December 19, 2011

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

RE: FTC COPPA Rule Review, 16 CFR Part 312, Project No. P104503

Intel Corporation would like to thank the Federal Trade Commission (FTC) for the opportunity to comment on the proposals to amend the Children's Online Privacy Protection Rule (COPPA Rule). Intel strongly believes that changes in technology should not erode privacy protections for children, and we appreciate the Commission's diligent work on this issue. In response to the Commission's request for comments on the proposed rule, Intel would like to offer the following views.

I. The Computing Continuum

Intel is a leading manufacturer of computer, networking, and communications products. Intel has almost 100,000 employees, operating in 300 facilities in 50 countries. In 2010, Intel had over $40 billion in revenue from sales to customers in over 120 countries. Intel develops semiconductor products for a broad range of computing applications.[1] These products are some of the most innovative and complex products in history. For example, an IntelCore i7® processor has over one billion transistors on each chip. It is our stated mission to serve our customers, employees, and shareholders by relentlessly delivering the platform and technology advancements that have become essential to the way we work and live. It is part of our corporate strategy to fulfill this mission by tackling big problems such as the digital divide, education, energy/environment, services, and health. However, we consistently hear that one of the barriers for using technology to address these problems is the concern that personal privacy will not be protected. Thus, Intel believes that putting in place a legal and regulatory system that provides for strong privacy protections is key to the growth of our business.

[1] Intel also has recently acquired McAfee, Inc., a leading security technology company, which operates as an independent subsidiary of Intel Corporation. McAfee provides products such as antivirus software, cybersecurity threat detection, family protection, and spam filtering.

Intel's core product, the microprocessor, drives computers and servers, thus directly impacting the online experience of most individuals. Intel sees the future growth of technology moving toward a computing continuum. Specifically, computing is moving in a direction where an individual's applications and data will move as that person moves through his or her day. The person will wake to being able to access data on a certain device in his or her home, will transition to a car that has access to those applications and data, will have access at work (which often will not be in a traditional office), and then will access the data and applications after work either at home or while socializing. To manage these applications and data, the individual will use a wide assortment of digital devices including laptop computers, tablets, televisions, and handheld devices.

The development of the computing continuum will have substantial benefits for consumers. One example illustrates this well. Soon, an individual's smartphone will be able to communicate with an individual's car (which some in Intel are calling a "computer on wheels"). The GPS functions in both devices will "know" that the devices are in the same location and that they are traveling at the same speed; thus, they will know that a specific individual is driving with the phone in the car. If the driver gets a text message, the message would not be displayed on the phone. Instead, the speaker in the car can ask the driver whether he or she wants the car's computer to read the text message. When the phone leaves the car, the devices will communicate with each other and the phone can again display text messages directly on the device.

The development of the computing continuum also allows computing to become personalized and contextually aware. Devices across the continuum will combine "hard sensing" and "soft sensing" inputs. For instance, "hard sensing" inputs would know whether a user is sitting in front of a laptop (via the laptop camera), whether an individual is sitting, walking, or running (through an accelerometer), whether an individual is chatting, commuting, or listening to music (through a device microphone), whether an individual is outdoors or indoors or whether it is light or dark (through sensors on the device), and the individual's location (through GPS). "Soft sensing" inputs could pull information from an individual's calendars, social networking activity, browsing habits, personal preferences, and device activity. For a simple example, a television will be able to determine which person is holding a remote control and can automatically change the interface and user experience to personalize it for each person. For a more complex interaction, a music player might determine that an individual is running, that it is the morning, and that the individual has been awake for at least 30 minutes. Based upon the individual's preference for listening to music in the morning while running, the music player will automatically know the appropriate music to play. The aggregation of context over time and over devices will fundamentally change the way that consumers interact with their computing devices.

Intel's goal is to provide the semiconductor products that will serve as the primary computing components for those devices. It is central to our strategy that individuals will have trust in being able to create, process, and share all types of data, including data that may be quite sensitive, such as health and financial information. One of our goals is to develop

technology that provides individuals with choice and control for how their devices will manage their data. Intel is well on its way to innovating these future technologies. However, all of this innovation requires a policy environment in which individuals feel confident that their privacy interests are protected. Building a trusted environment in a systemic way not only benefits consumers and increases their trust in the use of technologies, but is vital to the sustained expansion of the Internet and future ecommerce growth.[2] Intel encourages the FTC to consider the future growth of the computing continuum when finalizing the COPPA Rule.[3]

II. General Scope of the Proposed Rule

We would like to comment on two definitional aspects related to the scope of the proposed rule: (1) the definition of a "child" and (2) the definitions of the terms "website located on the Internet" and "online service."

A. Definition of a "Child"

COPPA defines a "child" as "an individual under the age of 13." In the proposed rule, the Commission does not advocate for a statutory change to raise the age for a "child" to cover a greater range of adolescents. We support the Commission's decision not to seek a change in the definition of a "child." Children under the age of 13 may not have the judgment or knowledge to make decisions about whether and how to divulge personal information online, but there is not sufficient empirical evidence to suggest that those same concerns apply to individuals over the age of 13. Moreover, COPPA's under-13 categorization has become the de facto global standard, with other jurisdictions internationally also basing their child privacy protections on this age range. Without further demonstrable evidence that the current statutory definition is inappropriate, we support the Commission's decision to not seek further legislative action on this issue.

B. Definitions of "website located on the Internet" and "online service"

One of the more significant aspects of the proposed rule is the Commission's decision to explicitly bring evolving technologies, such as mobile communications, interactive television, and interactive gaming, among others, within the scope of the COPPA definitions "website located on the Internet" and "online service." As discussed above, we believe that technology is moving in a direction of a computing continuum where devices will be connected and data will flow freely between different devices and platforms. Individuals, including children, will be

---

[2] Intel recently released a policy position paper outlining our views on the policy framework needed for the interconnected Internet environment. *See* John Miller and David Hoffman, "Sponsoring Trust in Tomorrow's Technology: Towards a Global Digital Infrastructure Policy," *available at* http://intel.ly/qDnMFR.

[3] Intel has long supported the passage of comprehensive U.S. federal privacy legislation, as we believe such legislation is foundational so that individuals can have trust and confidence in their use of technology. As a result, we have testified in Congress in favor of privacy legislation and have filed comments on the FTC preliminary staff report, *see* http://www.ftc.gov/os/comments/privacyreportframework/00246.html, and the U.S. Department of Commerce "green paper," *see* http://1.usa.gov/qmHaP5, advocating for such baseline privacy protections.

able to access the same information from many different devices and from many different locations.

We support the Commission's inclusion of these evolving technologies within the COPPA Rule. Not only is the change squarely supported by the statutory definitions, but it also would be nonsensical to have one set of rules apply to information collected from a PC, while a different set of rules would apply to the collection of that same information from a mobile application. We believe that the Commission's proposed approach is already being realized technologically and will only become more prevalent as technology continues to develop across a continuum. Thus, we urge the Commission to retain the proposed interpretation of these definitions in its final rule.

III. Definition of "Personal Information"

Intel would like to comment on three aspects of the proposed rule's treatment of the "personal information" definition: (1) the exception for activities necessary to protect the security and integrity of a website; (2) the issue of persistent identifiers; and (3) a video or audio file of a child.

A. Support for Internal Operations

The Commission proposes to expand the definition of "personal information" to include "screen or user names" and "persistent identifiers," when such items are used for functions other than or in addition to "support for the internal operations of the website or online service." In proposing to create a separate definition of "support for the internal operations of a website or online service," the Commission also proposes to expand that definition to include "activities necessary to protect the security or integrity of the website or online service." With this proposed change, the Commission states that it is recognizing operators' need to protect themselves or their users from security threats, fraud, denial of service attacks, user misbehavior, or other threats to operators' internal operations.

Intel believes that the addition of this definition is a necessary and important addition to the COPPA regulatory framework. As noted, Intel has recently acquired the security technology company McAfee. To provide necessary protections to computer systems, McAfee products analyze certain data such as IP addresses and URLs. Thus, a technology-neutral and sufficiently broad security exemption, such as that proposed by the Commission, is critical to ensure that efforts to protect users (and children) from malicious viruses, spyware, spam, and objectionable content are not impeded.

B. Persistent Identifiers

In its Statement of Basis and Purpose on the original rule, the Commission stated that persistent identifiers such as static IP addresses and processor serial numbers would not be considered "personal information" "unless such identifiers are associated with other

individually identifiable personal information." When discussing information stored in cookies, the Commission stated that "[i]f the operator either collects individually identifiable information using the cookie or collects non-individually identifiable information using the cookie that is combined with an identifier, then the information constitutes 'personal information' under the Rule, regardless of where it is stored." These two statements together have, to date, limited COPPA's coverage of persistent identifiers solely to those identifiers that are otherwise linked to "personal information" as defined by the Rule.

In the proposed rule, however, the Commission states that it believes that persistent identifiers can permit the contacting of a specific individual, and thus, should be included as part of a revised definition of "personal information." The Commission states that it does not agree with commenters who argue that persistent identifiers only allow operators to contact a specific device or computer. The proposed rule believes that, increasingly, consumer access to computers is shifting from the model of a single, family-shared, personal computer to the widespread distribution of person-specific, Internet-enabled, handheld devices to each member within a household, including children. The proposal states that such handheld devices often have one or more unique identifiers associated with them that can be used to persistently link a user across websites and online services, including mobile applications. Thus, the Commission argues that operators now have a better ability to link a particular individual to a particular computing device.

We disagree with the proposed rule, and believe that a per se expansion of the definition of "personal information" to include all unique persistent identifiers is unwarranted, both as a matter of policy and as a matter of technology. Instead, we believe that persistent identifiers should only be considered "personal information" if the identifiers contain or are likely to be combined with data that can be "reasonably linked to a specific consumer, computer, or other device."

Conceptually and as a matter of policy, Intel agrees that the definition of "personal information" should apply broadly to information that is reasonably likely to relate to an identifiable individual. We caution, however, against language that may apply to computers or devices that will not relate to an individual. With the development of the computing continuum, we will continue to see the use of unique identifiers in hardware and software that can be used to identify the device. There are many examples, however, in which the collection of these identifiers may be done in a way that does not make it reasonably likely that the information will relate to an identifiable individual. For example, servers will have data that is linked to having been stored or processed by that particular server. However, given the great number of individuals who may use a particular server, it may be highly unlikely that data will relate to an identifiable individual, and therefore it may be unduly burdensome to apply a privacy framework to that data. Any regulatory language on this topic should encourage product developers to design the use of these unique identifiers so they are unlikely relate to identifiable individuals. Language that sweeps in all identifiers would actually be counter to incentivizing this implementation of privacy by design.

A much better model would be to focus the new framework on a scope of data that is reasonably likely to relate to an identifiable individual, and over time to define what that means. The Commission could then offer guidance that organizations can use to take technical, business, or policy steps to make it unlikely the data will relate to an identifiable individual. An example of such a policy step would be for a company to commit in its privacy policy that it will not relate two different databases, and thereby subject itself to enforcement under either the COPPA Rule or Section 5 of the FTC Act if they act contrary to that representation. Such a representation should make the data unlikely to relate to an identifiable individual, and there would be sufficient enforcement recourse if the data was nevertheless linked improperly.

Additionally, as a matter of technology, the proposed rule's definitional expansion is also unwarranted. The development of the computing continuum does not mean that one person will only use one device. To the contrary, as computing becomes more ubiquitous, individuals will each interact with a variety of devices in a variety of ways. Several different members of a family, for instance, may interact with the Internet-enabled television, refrigerator, or car, sharing information back and forth and among a variety of devices. It will not be true, as the Commission proposes, that each individual will have a person-specific Internet-enabled device. Instead, virtually all devices will be Internet-enabled and those devices will be able to adjust their settings and content based upon the person with whom the device is interacting; many individuals may be using the same device and it may be adjusted to their preferences.[4] Under this scenario, the persistent identifiers of those shared devices may or may not be able to relate to an identifiable individual and whether the device does so is context dependent. Accordingly, we believe that the Commission's proposed per se treatment of persistent identifiers is incorrect and should not be included in the final proposal.[5]

C. Video or Audio File of a Child

In the proposal, the Commission states that it believes that the Rule's definition of "personal information" should be expanded to include the posting of video and audio files (including photos) containing a child's image or voice, which it purports may enable the identification and contacting of a child.

We believe that the Commission's proposed definition is both prematurely made and too broad. First, the Commission acknowledges that it only received little comment on the issue. Before proposing to expand the definition, it should have solicited additional public comment. Second, the Commission justifies its new definition by stating that facial recognition

[4] For instance, see the discussions in the book "Screen Future: The Future of Entertainment, Computing, and the Devices We Love," authored by Intel futurist Brian David Johnson and published in 2010 by Intel Press.

[5] We also disagree with the FTC's proposal to require parental consent if a persistent identifier trackers a user across websites, as this proposal could hinder the effectiveness of security protection. Security providers such as McAfee gather and analyze persistent identifier information across websites to prevent against security attacks. The FTC's proposal would mean that security services could not track any user who visited a child-directed website unless a parent provided verifiable consent. This proposal would interfere with providing security protection to child-directed websites and should be reconsidered.

technology can be used to identify persons, thus necessitating the inclusion of photos and video files within the definition. But in doing so, the Commission only cites to one magazine article.[6] The FTC has announced a workshop to gather more information on and to explore facial recognition technology.[7] It would seem prudent for the Commission to wait for that process to develop before using such technology as a reason to expand this rule.

Finally, the proposed definition is too broad from a practical standpoint. For instance, this definition could include the broadcast available over the Internet of a sporting event with children in the crowd. Also, many families are using internet connected security cameras in their homes, and these cameras will frequently capture video images of children who visit the home. Privacy risks from these situations are limited and it would seem to be outside the core of what COPPA is intended to cover. Thus, we propose limiting the Commission's new definition to "a photograph, video or audio file where such file contains a child's image or voice *which may reasonably allow identification of the child*" (proposed addition italicized), and to specifically carve out the use of cameras within the home. These limitations would protect children's privacy and also avoid unnecessarily bringing other conduct within the statute's scope.

IV. Authentication and Verifiable Parental Consent

As a form of determining verifiable parental consent, the Commission proposes allowing operators to collect a government-issued form of identification, such as a driver's license or social security number, and check it against databases of such information. We share the concern expressed by some[8] that this proposal would require a website operator to collect a great amount of parents' data, thus presenting privacy concerns.

This approach seems contrary to the need for collection limitations and data minimization expressed by the FTC's recent preliminary staff report on privacy. Further, we see no mention or reference to ongoing government-wide efforts to examine the issue of authenticating online identity. We encourage the Commission to collaborate with the National Strategy for Trusted Identities in Cyberspace (NSTIC), a White House initiative to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the privacy, security, and convenience of sensitive online transactions. The strategy calls for the development of interoperable technology standards and policies in which individuals, organizations, and the underlying Internet infrastructure can be authoritatively authenticated. It would seem that policies developed in this forum would aid the parental consent process under COPPA.

---

[6] *See* footnote 88 and accompanying text in the proposed rule.

[7] *See* http://www.ftc.gov/opa/2011/09/facialrec.shtm.

[8] *See* blog post by the Center for Democracy and Technology at http://www.cdt.org/blogs/emma-llanso/199ftc-rightly-keeps-coppa-focused-children.

V. Conclusion

Intel thanks the FTC for providing the opportunity to comment on the proposed rule. We look forward to continuing our engagement with the Commission to improve the effectiveness of the COPPA Rule and the overall protection of privacy.

Respectfully Submitted,

David A. Hoffman
Director of Security Policy and Global Privacy Officer
Intel Corporation

Brian Huseman
Senior Policy Counsel
Intel Corporation