February 18, 2011

By Electronic Filing

Federal Trade Commission
Office of the Secretary
Room H-113 (Annex)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Preliminary FTC Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" — File No. P095416

Dear Secretary Clark:

The Entertainment Software Association ("ESA") appreciates the opportunity to comment on the Commission's preliminary staff report on consumer privacy, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers."[1] The ESA is the exclusive U.S. organization dedicated to serving the needs of businesses that publish computer and video games for video game consoles, personal computers, and the Internet. With more than 30 members, the ESA represents nearly all of the major video game console manufacturers and game publishers in the United States.

The ESA commends Commission staff for holding several successful roundtables on consumer privacy issues over the last year and a half, which have culminated in the release of this preliminary report. Staff's efforts have fostered an important dialogue about consumer privacy in which the ESA is pleased to participate.

The ESA has long believed that innovation and a strong commitment to consumer privacy goes hand in hand with ensuring the continued growth of the entertainment software industry. With more than two-thirds of all American households playing video games, the entertainment software industry added $4.9 billion to the U.S. Gross Domestic Product in 2009 and continues to grow as a source of employment in communities across the nation.[2]

Recognizing the importance of building consumer trust, the ESA established the Entertainment Software Rating Board ("ESRB") in 1994. The ESRB is a nonprofit, self-regulatory body that, among other things, helps ensure responsible online privacy practices for the interactive entertainment software industry. In 1999, the ESRB's Privacy Online program became one of the first privacy seal programs sanctioned by the Commission as an authorized "Safe Harbor" under the Children's Online Privacy Protection Act ("COPPA").[3] The Privacy

[1] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2010) [hereinafter PRELIMINARY REPORT].
[2] *See* Entertainment Software Association, Industry Facts, http://www.theesa.com/facts/index.asp.
[3] For more information on the ESRB's Privacy Online program, please visit http://www.esrb.org/privacy/index.jsp.

Online program sets forth a number of requirements and best practices related to a variety of federal, state, and EU privacy laws and actively monitors the compliance of over 400 websites.[4] Many of the ESA's members voluntarily comply with the general privacy principles developed through the ESRB's Privacy Online program or privacy programs administered by other reputable self-regulatory entities.[5]

Based on more than a decade of experience with these self-regulatory programs, the ESA and its members believe that the Commission should continue to look to robust, enforceable self regulation as the primary mechanism for protecting consumer privacy in this era of rapid change. Self-regulatory programs not only can quickly adapt to evolutions in technology and business practices, but also can effectively promote both innovation and consumer privacy by fostering competition and promoting business practices that are most meaningful to consumers based on the context at issue.

EXECUTIVE SUMMARY

As staff work to finalize the preliminary report over the next year, the ESA urges staff to keep in mind the importance of developing a practical and flexible framework that is based on the context in which individuals and organizations interact. Context helps define consumer expectations, which have long been the standard the Commission has used to determine when and how privacy protections should be applied. For example, consumers have different expectations when they play a video game on their handheld or mobile device than when they browse the Web or pay their credit card bill online. Accordingly, the Commission should endorse general privacy principles that industries, and individual businesses, can build upon as new business models and technologies emerge in this ever-evolving digital economy.

In particular, the framework should be sensitive to the following contextual factors:

(1) ***Whether the Information Is Used Online or Offline***. While the report draws a number of analogies between online and offline activities, what is practical online may not always be so offline, and vice versa. For example, just-in-time choice might make sense for face-to-face transactions where an individual and a business are engaged in an ongoing dialogue. But, as explained below, such choice may be disruptive if required in the online gaming context, where the gaming user generally expects a seamless experience once game play has begun.

(2) ***The Industry in Which the Business Operates***. As staff appropriately recognize in the preliminary report, a sectoral approach to privacy is firmly ingrained in U.S.

---

[4] *See* Entertainment Software Review Board, Websites Certified by ESRB Privacy Online, http://www.esrb.org/privacy/sites.jsp (last visited Feb. 8, 2011).

[5] The ESRB, for example, actively monitors participating websites for compliance with six key privacy principles: (1) notice, (2) choice, (3) limiting data collection and retention, (4) data integrity and security, (5) data access, and (6) enforcement and accountability. *See* Entertainment Software Review Board, Web Publishers - Principles and Guidelines, http://www.esrb.org/privacy/reqs (last visited Feb. 8, 2011).

statutes and regulations.[6] If the U.S. moves toward broad-based consumer privacy protections, these 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. Consequently, the ESA urges staff to avoid prescribing specific privacy mandates and to instead focus on flexible principles that businesses can build upon to fit the particular circumstances in which they operate.

(3) ***The Type of Information at Issue***. Even within a given industry, it may be appropriate for different types of data to be subject to different standards. For example, individuals rightly expect that their Social Security numbers and debit card security codes will be treated with a greater degree of care than, for example, their usernames or IP addresses.

(4) ***Whether an Individual Has a Preexisting Relationship with the Business***. Individuals typically expect more personalized services from businesses with which they have long-standing relationships than from those with which they have not previously interacted. This is true online as well as offline. For instance, dedicated players of online games demand interactive features that allow them to create personalized gaming experiences, such as by building unique player-characters or designing custom in-game environments. These players may have different expectations about how console manufacturers and video game publishers are collecting and using their data than other participants who do not use these features.

In short, the ESA believes that it is vital that the Commission develop a practical framework that is sufficiently flexible to account for the various contexts described above and that can adapt as technologies and business models change. With this important point in mind, the remainder of the ESA's comments address some of the specific issues and questions raised in the preliminary staff report.

I. THE FRAMEWORK SHOULD NOT TREAT ALL INFORMATION WITHIN ITS SCOPE EQUALLY.

The preliminary report suggests that the scope of the proposed framework should be broad, reaching beyond personally identifiable information to include any "consumer data that can be reasonably linked to a specific individual, computer, or other device."[7] This approach would greatly expand the scope of transactions for which federal privacy obligations would be imposed.

---

[6] *See* Jessica Rich, Deputy Director, Bureau of Consumer Protection, Fed. Trade Comm'n, Roundtable Series 1 on Exploring Privacy 277:18-278:1 (Dec. 7, 2009), *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Dec2009_Transcript.pdf.

[7] PRELIMINARY REPORT, at ix.

This "reasonably linked" standard would include, for example, usernames, screennames,[8] avatars, IP addresses, MAC addresses,[9] cookie IDs, and device IDs[10] because each of these identifiers is, by definition, linked to a specific individual (usernames, screennames, and avatars) or a device (IP addresses, MAC addresses, cookie IDs, and device IDs).

Some of these identifiers, such as screennames and avatars, are employed specifically to avoid the collection of personally identifiable information, such as the user's name, likeness, address, landline or mobile phone number, e-mail address, Social Security number, or driver's license number. Tight regulation of these anonymous identifiers might have the unintended effect of encouraging more businesses to collect personally identifiable information, which could increase privacy risks for individuals.

Other identifiers, such as IP addresses, MAC addresses, cookie IDs, and device IDs, were created in order to enable the underlying technology, platform, or device to function. For example, in the Web-based video game context, as well as in other Internet-enabled gaming applications, collection and use of this data is often automatic, and subjecting its collection and use to heightened privacy protection, such as choice requirements, could prevent an individual's device or service from working. In addition, more detailed notice of how these identifiers are collected and used would only make privacy policies more complicated, with minimal consumer benefit.

Given the broad scope of the proposed framework, the ESA urges staff to clarify that the framework would not treat all information within its ambit equally. Rather, the application of the framework's principles should be calibrated based on the type of information that is at issue and the context in which the consumer data is collected and used. For example:

- Where the type of data that is at issue is particularly sensitive, such as the combination of financial and demographic data, it might make sense for some privacy practices to be particularly robust. In the video game industry, these types of information may be collected when consumers make purchases in online marketplaces where consumers can buy, for example, additional game features, new games, and other enhancements. While the Report appropriately recognizes that choice is not needed for such product and service fulfillment, the ESA's members still take steps to clearly inform consumers about how this information is collected and used and to help protect the security of this

[8] These comments employ the term "username" to mean the name users select solely for identification by a game or online service, while they employ "screenname" to mean the name users select for display to fellow users. While on many online services the same handle serves as both the username and the screenname, on others the two are distinct.

[9] A MAC address, or Media Access Control address, also called a physical address, is a unique number that identifies a computer or other device on a network. Curt Franklin, How Routers Work, http://communication.howstuffworks.com/convergence/router7.htm (last visited Feb. 9, 2011).

[10] A device ID is a generic term for the unique identifying number assigned to an electronic device by its manufacturer. Device IDs take a number of forms depending on device type and manufacturer.

information by implementing reasonable administrative, technical, and physical safeguards.

- In contrast, where a website operator requests that a user create a username and password to register for the website, the privacy by design principle may not be as robust and the choice and transparency principles may not apply at all since this information presents a minimal privacy risk to the user and choice can be implied by the creation of the account.

- In addition, anonymous identifiers, such as IP addresses, screennames, avatars, MAC addresses, cookie IDs, and device IDs serve various innocuous purposes that are helpful to businesses and present minimal privacy risks for consumers. In this context, choice should not be required, and privacy by design and transparency obligations should be calibrated based on context, such as the business's relationship with the individual.

These points provide a few examples of how a high-level, flexible privacy framework could appropriately apply to protect consumer privacy while ensuring that businesses remain able to offer innovative products and services.[11]

II. PRIVACY-BY-DESIGN MEASURES MUST BE FLEXIBLE SO THAT INNOVATION AND LEGITIMATE BUSINESS PRACTICES ARE NOT STIFLED.

The ESA supports flexibility in implementing privacy-by-design principles. However, the ESA is concerned that certain aspects of staff's data retention proposals may hamper innovation without providing consumers any meaningful privacy benefit.

A. Staff Properly Concluded That Company-Wide Privacy Measures Should Be Scaled to Their Operations.

Staff propose that "companies should incorporate substantive privacy and security protections into their everyday business practices and consider privacy issues systematically, at all stages of the design and development of their products and services."[12] This is a commendable goal, and the ESA's members strive to achieve it.

Staff also properly recognize that company-wide privacy measures must be tailored to avoid hindering innovation, which benefits businesses and consumers alike. Specifically, ESA agrees with staff's conclusion that company-wide privacy measures should "be scaled to each company's business operations" and that "[c]ompanies that collect and use small amounts of non-sensitive consumer data should not have to devote the same level of resources

[11] The voluntary, enforceable safe harbor industry codes recommended by the Department of Commerce's recent privacy green paper provide an alternative method to achieve this goal. *See* DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK 41-51 (2010) [hereinafter GREEN PAPER].

[12] PRELIMINARY REPORT at 44.

to implementing privacy programs as companies that collect vast amounts of data, collect data of a sensitive nature, or engage in the business of selling consumer data."[13]

The ESA agrees that while businesses should generally be attentive to the potential impact new products and services will have on consumer privacy (if any), the privacy-related policies and procedures implemented should vary with the type of product at issue, the data being collected, the size of the business, and the market in which the business is operating. Heightened restrictions may be appropriate where a company's business model depends primarily upon the collection and sale to third-parties of consumer data or requires the use of especially sensitive data such as health or financial data.

B. Inflexible Limits on Data Retention Time Periods and Purpose Specifications Are Inadvisable.

Staff seek comment on whether "there is a way to prescribe a reasonable retention period."[14] Any attempt to impose prescriptive limits on data retention time periods is inadvisable because such limits could impact legitimate business or operational purposes. For example, a publisher may need to contact a player of an online game long after that consumer's initial purchase of the game to inform the player of important software updates or significant changes in the terms and conditions for the online game service. In addition, a number of authorities, many of which are located abroad, require that companies retain data for a minimum time period for national security, law enforcement, and other purposes.[15] Explicitly defining the time period for which a company may retain user data would inevitably create irreconcilable conflicts with these nations' laws.

In addition, staff have asked whether the principle that businesses should retain data only for a "specific business purpose" needs further definition.[16] A definition that would limit use and data retention to narrowly defined purposes that are specifically described in a privacy notice could encourage companies to draft longer, more complicated privacy notices. To the extent the FTC further defines this concept, the ESA urges the FTC to recognize that a business's ability to retain consumer data should not be limited to the exact business purpose for which it was collected. Businesses often collect, use, and store data for multiple legitimate business purposes, some of which may not be known at the time the data is collected. For instance, information about an individual initially retained by a publisher of an online game to create enjoyable in-game experiences can later be used to assist in investigating incidents of cyberbullying, service attacks, or other violations of the provider's Terms of Service. If the business were compelled to delete the consumer data after the gaming session expires, the

---

[13] *Id.* at v-vi.
[14] *Id.* at A-1.
[15] *See, e.g.*, European Union Council Directive 2006/24 (Data Protection Directive), 2006 O.J. (L 105) 54 (EC) (Mar. 15, 2006), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (last visited Feb. 9, 2011) (requiring EU member states to ensure certain types of data are retained for at least six months and normally no more than two years, but authorizing states to require retention for periods of greater than two years where they are "facing particular circumstances that warrant an extension for a limited period").
[16] PRELIMINARY REPORT at 44.

business's ability to protect its users' safety and property rights and to enforce its Terms of Service would be impeded.

There also may be reuses of data that are important to continued innovation. For example, innovations such as caller ID and location-based services depend upon creative reuses of data. Thus, rather than trying to adopt one-size-fits-all purpose specification requirements, the ESA encourages the FTC to allow flexibility depending on, for example, user expectations and the benefits or drawbacks of permitting multiple uses.[17]

III. THE COMMISSION SHOULD EXPLICITLY RECOGNIZE THAT CONSUMER CHOICE REQUIREMENTS DEPEND UPON CONTEXT AND SHOULD REFRAIN FROM MANDATING ANY ONE-SIZE-FITS-ALL CHOICE MECHANISM.

The ESA supports the notion of simplified choice, but believes that any choice principle should be flexible and context-driven in order to accurately reflect consumer interests in both privacy and the development of innovative products and services.

A. Staff's List of "Commonly Accepted Practices" Should Recognize That Common Practices Will Depend on Context.

In its proposed privacy framework, staff identify a limited set of "commonly accepted practices" for which companies would be free to use consumer data without seeking consent. Specifically, companies would not need to obtain consent to use data for purposes of product and service fulfillment, internal operations, fraud prevention, first-party marketing, and legal compliance and other public purposes.[18] The ESA agrees that these business practices should not require consent, but urges staff to specify that this proposed list is not exhaustive.

In addition, the ESA agrees with staff that first-party marketing should be defined broadly to include sharing data with commonly-branded affiliates for their own use, sharing data with third party vendors who operate on the business's behalf, and using the data for contextual advertising. Similarly, the legal compliance and public purpose category should be interpreted broadly to fully protect the rights of the business, users, and third parties, even where consent is limited or lacking. For instance, in the context of intellectual property enforcement, an infringer is unlikely to wish to have his or her personal information collected, used, and disclosed for the purpose of enabling the business to initiate an infringement action. Nevertheless, data collection, retention, and disclosure must be permitted regardless of the infringer's expressed preferences in order to achieve the important public purpose of protecting intellectual property rights.

The ESA emphasizes, however, that while staff's attempt to identify commonly accepted practices for which consent is not required is laudable, the proposed list cannot be exhaustive because context matters. A comprehensive list for all situations is unachievable and

[17] *See* Verizon Department of Commerce Comment at 11-12; GE Department of Commerce Comment at 2. Comments are available at http://www.ntia.doc.gov/comments/101214614-0614-01/.
[18] PRELIMINARY REPORT at 54-55.

unworkable because what consumers accept as a common practice will depend upon a number of factors, including:

(1) ***Whether the Information Is Used Online or Offline***. Because e-commerce is driven by click through and conversion rates, consumers may have different expectations in the online context than in the offline context when it comes to sharing data about, for example, the stores that they visit.

(2) ***The Industry in Which the Business Operates***. In the video game context, for example, console manufacturers and video game publishers offer access to a number of online gaming features and content to consumers as a joint service. Even though the consumer data is not used solely for internal operations, consumers commonly understand and accept that their information must be shared between the console manufacturer and game publishers in order for these joint services to function.

(3) ***The Type of Information at Issue***. For example, while consumers commonly expect that a bank or a prospective employer will request a Social Security Number to conduct background or credit checks, such practice would not be commonly accepted if such information was requested by, for example, a retailer for marketing purposes.

(4) ***Whether an Individual Has a Preexisting Relationship with the Business***. Consumer expectations about how a business may collect, use, and disclose consumer data may vary depending on whether the consumer has purchased a product or service directly from the business before or has no direct relationship with the business.

Additionally, what consumers accept as a common practice evolves over time as once-new technologies become more familiar. For example, a decade ago many consumers were unfamiliar with the idea of publicly sharing status updates. Today, however, millions of consumers use microblogging services, such as Twitter, social networking websites, and video game handhelds to share this information broadly because they find these services to be valuable.

To the extent that the Commission wants to retain the concept of "commonly accepted practices," industry groups may be able to play a role in helping consumers learn more about an industry's common privacy practices. For example, an industry group could host a webpage that provides tools to improve transparency, including an overview of technical terms (such as web beacons) or simple illustrations of data flows (such as what happens when an Internet browser loads a web page). In turn, participating members could link to this page in their privacy policies as a way to simplify and shorten consumer notices. To be clear, not all members in a single industry should be obligated to use one particular industry privacy notice or link to a specific set of information. Rather, businesses should be free to leverage materials

prepared by an industry group if such information appropriately fits their technologies and business models.

B. Just-in-Time Choice Is Impractical in Some Contexts, Such As Video Games.

The ESA agrees with staff that in some contexts, it is appropriate to provide consumers with choice at the point when they provide their data. However, the ESA urges the Commission to clarify that just-in-time choice is not always possible or advisable. In the video game context, for example, it often would disrupt the user experience to require just-in-time choice every time a particular gaming website, console-based game, or online service, such as in-game chat, is launched or in-game advertising appears.

For instance, the presidential campaign of then-Senator Barack Obama relied on in-game advertising by purchasing virtual billboards in the car racing game Burnout Paradise.[19] These billboard messages reminded players living in swing states to register to vote early and to visit the campaign's website. Players of Burnout Paradise would have been frustrated if the game "hit the brakes" to ask for their consent to allow the campaign to use geographic information for this purpose. Accordingly, in circumstances where just-in-time choice would be disruptive, businesses should have the flexibility to rely on different choice mechanisms that are appropriate for the context, such as building user controls into the video game's menu or into the console's user control settings.

C. "Take It or Leave It" Choice Is Appropriate in Some Contexts.

In some circumstances, it is appropriate to offer choice as a "take it or leave it" proposition, whereby a consumer's use of the website, product, or service constitutes consent to the company's information practices. Some legitimate business models could not function if more stringent choice requirements were applied. For example, in order to offer consumers more choices for accessing game content, many publishers in the video game industry are publishing some games on a "free to play" basis or providing "free to play" versions of games, relying on advertising that may be targeted based on broad geographic location, time of day, or other factors, to cover the costs of developing and operating these games. It is clear from the nature of the games that there is an implicit exchange in which the game is free so long as such advertising can be provided. As long as the publisher notifies the consumer upfront that the game has such advertising so that the consumer can make an informed choice about whether or not to play the game, "take it or leave it" choice should be permitted.

D. Requiring Enhanced Consent for Teens Would Not Be Effective.

COPPA is clear that verifiable parental consent requirements apply only to children under 13.[20] While we understand that the FTC is not proposing to increase the age of persons covered by COPPA, it would be inappropriate for the Commission to go beyond the

[19] *See* ESA, http://www.theesa.com/gamesindailylife/advertising.asp (last visited Feb. 9, 2011).
[20] *See* 15 U.S.C. §§ 6501-6506.

limits of COPPA by imposing any enhanced consent requirements for teens absent an expansion in statutory authority.

Many industries, including the entertainment software industry, have developed their business practices and built compliance mechanisms in reliance on the "under 13" threshold for enhanced consent. Having to adjust these business practices and reengineer these mechanisms to accommodate a new form of enhanced consent for teenagers would not be a trivial exercise. In addition, there is no guarantee that enhanced consent requirements would actually benefit teens since there currently is no reliable way to differentiate teenagers from adults online.

Rather than requiring enhanced consent, which teens could quickly circumvent and which could discourage businesses from offering valuable online services to teens, the Commission should focus on improving digital literacy among teenagers. For instance, the Commission could build upon its existing educational resources, such as its successful AdMongo campaign, to create similar programs for teenagers.[21]

E. "Do Not Track" Mechanisms Should Avoid Market Disruptions and Should Be Industry Driven.

The ESA agrees with staff that do-not-track mechanisms must "not undermine the benefits that online behavioral advertising has to offer, by funding online content and services and providing personalized advertisements that many consumers value."[22] Advertising, and increasingly behaviorally targeted advertising, supports free and reduced-price online content, services, and mobile applications. If large numbers of consumers opt out of behavioral advertising, the free and open Internet as we know it could be transformed in ways that are hard to predict and difficult to reverse.

At this time, we do not believe that a statutory mandate implementing do-not-track requirements is necessary or advisable. The marketplace already offers a number of tools that consumers can use to control whether and how their online activities are tracked. These tools include applications (such as Ghostery), browser add-ons (such as the Targeted Advertising Cookie Opt-Out ("TACO") tool), self-regulatory tools (such as the opt-out mechanism offered through the Self-Regulatory Program for Online Behavioral Advertising), and do-not-track mechanisms that have been built in to new versions of web browsers (such as Internet Explorer 9's Tracking Protection). Statutory mandates could have the unintended consequence of preferring one technological solution over the others and could quickly become obsolete. Rather than chilling innovation in the development of new mechanisms for providing consumer choice, the ESA urges the Commission to encourage industry's important efforts in this area.

---

[21] *See* AdMongo.gov, http://www.admongo.gov (last visited Feb. 9, 2011).

[22] PRELIMINARY REPORT at 67.

While industry has developed a number of innovative browser-based technologies that enable consumers to exercise more control over how their web-based activities are tracked, extending these approaches to other online contexts, such as the gaming context, may present additional technical and practical challenges for implementing do-not-track functionality. In these circumstances, clear and simple privacy notices that inform consumers about how they can exercise choice are most appropriate.

IV. STAFF'S TRANSPARENCY PROPOSALS ARE LAUDABLE, BUT IMPLEMENTATION MUST DEPEND ON CONTEXT.

Like staff, the ESA believes transparency is central to a meaningful consumer privacy framework. But requiring businesses to provide consumers with more information, or more standardized information, does not guarantee that consumers will be more adequately informed. Rather, the transparency principle is best achieved when requirements are based on context. Below, the ESA lists specific ways in which the Commission can adapt the preliminary report's transparency proposals to best inform consumers while at the same time ensuring that the framework remains workable as technologies and business models continue to evolve.

A. "Standardized" Notices Should Be Industry Specific.

A "standardized" privacy notice will be most useful if it is specific to the particular industry at issue. Any attempt to reach standardization at a more universal level would require the terms to be so vague or the disclosures to be so lengthy that the policy would be of little value to consumers. Consumers likely expect that the notice provided by the website operator for a massively multiplayer online game, for example, will be different from that provided by the operator of a web-based email service. Industry should take the lead in developing greater standardization to encourage more concise privacy policies and to help simplify communication with consumers. To this end, industry groups could play a helpful role in driving such efforts.

B. The FTC Should Clarify the Meaning of a "Material Change."

The preliminary staff report states: "[u]nder well-settled FTC case law and policy, companies must provide prominent disclosures and obtain opt-in consent before using consumer data in a materially different manner than claimed when the data was collected, posted, or otherwise obtained."[23] Staff is correct to maintain the distinctions between material and non-material changes and between changes which apply retroactively and those which apply prospectively. That said, the preliminary report offers little guidance on the changes that rise to the level of a "material" change in various contexts. Given the broad categories of data that will be subject to the framework, this may result in businesses issuing multiple notices (and seeking multiple consents) over short periods of time for relatively minor changes. The ESA thus encourages the Commission to define "materiality" with a bright line that minimizes the

[23] *Id.* at 77.

risk of burying consumers in a flood of privacy notice updates from numerous online services. Like the boy who cried wolf, these notices would be ignored if they were too frequent.

C. Where Needed, Consumer Access to Data Should Depend Upon A Sliding Scale of Factors.

The ESA encourages the Commission to clarify that granular access to consumer data is unnecessary unless the data will be used for a decision-making purpose, such as whether to extend the consumer credit or to offer the consumer a particular product or service. In our experience, there is little, if any, consumer demand for data access outside this context. Requiring access in other circumstances could impose significant costs on businesses and create risks of identity theft with minimal corresponding consumer benefit.

To the extent that the need for access to a wider variety of consumer data can be demonstrated, the ESA supports staff's suggestion that a "sliding scale approach" be used to determine when consumers should have access to the data that is collected from and about them.[24]

V. COMMISSION AND INDUSTRY EFFORTS TO DEVELOP THESE PRINCIPLES AND TO ENCOURAGE MEANINGFUL PARTICIPATION CAN, AND SHOULD, BE COMPLEMENTARY.

In general, ESA believes that staff has developed a framework that industry can build upon through self-regulation and best practices. Industry is in a unique position to understand how this framework might apply in practice and to tailor the application of the principles accordingly.

The video game industry, for instance, has a strong track record of developing innovative solutions to privacy and other social issues. Specifically, parental controls on all of the major current generation console video game systems offer parents significant control over their children's online video game activities, including how they interact with others online. The controls are easy-to-use, widely recognized, and can be implemented in a matter of minutes.[25] Moreover, as the Commission is aware, the ESRB provides voluntary content ratings to the vast majority of video games on the market today.[26]

However, industry cannot do it all alone, and the Commission has an important role to play. This does not mean that the Commission should compete with or frustrate industry self-regulation by imposing prescriptive requirements that are based on universality rather than context. Rather, it is important that Commission and industry efforts be complementary. Consumer education is an example where industry and the Commission can work together and in parallel to educate consumers about privacy issues and to encourage consumers to take an active role in managing their information. While businesses are best

---

[24] *Id.* at 74.

[25] *See* Entertainment Software Association, Comments in COPPA Rule Review, P.104503 at 4-6 (June 30, 2010), *available at* http://www.ftc.gov/os/comments/copparulerev2010/547597-00048-54857.pdf.

[26] *See* Entertainment Software Review Board, http://www.esrb.org (last visited Feb. 9, 2011).

suited to educate consumers about privacy options specific to their particular products and services, the Commission can educate consumers more broadly about the importance of privacy and the contours of privacy law.

In addition, the Commission's enforcement activities should be limited to clear instances of unfair or deceptive practices that result in identifiable consumer harm.[27] For decades, the Commission has served this role effectively, and it should continue to do so. Bad actors who tangibly harm consumers through their lack of attention to privacy undermine consumer confidence in all innovative services, and Commission action against such entities is appropriate. However, the ESA urges the Commission to refrain from acting beyond the bounds of its authority by pursuing enforcement actions in other contexts that have the effect of imposing prescriptive rules on industry.

VI. CONCLUSION.

The ESA and its members are committed to protecting consumers' privacy, and we believe that staff's preliminary report provides an excellent springboard for encouraging further discussion around this vital issue. As the Commission prepares the final version of its report, the ESA believes that it should focus on the importance of developing flexible rules which can be applied by businesses as is appropriate to the industry in which they operate. By crafting a report which establishes general principles that can be adapted to a wide variety of contexts, the Commission can be certain that it is benefiting consumers both by ensuring that their privacy will be respected and by preserving opportunities for businesses to make innovative products and services available to them.

Respectfully submitted,

_____

Erin M. Egan
Lindsey L. Tonsager
COVINGTON & BURLING LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004

Counsel to the Entertainment Software Association

cc: Michael Warnecke, Senior Policy Counsel, ESA

[27] *See* Letter from the FTC to Hon. Wendell Ford and Hon. John Danforth, Committee on Commerce, Science, and Transportation, United States Senate, Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction, *reprinted in In re Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984) (stating that absent deception, the Commission will not enforce Section 5 against alleged intangible harms).