

**PREPARED STATEMENT OF**

**INTEL CORPORATION**

**before the**

**COMMITTEE ON ENERGY AND COMMERCE**

**SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION**

**U.S. HOUSE OF REPRESENTATIVES**

**on**

**“The BEST PRACTICES Act of 2010” and other**

**Federal Privacy Legislation**

**JULY 22, 2010**

## I. Introduction

Mr. Chairman and Members of the Subcommittee, I am David A. Hoffman, Director of Security Policy and Global Privacy Officer of Intel Corporation. I appreciate the opportunity to appear before you today to discuss federal privacy legislation and specifically the BEST PRACTICES Act circulated by Chairman Rush and the discussion draft bill circulated by Chairman Boucher and Ranking Member Stearns.

Intel Corporation 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. The two bills include many of the important concepts for a comprehensive U.S. privacy law, and we strongly support Congress' efforts to legislate in this area. I congratulate you on the work you have done to protect consumer privacy and to promote continued technological innovation. Intel thanks Chairman Boucher for putting forward such a thoughtful and important draft from which to build on, and with the minor changes discussed below, Intel supports the BEST PRACTICES Act and believes that its enactment would help further consumer privacy and the growth of the Internet.

## II. Need for Federal Privacy Legislation

Intel is the leading manufacturer of computer, networking, and communications products. Intel has over 80,000 employees, operating in 300 facilities in 50 countries. In 2009 Intel had over \$37 billion in revenue from sales to customers in over 120 countries. Intel develops semiconductor products for a broad range of computing applications. These products are some of the most innovative and complex products in history. For example, an Intel Core i7 processor has over 781 million 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.

Intel currently markets and is in the process of designing a wide array of products to work on these big problems. Our core product, the microprocessor, drives computers and servers, thus directly impacting the online experience of most individuals. Intel sees computing 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 having 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 servers, laptop computers, tablets, televisions, and handheld PCs. 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. 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.

Intel is not working alone to make these innovations a reality. Companies worldwide need to be able to work with each other to bring innovative solutions to the global market. In the technology sector, it is rare when one company can work in isolation, whether they are creating hardware components, portions of the software stack, or services layered on top of the hardware and software. Companies need access to the best available people, processes and technology, to continue the innovations necessary to drive the global digital infrastructure and remain competitive in the global marketplace. Laws and regulations impacting the ability to collaborate and share information need to keep pace with our technical need for such collaboration. At the same time, and in addition to these technical preconditions, building trust in the digital economy is an essential component of driving the global digital infrastructure forward. 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.<sup>1</sup> Intel strongly believes that comprehensive U.S. federal privacy legislation is a key mechanism for building this consumer trust in the Internet and ecommerce.

### III. Overall Framework of the Bill

Intel is pleased that the BEST PRACTICES Act is technology neutral and gives flexibility to the FTC to adapt the bill's principles to changes in technology. Maintaining technology neutrality in the legal framework provides protection for individuals in a rapidly evolving technological society, as the creation of legislative and regulatory requirements will invariably trail innovation of new technology. Therefore, a focus on the application of principles -- neutral to the technology used -- enables a flexible, effective, and timely response.

We are supportive of providing rulemaking authority to the FTC to flesh out certain specific requirements and to adapt the bill's provisions to changes in technology. This rulemaking authority will provide flexibility for the FTC to respond to further innovation in technology and business models, and can be further enhanced by the FTC's use of workshops and enforcement guidance. Specifically, we are pleased that the BEST PRACTICES Act allows the FTC to conduct rulemakings in several sections: Section 2(8)(B) (allows the FTC to modify the definition of "sensitive information"); Section 2(10)(C) (allows the FTC to modify the definition of "third party"); Section 102(b) (allows the Commission to conduct a rulemaking on the

---

<sup>1</sup> Intel has recently released a paper outlining our vision of the Global Digital Infrastructure, "*Sponsoring Trust in Tomorrow's Technology: Towards a Global Digital Infrastructure Policy*," available at [http://blogs.intel.com/policy/2010/07/intel\\_releases\\_global\\_digital\\_infrastructure\\_vision\\_paper.php](http://blogs.intel.com/policy/2010/07/intel_releases_global_digital_infrastructure_vision_paper.php).

content and delivery of notices to consumers); Section 102(d) (allows the FTC to modify the retention requirement for notices); Section 201 (allows the Commission to promulgate regulations on the accuracy of information); Section 202(j) and (k) (allow the Commission to promulgate rules on the exceptions to the right of access); Section 301 (the Commission can promulgate regulations on the Safeguards requirement); Section 404 (the Commission can approve a Choice Program); and Section 501(c)(2) (the Commission can promulgate rules regarding the reconstructing or revealing of identifiable information).

All of these issues in which Chairman Rush's bill has allowed for the possibility of FTC rulemaking are highly contextual. It is critical to note the importance of context and to allow flexibility so that the bill can continue to apply to the information necessary to create trust in the digital economy. Having this flexibility is the only way to ensure that this bill will be able to stand the test of time.<sup>2</sup> We also are supportive that the bill provides specific criteria that the Commission should use in making its determinations in those areas in which the FTC has been granted rulemaking authority. Only allowing the FTC to make rules that are consistent with congressional intent has worked well in other consumer protection statutes. *See, e.g.*, The CAN-SPAM Act of 2003, 15 U.S.C. 7702(17)(B) ("The Commission by regulation pursuant to section 7711 of this title may modify the definition in subparagraph (A) to expand or contract the categories of messages that are treated as transactional or relationship messages for purposes of this chapter to the extent that such modification is necessary to accommodate changes in electronic mail technology or practices and accomplish the purposes of this chapter."). As with CAN-SPAM, Intel recommends that the FTC make certain that all regulations issued under this rulemaking authority should also be technology neutral, and that most context specific determinations are best handled by individual enforcement actions.

We also are generally supportive of the bill's enforcement structure. We are pleased that both bills provide enforcement powers to the Federal Trade Commission and state Attorneys General. However, we prefer the provisions in the draft by Chairman Boucher that do not allow for a private right of action. We believe that allowing a private right of action will create unnecessary litigation costs and uncertainty for businesses, but will not have a corresponding benefit to protecting consumer privacy. We believe that strong and consistent enforcement by the FTC and the state attorneys general is more than sufficient to ensure compliance with the statute. Further, allowing for punitive damages, as in section 604 of the BEST PRACTICES Act, only further exacerbates the difficulties present in such a scheme. However, if a private right of action is included, we recommend also including the safe harbor from liability for those organizations participating in an approved Choice Program, as provided in Section 401(3) of Chairman Rush's bill.

---

<sup>2</sup> For instance, we support the bill's recognition of context in the definition of "covered information." The bill rightly recognizes that whether a unique persistent identifier, such as an IP address, should be covered under the statute is dependent upon how the IP address is used and whether it can identify a specific individual.

#### IV. OECD Fair Information Practices

Intel supports federal legislation based on the Fair Information Practices (FIPs) as described in the 1980 Organization for Economic Co-operation and Development (OECD) Privacy Guidelines. The principles in these guidelines are as follows:

- 1) **Collection Limitation Principle** – There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge and consent of the data subject.
- 2) **Data Quality Principle** – Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
- 3) **Purpose Specification Principle** – The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- 4) **Use Limitation Principle** – Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with principle 3, above, except: (a) with the consent of the data subject, or (b) by the authority of law.
- 5) **Security Safeguards Principle** – Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
- 6) **Openness Principle** – There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- 7) **Individual Participation Principle** – An individual should have the right: (a) To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him or her; (b) To have communicated to him or her, data relating to him or her (i) Within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him or her; (c) To be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) To challenge data relating to him/her and, if the challenge is successful to have the data erased, rectified, completed or amended.
- 8) **Accountability Principle** – A data controller should be accountable for complying with measures which give effect to the principles stated above.

#### V. Applying the OECD Fair Information Practices to these Bills

Intel is strongly supportive of the overall framework in both of the bills, as they apply many of the OECD FIPs principles. For example, we are pleased that Chairman Boucher's discussion draft requires express affirmative consent for collecting or disclosing sensitive

information, requires reasonable procedures to assure the accuracy of covered information, and requires businesses to maintain the security of information. We are especially pleased that Chairman Rush's bill goes further and includes provisions applying all of the OECD FIPs, and we want to discuss five areas in particular.

First, we are pleased that BEST PRACTICES Act incorporates the Fair Information Practice of Individual Participation by including an explicit requirement of providing reasonable access to individuals to data that pertains to them (Section 202). Providing individuals access to data that relates to them is a necessary mechanism to building trust in the use of technology. We believe that the bill contains a reasonable approach that requires a covered entity to provide specific information (with a number of well-grounded exceptions) to individuals when the entity denies the individual a right, benefit, or privilege based upon the information. Yet when the covered entity does not deny the individual a right, benefit, or privilege, then a general notice or representative sample is all that is required. This middle-ground approach recognizes the realities of business operations, while at the same time providing strong consumer protections.<sup>3</sup>

Second, we are supportive of Chairman Rush's incorporation of the data minimization principle (Section 303). The large number of security breaches show us that the best way to mitigate the potential for harm to the individual is for the organization to minimize the amount of information it stores. Additionally, traditionally a data minimization provision is coupled with a collection limitation provision, which limits the amount of data to that which is necessary to fulfill the specified purpose of the data collection. We believe additional implementation of a collection limitation requirement should also be considered during discussions of the bill.

Third, we support the principle of purpose specification, which is included in Section 101(3) and (4) of the BEST PRACTICES Act. Purpose specification requires a business to look at the facts and circumstances through which the data is collected, and requires analyzing the collection from the perspective of why the individual believes he or she is providing the data. The OECD definition of Purpose Specification states that the purpose "should be specified not later than at the time of data collection." Given that privacy policies are only rarely read in detail by individuals, it is more appropriate to look to the context of the collection of the data to define the specified purpose. As smaller handheld computing devices are increasingly used over the next few years, it will be even more important to focus on the context of the collection, as the reading of lengthy privacy policies will be even more unlikely. Thus, we are also pleased that Section 102 mandates that notices must be "concise, meaningful, timely, prominent, and easy-to-understand" and that the section also takes into account that short notices may be appropriate, based upon such factors as the devices upon which notices are given.

---

<sup>3</sup> We are uncertain, however, whether it would be considered a denial of a "benefit" if a covered entity were to prohibit an individual from using a free web service based upon information that the entity possesses. However, such specific compliance questions like this could be addressed in rulemaking proceedings.

Fourth, we strongly support Chairman Rush's inclusion of the concept of accountability in Section 302 of the draft. Accountability is a well-established principle of data protection, having longstanding roots in many of the privacy and security components comprising global trust legislation.<sup>4</sup> Accountability requires an organization to make responsible, disciplined decisions regarding privacy and security. It shifts the focus from an obligation on the individual to have to understand complicated privacy notices to an organization's ability to demonstrate its capacity to achieve specified objectives. The accountable organization complies with applicable laws and then takes the further step of implementing a program ensuring the privacy and protection of data based on an assessment of risks to individuals. For example, companies can demonstrate accountability by innovating to build trust, such as by developing and selling more secure and privacy-enhancing component parts that have been vetted through processes such as development lifecycles that have privacy and security integrated as foundational elements. Intel and other like-minded companies are currently committing significant resources to "being accountable" in this way now, and we believe that the accountability provision is one of the more significant provisions in the draft.<sup>5</sup>

Finally, while some organizations may believe that the Fair Information Practices concepts do not provide them with great enough certainty to construct their compliance programs, we feel strongly that any bill must be focused on these high level principles and concepts so that it will stand the test of time in an environment where technology is rapidly evolving. And the bill's approach to allow the FTC to further define and enforce flexible requirements, while gaining the assistance of industry and consumer groups to best define enforcement guidance, is the correct approach.<sup>6</sup>

## VI. "Use and Obligations" Model

Intel is pleased that both bills have incorporated the concepts of "operational purpose" and "service provider" and have excluded uses in those definitions from the notice and consent

---

<sup>4</sup> Although the definitions of accountability vary, a good approximation of the accountability concept is the following: "Accountability is the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations. Accountability goes beyond responsibility by obligating an organization to be answerable for its actions". Center for Information Policy Leadership, submission for Galway conference convened with the OECD in Dublin, Ireland.

<sup>5</sup> We discuss in Section IX of the testimony how the concept of accountability can be incorporated into and further defined in a self-regulatory choice program.

<sup>6</sup> We would like to point out two additional provisions that might need further clarification as the legislative drafting process occurs. First, we have questions regarding the definition of "publicly available information" in Section 2(7). Under this provision, we are uncertain whether the phrase "widely distributed media" in Section 2(7)(A)(ii) would include information distributed on the Internet, including "covered information" posted by third parties. Second, we are uncertain about how an individual's revocation of consent in Section 103(c) would work in practice. That section does not state what obligations a covered entity has with regards to covered information once an individual executes a subsequent opt-out. Further, the section is silent as to a covered entity's obligations with regards to information already transferred to a third party under a covered entity's privacy policy. Operationally, it would be highly impractical to take any action regarding data already legally transferred to a third party; if the section is to contain any post opt-out obligations, it likely would have to apply only to subsequent uses by the collecting "covered entity" or transfers of data to third parties.

provisions. Intel supports what is known as a “use and obligations” model, which has been thoroughly explained in The Business Forum for Consumer Privacy’s paper entitled “A Use and Obligations Approach to Protecting Privacy,” *available at* [http://www.huntonfiles.com/files/webupload/CIPL\\_Use\\_and\\_Obligations\\_White\\_Paper.pdf](http://www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf). The “use and obligations” framework states that the way an organization *uses* data determines the steps it is *obligated* to take to provide transparency and choice to the consumer, to offer access and correction when appropriate, and to determine the appropriateness of the data — with respect to its quality, currency and integrity — for its anticipated use. The model notes five categories of data use where individuals implicitly give consent to the collecting entity and service providers based on the context of the provision of their data. These five categories of data use are: (1) fulfillment; (2) internal business operations; (3) marketing; (4) fraud prevention and authentication; and (5) external, national security and legal.

We believe that Chairman Rush’s “operational purpose” definition rightly covers these five categories of information and appropriately comes to the conclusion that neither notice nor choice are required for purposes such as processing a customer’s transaction, website analytics, fraud prevention, complying with a court order, etc. We slightly disagree with the bill’s approach on the use of data for marketing purposes, however.

The BEST PRACTICES Act excludes from the definition of “operational purpose” any data that is used for marketing or advertising (Section 2(5)(B)(i)). We believe, however, that notice and opt-out choice should not be not required for *all* marketing activities. Instead, we support The Business Forum for Consumer Privacy’s model that “just-in-time” notice must be provided if the marketing initiatives would *not be expected by the consumer*. For other marketing, companies must provide an easy-to-read, discoverable privacy policy. Because we believe that reasonable consumer expectations should be the controlling factor in deciding whether notice is required, we thus support the provision in Section 2(5)(B)(ii) that excludes from the definition of “operational purpose” the use of information that would not be expected by a consumer acting reasonably under the circumstances. We believe that this concept should be guiding for both clauses in Section 2(5)(B).

## VII. Privacy by Design

Over the past several years, regulators in multiple jurisdictions have called for more formalized and widespread adoption of the concept known as “Privacy by Design.” Privacy by Design asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must become an organization’s default mode of operation. The consensus view of these regulators – including the European Union’s Article 29 Working Party, the FTC, and the European Data Protection Supervisor – has been that the voluntary efforts of industry to implement Privacy by Design have been insufficient.

Although Intel is pleased that Section 302 of the BEST PRACTICES Act incorporates the principle of accountability (of which Privacy by Design is one form), we believe that Section 302 should specifically include a Privacy by Design provision as well. A Privacy by Design principle

should encourage the implementation of accountability processes in the development of technologies and services. To achieve its objective, the principle should avoid mandatory compliance to detailed standards, or mandatory third party detailed product reviews, as this would decrease time to market and increase product costs. This would be particularly the case when it is unclear whether third parties would have the appropriate resources or skill sets to effectively review the technology. Instead, a Privacy by Design accountability model should focus on making certain privacy is included as a foundational component of the product and service development process.

Intel views Privacy by Design as a necessary component of our accountability mechanisms that we implement in our product and service development processes. We would encourage the Subcommittee to include a provision in the bill specifically requiring that organizations ensure that privacy is included as a principle in product and service development processes.

#### VIII. Self-Regulatory Choice Program

Intel strongly supports Title IV of the BEST PRACTICES Act, which establishes a safe harbor for participation in a self-regulatory choice program. Intel has long been a supporter of privacy trust mark programs, and believes they should be fostered to provide mechanisms to work with organizations on their accountability processes. In the past, I have served on both the Steering Committee for BBBOnline, and on the Board of Directors of TRUSTe (on which I was Chair of the Board's Compliance Committee). Privacy trust marks, when provided with the benefit of a safe harbor through legislation, and when assisted by robust regulatory enforcement, can be the best mechanism to make certain that companies proactively put in place the organizations, systems, tools, policies, and processes necessary to proactively respect the privacy of individuals. We believe that in many instances, this co-regulation can be more effective than government or private enforcement alone, and we are pleased that the bill will incentivize businesses to participate in strong and robust programs.

We encourage the drafters, however, to specifically link the Accountability principle found in Section 302 back to Title IV's self-regulatory choice framework, and make explicit that participants in a self-regulatory choice program must incorporate accountability concepts into their requirements. Additionally, when the FTC is devising the criteria that must be present in self-regulatory programs in order to gain approval under the statute, we encourage the Commission to look to the work currently occurring between industry, think tanks, and government representatives that is further defining the elements of an accountable organization.<sup>7</sup>

Further, such Choice Programs will only be effective if individuals have knowledge of the opt-out provisions of Section 403(1)(A). We thus support the consumer and business education

---

<sup>7</sup> We would specifically direct the FTC's attention to the Center for Information Policy Leadership's Galway Project, mentioned above.

campaign required under Section 702 of the BEST PRACTICES Act. The FTC conducted a highly successful education campaign to promote the National Do Not Call Registry,<sup>8</sup> and we are pleased to see that a similar effort would be conducted with this bill.

IX. Conclusion

Intel again thanks Chairman Rush and the Subcommittee for the opportunity to engage in this debate. We are appreciative of the considerable thought that was put into both bills, which has allowed us to have this discussion today. In addition, Intel is supportive of moving forward with the BEST PRACTICES Act, and we look forward to continuing our engagement in helping to think about ways to improve the effectiveness of the U.S. legal framework and the overall protection of privacy.

---

<sup>8</sup> See [www.donotcall.gov](http://www.donotcall.gov).