entertainment® software association

Via Electronic Mail November 9, 2018

National Telecommunications and Information Administration (NTIA)
U.S. Department of Commerce
ATTN: Privacy RFC
1401 Constitution Avenue NW
Room 4725
Washington, DC 20230
privacyrfc2018@ntia.doc.gov

Re: Request for Public Comments: Developing the Administration's Approach to Consumer Privacy

To Whom It May Concern:

The Entertainment Software Association (ESA) welcomes the opportunity to provide comments in response to the National Telecommunications and Information Administration's (NTIA's) proposed framework for developing the Administration's approach to consumer privacy. ESA is the U.S. trade association for more than 30 companies that publish interactive entertainment software for video game consoles, handheld devices, personal computers, and the internet.[1] Our members not only create some of the world's most engaging online experiences for consumers, but also are at the cutting edge of developing innovative new technologies, such as virtual reality (VR), augmented reality (AR), and mixed reality (MR) headsets and the latest console and handheld video gaming devices.

Given the wide range of devices and platforms through which consumers experience our members' products and services, ESA agrees with the NTIA's focus on flexible outcomes and risks, rather than prescriptive mandates, to ensure that the privacy of consumers' personal information is protected. Below we comment on some of the key privacy outcomes, goals for federal action, and key terms contained in NTIA's proposed framework.

Privacy Outcomes

ESA agrees that the Administration's approach to privacy should be based on privacy outcomes, while giving organizations the flexibility to determine how best to operationalize those outcomes based on their unique products, resources, and risks. Such an approach enables organizations to provide privacy controls that evolve with changes in technology and business models, and that are consistent with consumers' reasonable expectations across a wide range of contexts.

As an organization that represents members publishing games and offering video game services across a wide range of devices and platforms, ESA is uniquely qualified to provide

[1] *See* Entertainment Software Association, Membership, http://www.theesa.com/about-esa/members/.

concrete examples of why an outcome-based approach is needed to protect consumers while encouraging innovation:

- Outcome: Transparency. ESA supports the notion that "[u]sers should be able to easily understand how an organization collects, stores, and shares their personal information," and is encouraged by NTIA's acknowledgment that "transparency can be enabled through various means."

  ESA's members are continuously striving for new ways to effectively inform users without detracting from the quality of the interactive entertainment software. In our experience, the means for the disclosure may vary depending on how the consumer interacts with the product. For example, notices and privacy settings within a game can sometimes be more effective than scrolling through a lengthy privacy policy on a television screen the first time a video game is played. And while check boxes or buttons might work well in some contexts, swiping right or raising a hand might work just as well (or better) in others. Consequently, transparency outcomes should not require specific formats or procedures that are built for today's websites and mobile apps and should instead be flexible enough to permit (and encourage) more creative approaches that may be more understandable and accessible for consumers using future generations of video game consoles, VR/AR/MR headsets, televisions, and other devices.

  In addition, the level of transparency should vary depending on the sensitivity and risk of the type of personal data collected. For example, consumers do not expect the same level of detail in a privacy notice describing how a player ID and game play data is collected and used for video game services as in a privacy notice describing how financial account information is used for marketing.

- Outcome: Control. ESA also agrees with NTIA that the degree to which users can exercise control over the collection, storage, and disclosure of personal information "should depend on context." For example, notwithstanding a consumer's desire to delete her account after being suspended for cheating in a video game, the publisher might need to retain some account information to help prevent the person from re-registering in violation of the game terms of service and to improve the publisher's anti-cheat measures.

  In addition, any federal privacy framework should encourage a wide range of business models. For example, in order to offer consumers more choices for accessing game content, many publishers in the video game industry are offering some games on a "free-to-play" basis, relying on advertising that may be targeted to cover the costs of developing and operating such games. Prohibiting publishers from offering different pricing options or service levels to individuals who opt-out of having their personal data used for advertising would cripple this ad-supported business model. Instead, as long as the publisher notifies the consumer upfront that the game includes targeted advertising so that the consumer can make an informed choice about whether to play the game, such business models should be permitted.

- Outcome: Access, Deletion and Correction. The NTIA framework correctly recognizes that consumers should have *qualified* access to and ability to alter or delete personal data that they have provided. Limitations on these rights are necessary, for example,

where the original information is needed to detect security incidents, or to investigate (and prevent) incidents of cyberbullying, cheating, threats to the business's intellectual property, and other violations of the terms of service.

Moreover, any data access obligation should be designed to avoid the unintended consequence of putting consumers at risk of identity fraud. Importantly, organizations should be able to satisfy the access obligation by disclosing *categories* of information collected, rather than having to provide specific pieces of an individual's personal information, which increases the risk that an organization might inadvertently provide the consumer's personal data to a malicious actor posing as the consumer. For example, once a hacker obtains details about the consumer through one data breach, the hacker will likely be able to use that stolen information to "verify" the consumer's identity across a number of other websites and services, and leverage the access right to obtain even more detailed and sensitive information about the user.

For these reasons, ESA encourages NTIA to retain its proposed risk-based approach focusing on outcomes, and to resist any calls for more prescriptive mandates. A more prescriptive approach would undermine organizations' efforts to adopt privacy-protective measures that are understandable by and accessible to consumers based on the specific context.

Goals for Federal Action

The privacy outcomes described above are most likely achieved if NTIA supports the following goals for federal action:

- Goal: Harmonizing the Regulatory Landscape. ESA agrees that the regulatory landscape should be harmonized so that organizations are not faced with duplicative and contradictory privacy obligations. For example, with the European Union General Data Protection Regulation (GDPR) in force as of May 25, 2018,[2] many ESA members must now comply with privacy obligations both in the United States and in the European Union. The Administration's approach to privacy should therefore avoid major conflicts with international privacy frameworks.

  ESA also applauds NTIA's recognition that the U.S.'s current sectoral approach must nevertheless be maintained in order to address the varying privacy risks raised by different industries. The framework's privacy protections must account for the fact that, for example, a video game publisher's privacy practices are – and should be – much different from those of a healthcare provider. Moreover, application of the framework's principles should be calibrated based on the type of information at issue and the context in which the consumer data is collected and used. Under this approach, the framework can both provide legal clarity and consistency with respect to organizations' privacy obligations, while permitting organizations to build upon sector-specific principles that fit the particular circumstances in which they operate.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural personas with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR").

- Goal: FTC Enforcement. ESA agrees that the FTC is the appropriate federal agency to enforce consumer privacy (with the exception of sectoral privacy laws outside of the FTC's jurisdiction), but ESA encourages NTIA to ensure that the final framework also highlights the important role that self-regulation can play in protecting consumer privacy.

  ESA is in a unique position to provide an example of successful self-regulation by industry, and how such efforts could potentially create safe harbors to regulatory enforcement. In 1994, ESA established the Entertainment Software Rating Board (ESRB), a nonprofit, self-regulatory body that helps ensure responsible online privacy and advertising practices for the interactive entertainment software industry. Among other things, the ESRB established a Privacy Certified program, which consults members on how best to achieve compliance with a variety of federal, state, and EU privacy laws, and actively monitors compliance of over 1,000 websites and mobile applications. In 2001, the program became one of the first programs sanctioned by the FTC as an authorized "Safe Harbor" under the Children's Online Privacy Protection Act ("COPPA"), and the program also helps members secure certification under the EU-U.S. Privacy Shield Framework through protocols administered by the Department of Commerce.[3]

  Such self-regulatory programs should be the primary mechanism for protecting consumer privacy in the era of rapid change—particularly given the importance of being able to adapt to fast-paced evolutions in technology and business practices.

In short, ESA believes that a federal privacy regulatory framework must support several interrelated goals, many of which are enumerated by NTIA's proposal: the framework must provide legal clarity and be technology neutral, while at the same time affording sufficient flexibility to permit organizations to tailor their privacy controls to their unique circumstances and to create new, innovative ways to protect consumer privacy.

Key Terms

The key terms underlying any privacy framework must be sufficiently tailored to ensure that the framework adequately protects consumer privacy without creating overbroad, unnecessarily burdensome obligations on businesses. Importantly, the federal privacy framework should avoid defining the term "personal information" too broadly. The California Consumer Privacy Act's (CCPA's) definition, for example, includes any information that is "capable" of being associated with a particular consumer.[4] And the EU's General Data Protection Regulation (GDPR) defines personal data as "any information relating to an identified or identifiable individual."[5] Such definitions are so broad and unclear that they can be perceived to be limitless, at great expense to innovation.

Moreover, broad definitions of personal information could inadvertently do more harm than good with respect to protecting consumer privacy. For example, an overly broad approach

[3] For more information about the ESRB's online and mobile privacy program, see http://www.esrb.org/privacy/index.aspx.
[4] Cal. Civ. Code § 1798.140(o)(1).
[5] Art 4(1), GDPR (emphasis added).

may remove the incentive for organizations to use privacy-protective measures, such as using screennames, avatars, and device identifiers in lieu of more personal information (such as the user's actual name, photograph, address, phone number, or e-mail address). In addition, given that the risks of exposing de-identified data are significantly less than the risks of exposing personal data that identifies a particular consumer,[6] the two should not be treated the same under any federal privacy framework.

The definition of "personal information" is therefore a key area in which the United States can set a better example for the rest of the world by adopting a more risk-based definition that encourages companies to appropriately balance innovation with the impact on consumer privacy by using measures such as data pseudonymization and de-identification.

* * *

ESA and its members are committed to providing consumers with both strong privacy protections as well as innovative interactive entertainment software experiences, and any federal privacy framework should further such commitments. NTIA's draft proposal for the Administration's approach to consumer privacy is an excellent way to enable the United States to promote a flexible, commonsense approach to privacy that harmonizes the regulatory landscape while also being capable of keeping up with technological progress. ESA appreciates NTIA's effort on the draft proposal, and looks forward to working with you as the framework continues to develop.

Sincerely,

Stanley Pierre-Louis
Interim President and CEO
Senior Vice President and General Counsel

[6] Simson L. Garfinkel, *De-Identification of Personal Information*, NISTIR 8053, National Institute of Standards and Technology, at iii (2015) ("De-identification can reduce the privacy risk associated with collecting, processing, archiving, distributing, or publishing information").