexibility for novel business models and technologies and allowing a variety of methods to achieve privacy outcomes.

- *Comprehensive application*. Any action should apply to all private-sector organizations that collect personal data not otherwise subject to the sectoral laws noted above.

- *Employ a risk- and outcome-based approach* . "Risk-based approaches allow organizations the flexibility to balance business needs, consumer expectations, legal obligations, and potential privacy harms, among other inputs. . . ."

- *Interoperability*. This goal would develop "a regulatory landscape that is consistent with the international norms and frameworks in which the United States participates, such as the APEC Cross-Border Privacy Rules System."[3]

- *Incentivize privacy research*. The government should encourage development of products and services that improve privacy protections.

- *FTC enforcement*. The RFC stated that the FTC is the appropriate federal agency to enforce consumer privacy, with exceptions for certain areas covered by the sectoral laws noted above (e.g., HIPPA).

- *Scalability*. Small businesses that collect little personal information and do not maintain sensitive information should not be primary enforcement targets as long as they are making good-faith privacy protection efforts.

## Request for Comment

Below are some of the key questions the RFC identified for comment.

- *Feedback on the sets of core primary outcomes consumers can expect and high level goals*:
  - Are there other outcomes and goals that should be considered?
  - Are descriptions clear?
  - What are the risks to these outcomes and goals?
- *What steps should the Administration take to effectuate the outcomes and achieve the goals?*
  - Executive action?
  - Recommended statutory changes?
  - Other means?
- *Definitions*
  - Are there any terms that need more precise definition?
  - Any suggestions on how to define terms and what definitions should be?
- *FTC*
  - Any changes needed regarding FTC's resources, processes, or statutory authority?
- *Cross-border Trade Benefits*
  - If other countries replicated the outcomes and goals described in the RFC, would it be easier for US companies to provide goods and services in those countries?
- *U.S. Leadership*
  - Are there other ways to achieve U.S. leadership that are not included in this RFC? Any outcomes or goals in this RFC that are detrimental to U.S. leadership?

## Highlights of Responses Received by NTIA

Commenters generally praised NTIA's efforts to develop a consensus among the many privacy stakeholders. Most industry commenters supported federal privacy legislation that would create a level-playing field for all private sector entities handling personal data. Several public interest groups also supported a legislative approach but suggested the focus should be more on consumer rights rather than the risk based approach proposed by the NTIA.

Commenters differed on whether new federal privacy legislation should preempt state privacy laws. Industry commenters generally supported preemption of state laws, arguing that preemption would create uniformity and certainty in compliance and user expectations. On the other hand, several public interest groups urged that states should be able to adopt and enforce stronger privacy protections.

Commenters generally supported keeping the FTC as the primary federal agency responsible for privacy enforcement. The FTC commented that if given more authority, it would need additional tools and resources to carry out expanded privacy enforcement. Public interest groups urged that the FTC be given additional resources as well as broader rulemaking and civil penalty authority to strengthen FTC enforcement powers. Public interest groups

and others also argued that in addition to the FTC, state attorneys general should have authority to enforce both federal and state privacy laws.

**Many commenters suggested that U.S. privacy laws should be aligned with international standards to allow for flexibility and consistency across borders.**

Finally, many commenters suggested that U.S. privacy laws should be aligned with international standards to allow for flexibility and consistency across borders.

## Notes

1. *https://www.ntia.doc.gov/federal-register-notice/2018/request-comments-developing-administration-s-approach-consumer-privacy*.
2. All comments submitted to the NTIA can be viewed at *https://www.ntia.doc.gov/other-publication/2018/comments-developing-administration-s-approach-consumer-privacy*.
3. APEC (Asia-Pacific Economic Cooperation) Cross Border Privacy Rules System, *available at http://cbprs.org/default.aspx*, requires participating businesses to implement data privacy policies consistent with the APEC Privacy Framework developed by APEC members to facilitate and protect cross border flows of personal information among APEC economies. Members of APEC include the United States, China, Russia, Mexico, Canada, Australia, South Korea, Japan, and many countries in Southeast Asia.