



January 26, 2011

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

RE: FTC Staff Preliminary Report on Protecting Consumer Privacy - File No. P095416

Intel Corporation commends the staff of the Federal Trade Commission (FTC) for their outstanding work on the preliminary report on consumer privacy. We believe that the report will make valuable contributions to the ongoing debate about how best to protect consumer privacy; we especially note that the FTC's process for undertaking its review of privacy policy has been a model for transparency and the solicitation of stakeholder views. In response to the Commission's request for comments on the preliminary report, Intel would like to offer the following views.

I. The Computing Continuum

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'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 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.

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 (see Attachment A to this comment). 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 user'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 users 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.¹ Intel encourages the FTC to consider the future growth of the computing continuum when finalizing its report.

II. Need for Federal Privacy Legislation

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.² We encourage the final report to specifically advocate for the adoption of federal privacy legislation.

Intel is not working alone to make the innovations that would result from the development of a computing continuum 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. Intel strongly believes that comprehensive U.S. federal privacy legislation is a key mechanism for building this consumer trust in the Internet and ecommerce.

We disagree with the arguments some have advocated against the adoption of legislation, particularly that privacy legislation would stifle innovation and would hinder the growth of new technologies by small businesses. Instead, we believe that well-crafted legislation can actually enable small business e-commerce growth. For example, Intel has publicly supported legislation introduced in the 111th Congress, The BEST PRACTICES Act of 2010, H.R. 5777 (with the exception of the bill's proposed private right of action). We supported that legislation in part because it was technology neutral and gave 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

¹ 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," (attached to this comment as Attachment B).

² For example, Intel recently testified before Congress in favor of "The BEST PRACTICES Act of 2010." A copy of the written testimony is attached as Attachment C.

society, as the creation of legislative and regulatory requirements will invariably trail innovation of new technology. Technology neutrality also ensures that the regulatory environment does not favor an incumbent business model and can account for new business growth and innovation. Therefore, a focus on the application of principles -- neutral to the technology used -- enables a flexible, effective, and timely response.

Moreover, many of the issues present in a privacy regulatory scheme are highly contextual. Legislation can provide a baseline set of rules for all businesses while at the same time allowing for flexibility through the allowance of FTC rulemaking proceedings. Flexibility is critical so that legislation can continue to apply to the information necessary to create trust in the digital economy and can stand the test of time.³ Technology neutral and flexible legislation can actually aid small business growth as it provides a clear set of “rules of the road” for everyone, while at the same time allowing those rules to be adapted to each business’ unique situation. Under the current regulatory environment where there is no set of baseline protections, many small businesses are left floundering while attempting to figure out what consumers, the market, or regulators expect. We thus believe that federal privacy legislation can help all actors in the marketplace.

III. Adoption of the Full Set of Fair Information Practices

Intel strongly supports the FTC’s recognition that privacy regulation should encompass the full set of fair information practices. We believe this is one of the more significant aspects of the staff’s preliminary report. 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

³ In our 2010 testimony on privacy legislation, Intel stated that it supports FTC rulemaking that also provides specific criteria that the Commission should use in making its determinations. 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.”).

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.

We are pleased that the preliminary report recognizes that all of the FIPs are necessary to adequately protect consumer privacy. 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 federal legislation or privacy regulatory framework 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. Thus, we would like to address four aspects of the FIPs in particular: (1) accountability through privacy by design; (2) access; (3) data minimization and collection limitations; and (4) purpose specification.

A. Accountability Through Privacy by Design

As the staff report recognizes, 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 and the European Data Protection Supervisor – has been that the voluntary efforts of industry to implement Privacy by Design have been insufficient.

Intel is very supportive of the report's call for incorporation of Privacy by Design, which is one form of the Fair Information Practice of accountability. Accountability is a well-established principle of data protection, having longstanding roots in many of the privacy and security components comprising global trust legislation.⁴ 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 accountability is one of the more significant consumer protections.

The staff report correctly recognizes that 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 applaud the report's recognition that a privacy framework should specifically require that organizations ensure that privacy is included as a principle in product and service development processes.

B. Access

Intel supports the adoption of the Fair Information Practice of Individual Participation by including in legislation or a privacy framework an explicit requirement of providing reasonable access to individuals to data that pertains to them. Providing individuals access to data that relates to them is a necessary mechanism to building trust in the use of technology.

⁴ 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.

We recommend that in its final report, the FTC adopt the framework contained in The BEST PRACTICES Act. Section 202 of that bill provided 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 under the bill. This middle-ground approach recognizes the realities of business operations, while at the same time providing strong consumer protections.

C. Data Minimization and Collection Limitations

Intel supports the preliminary report's call for adoption of a principle of data minimization. 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 is also a necessary component of any privacy framework.

D. Purpose Specification

Intel also supports the principle of purpose specification. 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." As the report recognizes, 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 pleased with the report's call for notices that are concise, meaningful, and easy-to-understand. We also support the report's recognition that short notices may be appropriate, based upon such factors as the devices upon which notices are given.

IV. Other Provisions

In addition to these specific aspects of the Fair Information Practices, Intel would like to address five other items discussed in the staff's report: (1) the report's recognition of "commonly accepted practices" for which notice is not required; (2) self-regulatory programs; (3) the definitional scope of the proposed framework; (4) the need for greater consumer education; and (5) the report's endorsement of a browser-based "Do Not Track" system.

A. “Commonly Accepted Practices”

Intel is pleased that the staff report has recognized that there are some practices that are so “commonly accepted” that neither notice to consumers nor consumer choice is required for those actions. Intel has supported such a concept where certain “operational purposes” are excluded from normal notice and consent requirements. For instance, Intel has endorsed the “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.”⁵

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 the report’s examples of “commonly accepted practices” 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 report’s characterization on the use of data for marketing purposes, however. The report states that first-party marketing would be a commonly accepted practice, but that third-party marketing would not be. We believe, however, that the final report should more fully explore the concept of a third-party “service provider” that is contractually or technically bound to a first party to provide the same level of privacy protection.

Advertisers often operate within a complex network of business relationships and often share information with third parties for a variety of marketing operations. There are usually contracts governing that relationship that may require the third-party to provide the same treatment of data as the first party collecting that data; the first party may also put in place various technical measures that restrict the subsequent use of that data by additional third parties. Depending upon the treatment of the data via such contracts and technical means, the use of a consumer’s data by an advertising network might essentially be equivalent to the use of data by a “first-party” marketer. We recommend that the final report fully examine this aspect of the structure of the online advertising industry and reflect such service provider concepts in more detail.

⁵ This paper can be found at http://www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf

B. Self-Regulatory Programs

Although we advocate for privacy legislation, Intel also supports the preliminary report's recognition of the valuable role that industry self-regulatory programs can play in promoting consumer trust. 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. 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 favor legislation that will incentivize businesses to participate in strong and robust programs.

C. Definitional Scope of the Proposed Framework

Rather than contending that only "personally identifiable information" should be protected by the report's proposed framework, the staff report states that the framework should apply to all commercial entities that collect data that can be "reasonably linked to a specific consumer, computer, or other device."

Conceptually, Intel agrees that the framework should apply broadly to information that is reasonably likely to relate to an identifiable individual. However, Intel cautions against language that may apply to computers or devices that will not relate to an individual or a small group of individuals. 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.

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 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.

D. Need for Greater Consumer Education

Intel agrees with the report's position that strong consumer education is needed to better inform individuals about data practices and steps they can take to protect their information. The FTC conducted a highly successful education campaign to promote the National Do Not Call Registry, and we would encourage the Commission to conduct a similar effort on this issue. Moreover, we would call the Commission's attention to efforts surrounding Data Privacy Day, an annual international event to raise awareness and generate discussion about information privacy.

Over the past few years, privacy professionals, corporations, government officials and representatives, academics, and students in the United States, Canada, and 27 European countries have participated in a wide variety of privacy-focused events and educational initiatives in honor of Data Privacy Day. They have conducted discussions, examined materials and explored technologies in an effort to bring information privacy into our daily thoughts, conversations and actions. Data Privacy Day has also provided an opportunity to promote teen education and awareness about privacy challenges when using mobile devices, social networking sites and other online services. We would encourage greater U.S. government involvement in this event in order to raise privacy awareness and specifically encourage the government to partner with non-profits and industry to develop similar programs.

E. "Do Not Track" Mechanism

The preliminary report endorses the concept of "Do Not Track," which the report suggests would provide a more comprehensive method of providing consumer choice. The report states that the "most practical method" of providing uniform choice for online behavioral advertising would be through the placing of a persistent cookie on a consumer's browser. Although we agree with the concept of providing greater consumer choice, we think that comprehensive privacy legislation could better accomplish the goal of achieving greater consumer choice than a Do Not Track mechanism purportedly would provide. Further, the report's strong preference for a browser-based choice mechanism is too narrowly focused in light of the development of the computing continuum.

Although the privacy issues present in online behavioral advertising have garnered a great deal of attention in the current policy debate, we continue to believe that a baseline set of protections that apply to all actors and all sets of data is the preferred policy choice. We believe that the issues that would be presented by a Do Not Track system are the same types of issues that would be addressed by privacy legislation (What personal information is subject to its coverage?, What is meant by "tracking?", Would consumers have to ensure that each device that accesses the Internet recognizes their choice?, Are their preferences carried over?, etc.). Rather than sorting through these complex issues for only the subset of online behavioral advertising, policymakers should instead address these issues holistically to address the larger issue of trust for all data, both online and off.

Additionally, we think that the report's endorsement of a browser-based solution for providing consumer choice does not fully recognize the interaction of devices that is beginning to take place in the computing continuum. In the continuum, data will transfer from device to device as a person goes about their day. Most of these devices will not be accessing the Internet from a browser, but instead will be Internet-enabled through various software applications (apps) or with some other common interface that allows for personalization and contextual awareness to occur across devices. By endorsing a browser-based mechanism today, the Commission potentially locks in innovators to the current technology and does not provide businesses with the technology neutrality and flexibility that the Fair Information Practices otherwise provides. Rather than encouraging a browser-based mechanism for behavioral advertising (or suggesting that Do Not Track should be extended beyond the browser to apps or other non-browser connections), we instead believe that the Privacy by Design principle wholeheartedly endorsed by the report should be the guiding principle for protecting consumer privacy. That principle, which is flexible, technology neutral, and allows for adaptation to each particular circumstance and for the development of the computing continuum should be the final report's preferred approach.

V. Conclusion

Intel thanks the FTC for their outstanding work in soliciting a wide array of stakeholder views and issuing a seminal contribution to the privacy debate. We look forward to continuing our engagement with the Commission to improve the effectiveness of the U.S. legal framework and the overall protection of privacy.

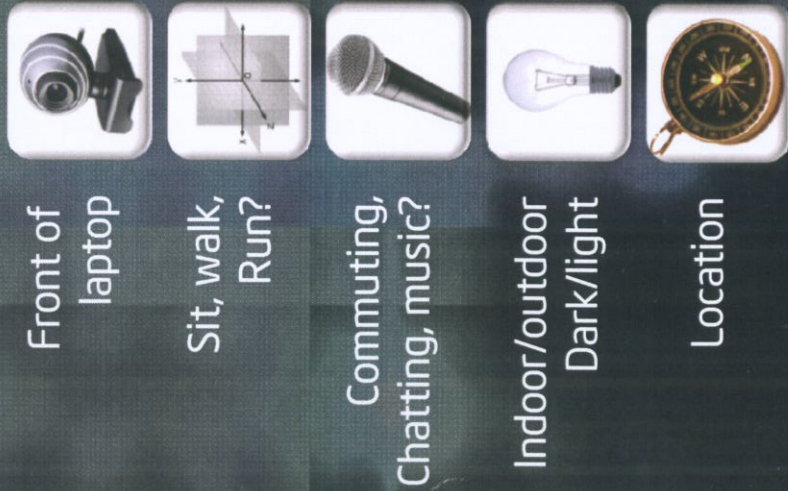
Respectfully Submitted,

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

Brian Huseman
Senior Policy Counsel
Intel Corporation

Smart services

Hard sensing



Context

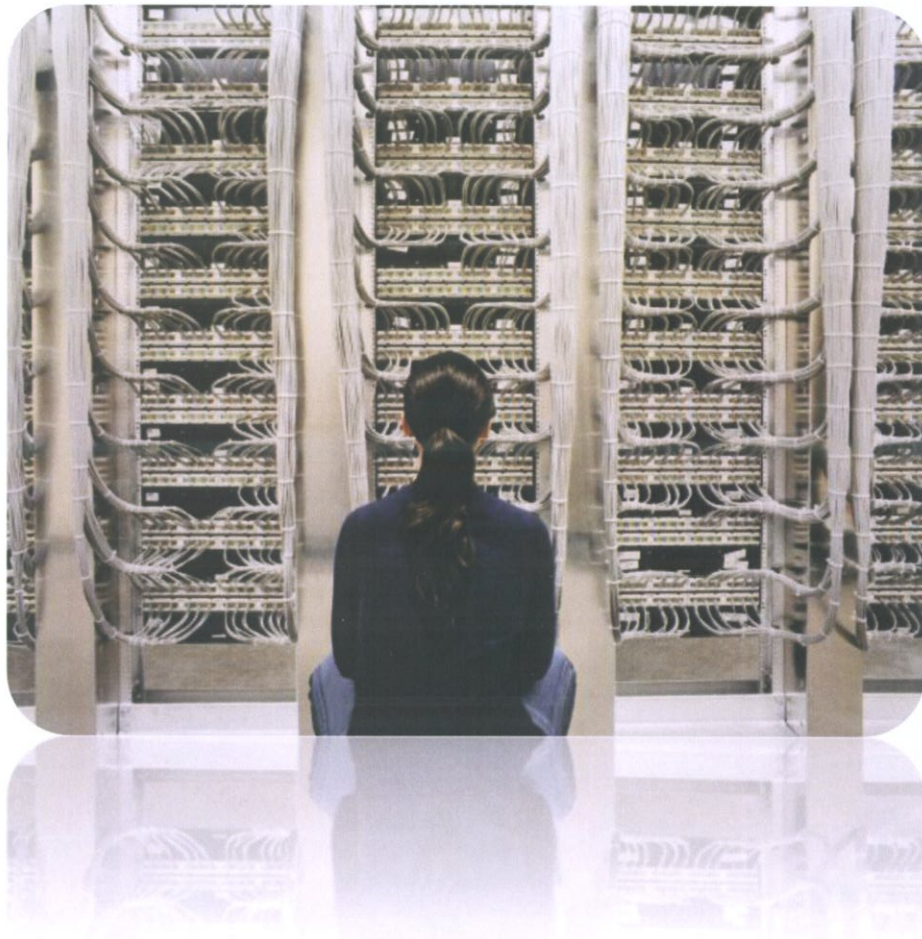
Soft sensing





Sponsoring Trust in Tomorrow's Technology: Towards a Global Digital Infrastructure Policy

By John Miller and David Hoffman



The information contained in this document represents the current view of Intel Corporation on the issues discussed as of the date of publication.

This document is for informational purposes only. INTEL MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

© 2010, Intel Corporation. All rights reserved. Intel, the Intel logo, Intel Sponsors of Tomorrow, and the Intel Sponsors of Tomorrow logo are either registered trademarks or trademarks of Intel Corporation in the United States and/or other countries.

**Other names and brands referenced herein may be claimed as the property of others.*

Contents

| | | |
|------|---|----|
| I. | Executive Summary | 1 |
| II. | Introduction | 2 |
| III. | Toward a Global Digital Infrastructure Policy | 3 |
| | a. GDI Components | 3 |
| | 1. Openness | 4 |
| | 2. Interoperability | 4 |
| | 3. Enabling Economic Growth | 4 |
| | b. GDI-POLICY Mechanisms | 5 |
| | 1. Triangle of Trust | 6 |
| | 2. Flexible Technology Neutral Laws and Regulations | 7 |
| | 3. International Cooperation and Global Standards | 9 |
| | 4. Accountability Systems | 11 |
| IV. | Intel's Accountability Model and Ecosystem Role | 14 |
| V. | Conclusion and Recommendations | 17 |

Case Studies and Additional Information

| | | |
|-----|--|----|
| 1. | Network Fragmentation Risks | 4 |
| 2. | Internet Policy | 5 |
| 3. | Cybersecurity R&D | 7 |
| 4. | Cryptography | 8 |
| 5. | Smart Grid..... | 9 |
| 6. | Government Procurement and Assurance | 10 |
| 7. | Cyber Crime/Cyber Attacks..... | 11 |
| 8. | Accountability & Galway Project | 12 |
| 9. | Privacy by Design & Accountability | 13 |
| 10. | Data Privacy Day | 16 |

Graphics/Charts

| | | |
|----|------------------------------------|----|
| A. | Triangle of Trust..... | 6 |
| B. | Secure Development Lifecycle..... | 12 |
| C. | SPP Team & Matrix Influencing..... | 15 |

AcknowledgementsAddendum

I. Executive Summary

In 2010, 6 million young scientists competed to show how they intend to invent the future. Intel's International Science and Engineering Fair (ISEF), the world's largest pre-college science competition, brought over 1600 finalists from 59 countries and regions to San Jose, California, to compete for over 4 million US dollars in prizes and scholarships.¹ The ISEF event helps demonstrate the global nature of technology innovation, and the tremendous value that can be gained by allowing the world's brightest young minds to work together. Many of the participants' projects were focused on Internet technology, at least in part because the Internet has become synonymous with innovation and global connectivity. Intel believes it is critical to foster continued Internet technology innovation, such as embodied by the ISEF, to continue to enable the world to make dramatic advancements rooted in the global connectivity provided by the network.

However, with all of the focus on the global nature of the Internet, an important development has been largely overlooked. The Internet is not only global, but predominantly operates via interoperable hardware and software products which are not varied significantly amongst individual countries and are deployed worldwide. These foundational information and communications technology (ICT) products make up a global digital infrastructure (GDI) that is the central nervous system of not only innovation, but economic development and social interaction. As reliance by individuals and businesses on the GDI increases, there is a corresponding increase in the value users place upon the security of the network and the protection of data traversing the network, including personal data that relates to identifiable individuals. Yet this need for trust in the security and privacy provided by the GDI is increasingly challenged by the rapid increase of malicious threats to the network and data. It is critical that the GDI continue to promote innovation of security and privacy measures at a pace equal to the development of these threats.

To help provide for the innovation of new security and privacy technologies needed to ensure that the GDI continues to thrive, another type of innovation is necessary: policy innovation and the development of a global digital infrastructure policy (GDI-Policy). A unified GDI-Policy informed by cross-border policy cooperation provides an opportunity to help nurture the GDI. This paper lays out the components that have driven the success of the GDI, describes the necessary mechanism of a GDI-Policy; and provides concrete recommendations to help achieve the GDI-Policy.

A successful GDI-Policy should build off of the following common components that have helped make the GDI ubiquitous and flourishing:

- openness²,
- interoperability, and
- enabled economic growth

The three components noted above point to the policy environment that is necessary for the GDI to continue to evolve and prosper. Our recommendation is that this policy environment should include the following mechanisms:

¹ <http://www.intel.com/education/isef/>

² In the context of this paper, openness refers to the ability for any individual to participate in the "network". The current design and nature of the Internet does not restrict who can access the network and thus it is "open" to participation from all.

- A 'Triangle of Trust' model,
- Flexible technology neutral laws and regulations,
- International cooperation and global standards, and
- Accountability systems.

We realize Intel cannot achieve this vision of a GDI-Policy alone. So we invite policymakers to join a constructive dialogue around the following specific recommendations which we believe will help make this policy vision a reality:

- Putting an end to import, export and use restrictions on cryptography for COTS and public research.
- Holding international discussions involving all stakeholders in the Triangle of Trust on the topic of decreasing cyber attacks, with the goal of reaching agreement on mechanisms for limiting the proliferation of such attacks.
- Increasing understanding and implementation of accountability practices amongst public and private sector organizations to an accepted global framework or standard, increased international government funding of NGOs as certifying agencies, and the development of robust, harmonized, coordinated and predictable enforcement mechanisms against noncompliant entities.
- Deepening government/private sector partnerships and international collaboration on cybersecurity research.
- Promoting the widespread adoption of a unified certification process and global standards for product assurance and product security to ensure a secure platform for the GDI. More specifically, we recommend improving the reliability and cost effectiveness of the Common Criteria evaluation and certification scheme by adopting a tiered approach to certifications (allowing companies to attest to compliance with an accepted global standard for certain levels of products, and for third parties to verify company attestations), expanding Common Criteria to development processes, and broadening the international mutual recognition of Common Criteria.

II. Introduction

New innovations in ICT come about every day, from all corners of the globe, and continue to drive the GDI into the future. Yet, this process is stalled and sometimes blocked by a confusing and often conflicting array of country specific laws and regulations. While technological innovation must continue at a rapid rate, a different type of innovation is necessary as policymakers grapple with the challenges of shepherding the GDI in the coming decades: policy innovation and the development of a global digital infrastructure policy (GDI-Policy). Indeed, this need to develop policies aimed at making the digital environment reliable and secure is becoming an important agenda item for governments and policymakers around the world as the Internet increasingly becomes an indispensable social medium and continues to foster economic growth. However, a siloed, country-specific regulatory approach may unintentionally disrupt a networked environment dependent upon global interoperability and connectivity.

Section III of this paper lays out in greater detail the GDI components, GDI-Policy mechanisms and the recommendations discussed above, and also provides several case studies and additional information to help illustrate GDI-Policy concepts, problems and solutions in practice. Section IV focuses on how Intel has implemented these concepts in our activities.

III. Toward a Global Digital Infrastructure Policy

a. GDI Components

Over the past decade, innovations in information and communications technology (ICT) have driven the growth of the publicly accessed Internet, and have become foundational tools directly affecting individuals' lives and impacting the functioning of virtually all businesses and government entities. The following components have made the GDI ubiquitous and successful and will be further impacted by where technology is headed:

- Openness,
- Interoperability³, and
- Enabled economic growth⁴

In the not so distant future, individuals will expect to have ubiquitous access to their data and applications, as provided by a variety of interoperable devices (e.g. PCs, Notebooks, Netbooks, MIDs, smart phones, home appliances, cars, etc.). Intel's vision is to enable the evolution of the GDI by innovating platform and technology advancements across the breadth of those devices, which will help tackle big problems such as education, energy/environment and health. As the use of the technology evolves, how innovations are implemented to meet the privacy and security expectations of individuals will also need to be fundamental components of the technology.

This future use of technology can be facilitated by open and voluntary technology standards, which enable fair competition, and further reduce product costs – benefitting consumers and driving trust across GDI technologies. Intel, given its role at the center of the GDI ecosystem, is uniquely positioned to integrate innovative security and privacy features into the core silicon building blocks laid at the foundation of both the commercial Internet communications infrastructure as well as a significant percentage of consumer and business client platforms.

Certain aspects of the current privacy and security policy structure, when examined globally, seem opposed to the optimal functioning of the GDI. Existing policies are often fragmented, uncoordinated, or geographically based. Each country sets its own rules and regulations in technology, privacy and security policy areas independently, and many countries lack developed privacy and information security laws and regulations entirely. With regard to privacy protection in the EU there is considerable multi-national coordination and intergovernmental cooperation to provide for a common market and the EU Data Protection Directive provides for a high level of accountability on corporate data processors operating in the region. However, even in the more cooperative European privacy environment there are

³ The ability of two or more systems or components to exchange information and to use the information that has been exchanged. (IEEE)

⁴ Example: in 2008, the OECD reported that "Over 1995 – 2006, growth in gross value added (GVA) was higher in the ICT sector than the whole business sector". <http://www.oecd.org/dataoecd/44/56/40827598.pdf> ; Page 25

examples of barriers created by non-harmonized regulation of the GDI. For example, the European Union registration and notification requirements vary widely between countries with little harmonization of process, creating inefficiencies that make demonstrating accountability even more difficult for corporations operating across the region.

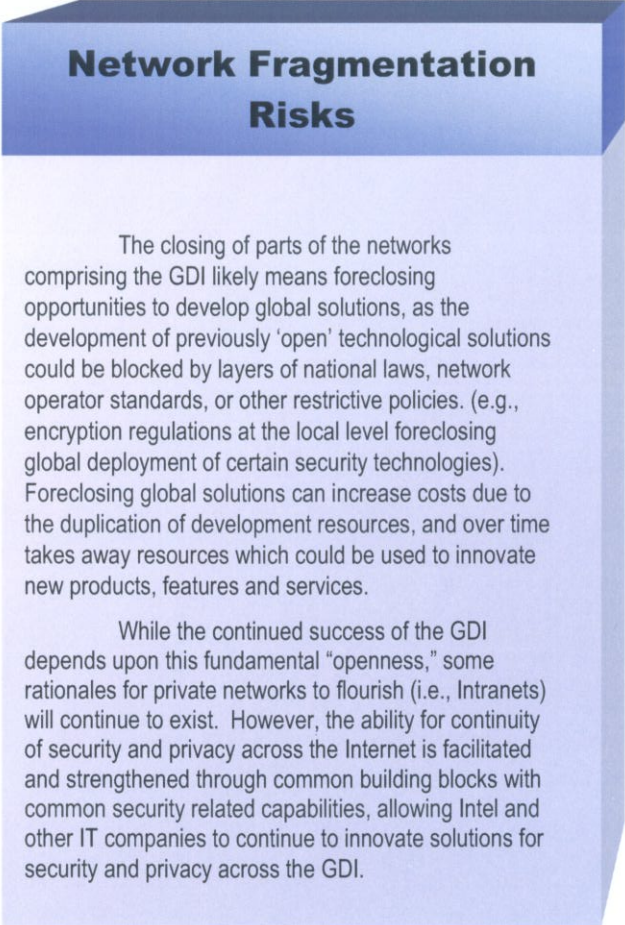
Such barriers create a need to examine in more detail the three components that have made the GDI successful: (1) maintaining openness; (2) maximizing interoperability; and (3) spurring economic development.

Openness. The GDI was built on a principle of “openness,” encouraging an environment marked by the free flow of data across borders, and an architecture allowing innovative new technologies and ideas to be launched globally. A major risk to the continued growth of the GDI is closing it off by allowing technology or network fragmentation, which can impede individuals from participating in the global network. This fragmentation can take many forms, such as segmented telecommunications networks, country specific filtering requirements and local standards. Rather than struggle to apply a regulatory scheme that is arguably inapposite to GDI telecommunications, governments around the globe should apply GDI-Policy principles such as technology neutrality and flexible laws and regulations which encourage openness.

Interoperability. An important benefit of the GDI is seamless operation of networks (or the network) irrespective of geographic borders. This interoperability has been enabled largely by global technical standards, yet the current policy environment is increasingly creating barriers to interoperability which threaten to undermine the benefits of these standards. For example, if security and authentication features based on international peer reviewed cryptography ciphers are not allowed in systems deployed in some countries, then global service providers may have great difficulty in enabling parties to adequately authenticate the trustworthiness of international transactions.

Driving adoption of a GDI-Policy helps avoid such interoperability innovation issues, allowing innovators to focus on meeting the needs of the entire GDI.

Enabled Economic Growth. 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



Network Fragmentation Risks

The closing of parts of the networks comprising the GDI likely means foreclosing opportunities to develop global solutions, as the development of previously 'open' technological solutions could be blocked by layers of national laws, network operator standards, or other restrictive policies. (e.g., encryption regulations at the local level foreclosing global deployment of certain security technologies). Foreclosing global solutions can increase costs due to the duplication of development resources, and over time takes away resources which could be used to innovate new products, features and services.

While the continued success of the GDI depends upon this fundamental “openness,” some rationales for private networks to flourish (i.e., Intranets) will continue to exist. However, the ability for continuity of security and privacy across the Internet is facilitated and strengthened through common building blocks with common security related capabilities, allowing Intel and other IT companies to continue to innovate solutions for security and privacy across the GDI.

access to the best available people, processes and technology, irrespective of country of origin, to continue the innovations necessary to drive the GDI, and remain competitive in the global marketplace. At the same time, in addition to these technical preconditions, building trust in the

Internet Policy

The need for reliable and scalable operations of the GDI suggests that effective private sector partnership with governments and other stakeholders can best achieve desired results. For example, the policy for allocating resources such as name space management and IP addresses has changed since the initial deployment of the Internet forty years ago. Additionally, the technology which provides for the mapping function between IP addresses and node names (DNS) has evolved. An examination of the current environment suggests the manner in which stable and reliable DNS operations have developed has benefited society by evolving policies that provide for accountability. Further, Internet governance is not monolithic - some current root DNS servers are operated by government or related agencies, some are operated by NGOs, and some are operated by the private sector (often in a supporting role to entities such as universities, research consortia, etc.).

Implementation of the GDI-Policy as articulated in this paper can help guide us through the current policy debates involving Internet governance. Security and stability are of the utmost importance to continued growth of the Internet, as these features in turn spur innovation and opportunity. Consistent, secure and predictable operation of the DNS is critical to ensuring the security and stability of the Internet, and the private sector is the best place to continue to provide for predictable operations and support of the DNS, while working within the Triangle of Trust to develop the best policies for implementing those operations.

GDI-Policy supports the principles of an open, autonomous, and fair Internet, and these principles can be equally applied to inform continuing debates over future governance of the Internet. Intel supports the current stable operation by ICANN, and continued private sector administration and management of the DNS.

digital economy is an essential component of driving the GDI forward. Building a trusted global environment in a systemic way not only benefits consumers and increases their trust in the use of GDI technologies, but is vital to the sustained expansion of the Internet and future ecommerce growth.

a. GDI-Policy Mechanisms

There is a growing recognition amongst policymakers worldwide that the legal and regulatory status quo in the areas of privacy and information security does not provide adequate levels of trust to sustain the GDI.⁵ While change seems inevitable due to increasing concerns surrounding cybersecurity, critical infrastructure protection, encryption, and other emerging policy issues, the question is which one of two divergent paths the change will follow:

(1) Individual countries increasingly and in isolation

pass laws endeavoring to 'regulate' different aspects of the GDI; or

(2) Multi-jurisdictional and transborder efforts gain significant traction, leading to some form of extra- or intergovernmental coordination between and cooperation amongst states in the management of the GDI.

⁵ Some examples include:

- Rockefeller/Snow Cybersecurity Act of 2009 (S. 773) – see “findings”
- The EU is currently revisiting Directive 95/46/EC in an effort to make it more adequately address 21st century privacy challenges.
- Country specific security assurance certifications exist around the world (e.g., UK, Russia, China)

The nature of the GDI encourages us to choose the path centered around policy structures and processes that are similarly global in scope and rooted in innovative thinking. The common elements of current and contemplated privacy and security laws and regulations can help inform the nuanced requirements of how these GDI-Policy structures take shape.

Navigating the increasingly confusing and non-harmonized patchwork of global legislation with respect to privacy and security to extract elements common across cultures presents challenges. There are efforts to harmonize around central standards or legislative approaches (the EU 95/46 Directive is a useful example). However, there will always be situations where individual countries' unique historical, political, socio-economic or religious environments necessitate specific approaches to the protection of personal data or how security can best be achieved. These unique culture-specific environments also shape the expectations of citizens as to how their rights will be respected by those who collect and process information that pertains to them.

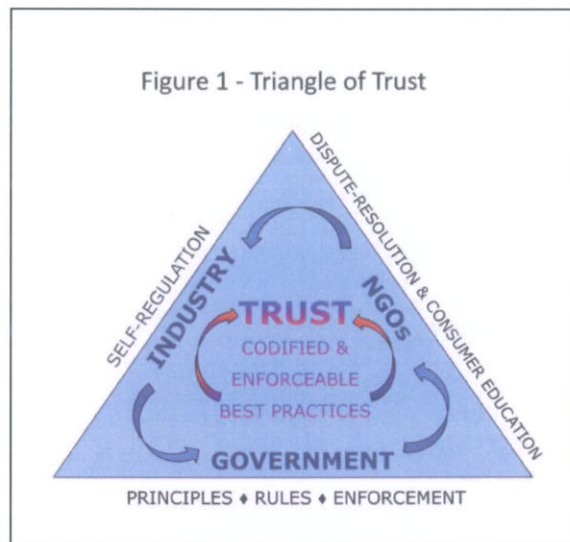
Due to the difficulty in creating a global program out of such a patchwork, one useful approach is to continue to look to the high level principles which have gained broad acceptance (albeit to different extents in varying jurisdictions) over the past 40 years, and to how those principles have been applied in some of the major privacy and security legal and policy efforts around the globe.

While certain novel transborder processes and structures may be needed to help implement a GDI-Policy vision, an examination of the current legislative and regulatory environment in privacy and security reveals certain mechanisms which can provide the foundation for a more productive policy environment:

1. Public-Private-NGO Partnerships:

The Triangle of Trust. No single entity can achieve the goal of building trust in the GDI; it is clearly a shared responsibility. At Intel we recognize the role of governments, industry, and Non-Governmental Organizations/advocacy groups (NGOs) working together to form a “triangle of trust.” (See Figure 1.)

- Government should establish the “base” of the Triangle by creating high level compliance principles and rules, and by conducting robust, predictable and harmonized enforcement.
- Industry comprises one of the “sides,” working with government to propose best practices which can allow companies to comply with laws and regulations.
- NGOs form the final “side,” assisting both government and industry to codify industry best practices, handle dispute resolution to free up scarce government enforcement resources for more pressing issues, and to help educate individuals and privacy/information security professionals.



Cybersecurity R&D

Government funding for cyber security research is increasing, as it has been noted as a priority in many countries. However, to date much of government funding for cyber security research has been done using methods that frustrate international and government-industry collaboration. For example, many funding models prohibit citizens of other countries from participating in the research. Also, some models create intellectual property restrictions which discourage industry collaboration. Governments should look to existing models that have created successful international industry-government-academic collaborations in research.

The private sector is poised to be a helpful partner to governments as they build out a GDI-Policy. Governments and industry should work together to develop a policy and regulatory environment informed by the principles of openness, fairness, and flexibility. For there to be “predictable enforcement” of “flexible technology neutral laws and regulations”, robust context specific implementation guidance is necessary. Industry best practices can play an important role in developing this enforcement guidance. NGOs can play an important convening role to help document this enforcement guidance. Finally, NGOs can help alleviate overburdened government resources by providing services for the external validation and certification of company programs/practices. To accomplish this goal, government and industry should work

together to promote NGOs as indispensable trusted partners in the efficient and trustworthy functioning of the GDI.

2. Flexible Technology Neutral Laws and Regulations. Sensible regulation of the GDI need not require the creation of new principles. Ample flexibility exists in many current laws, principles and regulations dealing with aspects of data protection, privacy and security.

For example, the OECD Guidelines on the Protection of Privacy and Transborder Data Flows contain a Security Safeguards Principle stating, “Personal data should be protected by reasonable security safeguards.”⁶ The EU Data Protection Directive contains a similarly flexible Article regarding security, providing Data Controllers “must implement appropriate technical and organizational measures to protect personal data ...” and should consider “the state of the art and the cost” of security measures.⁷ While the U.S. takes a sectoral approach to privacy and information security law, ultimately the approach taken with respect to information security has proven similarly flexible, at least in the sense that U.S. laws in this area are generally not proscriptive.⁸

A common historical thread regarding information security running through the EU Data Protection Directive, OECD guidelines, and U.S. privacy law is the absence of detailed regulations which would mandate or otherwise compel adoption of any one specific technology. This technology neutral approach to regulation allows engineers to do what they do best: solve problems. By describing neutral principles and objectives, global innovators can collaborate on the best way to implement solutions.

⁶ OECD Guidelines, Security Safeguards Principle, No. 5.

⁷ EU Directive 95/46/EC, Art. 17(1).

⁸ It should be noted there are exceptions in the U.S., such as the extension of CALEA, a 1994 law requiring telephone companies to design their networks to make them easy for law enforcement to tap into the internet.

We can look both to past efforts such as the key escrow scheme considered by the U.S. in the 1990s⁹ and ongoing regulatory efforts in the encryption area in a number of jurisdictions to provide further support for this concept. Currently, encryption laws and regulations in the U.S., China, Russia and other countries variously impose regulations ranging from limited export controls to import authorization/declaration requirements for ICT products with cryptographic technology to restrictions on distribution, sales and use of such products (including R&D and manufacturing in some cases).¹⁰ Some of these regulations have the impact of requiring the adoption of certain country specific standards and technologies, which run the risk of mandating a particular technology as the innovation that must be deployed. Even the application of more limited encryption export controls by the US is increasingly creating burdens and supply chain instabilities, since the substantial liberalization of the controls a decade ago are now being outpaced by the pervasiveness of encryption capability in ICT products. Such

Cryptography

The use of encryption technologies is already pervasive in COTS software products such as web browsers and email programs, and increasingly in hardware products (e.g., components with cryptographic capability) requiring security solutions to mitigate attacks and vulnerabilities compromising computers and network integrity. When one considers cryptography is also a key enabler of secure Internet-based commercial transactions (e.g., financial and banking transactions), it is clear the need for mass market encryption products will continue to grow in the global digital processing age. The mass deployment of new technologies, including portable and wireless computing devices that transfer and store an ever-increasing amount of digital data, is further accelerating the need for encryption-based security technologies in both software and hardware.

Building the trust in the digital economy vital to the sustained expansion of the GDI and future ecommerce growth requires continued development of technologies making use of robust cryptography. And yet, several nations seem committed to controlling cryptography, ostensibly to increase security. (e.g., the US, China and Russia).

Intel and others in industry are leading efforts to improve such potentially counterproductive regulatory efforts by continuing to focus on providing strong encryption and thus robust security, and promoting the reasonable use of cryptography as a key enabler in developing the security technologies that currently protect the GDI. The industry perspective is we can best mitigate the security risks threatening economic growth with robust, peer reviewed, public encryption ciphers and internationally inter-operable cryptography standards. This technology neutral approach (achieved through peer review and similar processes) provides the strongest cryptography and the best security and privacy, and also points out why standards-based encryption rather than proprietary encryption is not only more secure, but facilitates international interoperability and standards, while avoiding the mistakes of the past.

⁹ This scheme largely revolved around conditioning encryption export control liberalization on a requirement to build capability into products permitting law enforcement access to the plaintext of encrypted information. The approach began with a Clipper Chip program requiring escrow of decryption keys with relevant government agencies, a model that later evolved into a key recovery approach allowing for self-escrow in many cases. However, this policy proved technologically infeasible, socially controversial and procedurally unworkable. The debate around the program led to the conclusion that a key escrow scheme would introduce a security weakness into GDI products as opposed to enabling innovators to develop increasingly secure products with a focus on allowing the best experts around the world to test open algorithms for flaws. The resulting regulatory approach has largely been technologically neutral and market driven. This approach unleashed security-related innovation and, more broadly, helped to foster economic growth, promoted the health of the digital economy, and improved the competitive advantage of U.S. companies – all without sacrificing the security of the cyberspace infrastructure. This regulatory approach has largely stayed in place for approximately twenty years, and only now needs focused US attention to make certain its technology neutral and market driven aspects continue to apply to COTS that are increasingly integrating more powerful cryptography.

¹⁰ See, e.g., Regulations on the Administration of Commercial Cipher Codes, promulgated and effective as of October 7, 1999, Provisions on the Administration of Production of Commercial Cipher Products, promulgated, and effective as of January 1, 2006, and Provisions on the Administration of Commercial Cipher Research, promulgated, and effective as of January 1, 2006.

proscriptive technology focused regulations are forcing companies like Intel and its customers to attempt to preserve the ability to functionally disable (fuse off) innovative security technologies in products sold in some countries. If not for these regulations, these security enhancing features would be deployed globally. Fusing off this technology creates portions of the GDI that operate in a less secure environment and over time will frustrate interoperability and international transactions, as well as creating manufacturing inefficiencies that could hinder

Smart Grid

Currently enacted cybersecurity legislation in China (e.g., MLPS), and contemplated regulation in the U.S. and elsewhere shares the common goal of securing the critical infrastructure from cyber threats. Although there is not a common definition of the “critical infrastructure” (CI), as a high-level principle, promoting measures aimed at protecting the most critical elements of the global digital infrastructure should be a component of GDI-Policy. At a finer level of granularity, we can identify commonalities across proposed definitions, and conclude that most definitions of the critical infrastructure must include the power, water, national security, information and finance sectors.

While each country shares a common goal of securing these sectors, many have different ideas of how best to do so. Unfortunately, several countries appear to favor the creation of national standards which may function as barriers to the use of technology developed or manufactured abroad, even while many are at the same time looking to modernize their uses of technology. Efforts by multiple governments to develop “smart grid” technology provide an illustrative example. To achieve scale, drive down cost, and gain the benefit of the best innovators in the world collaborating to produce the most innovative solutions for the smart grid, it is crucial that countries do not impose divergent or conflicting regulations on smart grid technology. Yet at the same time, all governments will want to ensure that individuals receive and use power in their homes with the most robust security and privacy protections possible. Incentivizing technology developers and implementers to develop solutions based on global principles common across many divergent cultures is the best means to achieve this goal.

innovation. GDI-Policy solutions should encourage technical innovation, collaboration and openness rather than proscriptive security measures or the imposition of standards which require the adoption of a particular technology.

3. International Cooperation and Global Standards. Just as the GDI itself is a network of networks – and requires hardware and software working together to create a trusted stack – governments must work together to create a networked regulatory framework – a policy and legal infrastructure which promotes continued innovation and enabled economic growth. In developing solutions to the privacy and security problems threatening the GDI, we should avoid creating geographically siloed regulations that may impede the global interoperability and network connectivity that have spurred the growth of the GDI. Governments would also be well-advised to avoid taking confrontational action which may provoke country specific regulation. While some coordinated efforts have been carried out such as the effort led by the Spanish Data Protection Agency (which resulted in the Joint Proposal for a Draft of International Standards with regard to the processing of Personal

Data),¹¹ and the Council of Europe’s Convention on Cybercrime,¹² additional efforts are needed as more policymakers at various other national governments continue to draft legislation, in areas such as cybersecurity, with little to no attention paid to cross-border realities.

¹¹ http://www.privacyconference2009.org/dpas_space/Resolucion/index-iden-idphp.php

¹² <http://conventions.coe.int/treaty/en/treaties/html/185.htm>

Technology and policy collaboration across borders is attainable if nations honor one another's cultural traditions, and focus on conditions common across cultural boundaries, such as demonstrated by the APEC Data Privacy Pathfinder Project, and on principles calling for designing privacy into products, services and business processes.¹³ Designing in privacy includes a flexible set of principles allowing for technology companies to honor local traditions, while developing innovations which not only attempt to solve problems in the common conditions we share, but to do so while improving the privacy of all individuals. A similar approach is visible in efforts to articulate how to design security into products, services and business processes, for instance through the use of a secure development lifecycle. Security assurance - or the process by which we drive robust security into computer systems, hardware and software - is a critical requirement for addressing vulnerabilities and improving computer security, as well as being vitally important to critical infrastructure protection. Intel and our industry partners are engaged in a number of standards efforts designed to increase security assurance. For example, there is great potential value in multi-lateral certifications for security such as Common Criteria. GDI-Policy efforts should focus on how we can improve the reliability and cost effectiveness of these processes while at the same time promoting them to better provide increased security.

Global standards provide a primary means by which we can encourage and give force to intergovernmental cooperation. As we survey the global standards landscape, it is clear GDI-related standards can play an increasingly prominent role, particularly in developing security policy areas such as security assurance, as an alternative to uncoordinated recent major legislative efforts in the US, China and elsewhere.

Government Procurement & Assurance

One method by which governments are looking to better secure the critical infrastructure is to use government procurement regulations to improve the assurance level of hardware and software. Industry plays a critical role in increasing the measurable assurance level of the GDI. Assurance concerns are generally of three types: **(1) Supply Assurance** (Governments are concerned about whether they will have adequate access to the technology they need); **(2) Functionality Assurance** (Governments are concerned by the number of errata and security updates needed for COTS and software); **(3) Security Assurance** (Governments are concerned about whether individuals may be able to intentionally place security compromises in hardware and software).

While these assurance concerns are legitimate, the direction in which governments appear headed to try to solve them may do more harm than good. For instance, government initiatives to try to 'guarantee' better assurance by passing restrictive government procurement guidelines for purchasing hardware or software, or local technology certification guidelines or similar measures, may effectively weaken government systems themselves by splitting them off from the COTS products driving the GDI as a whole. Indeed, COTS products are more likely to contain the security and privacy technology measures demanded by the marketplace, and that innovative companies have been incentivized to create.

Furthering the adoption of global security standards such as Common Criteria provides a productive mechanism by which governments may address their assurance concerns. Intel is currently participating in efforts to revitalize Common Criteria. If industry is successful in demonstrating accountability by consistently providing reasonable assurance, and demonstrating the robustness of our products and manufacturing processes, innovative companies will be emboldened to invest development resources in creating security features for the global market, thereby increasing the overall security of the GDI in a cost effective manner.

¹³ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf

Cyber Crime ~ Cyber Attacks

The well-publicized increasing militarization of cyberspace and the growing threat of alleged state-sponsored, endorsed, or affiliated cyber attacks against other governments and multinational corporations underscore the need for international collaboration. Cyber security incidents have resulted in corporations, governments, and NGOs coming together to scope the severity of the threats and to coordinate responses. However, these efforts have all too often resulted in more finger-pointing over the purported political motivations for state sponsorship of the attacks than credible attempts at solving the underlying problem. This is an example of where all stakeholders would be better served working to find international methods to (1) develop a system of globally harmonized cybercrime laws; (2) share information to find the malicious actors responsible for the attacks; (3) use cross-border cooperation by law enforcement to apprehend those responsible, (4) punish them in accordance with globally harmonized enforcement principles, (5) collaborate on codifying best practices to eliminate the security weaknesses seized on to enable the attacks in the first place, and (6) deploy new technologies based on global standards which will increase the security robustness of the GDI.

4. Accountability Systems. Private sector companies should work together with all stakeholders - governments, NGOs, and users themselves - in creating and increasing trust. The primary means by which they can do so is by demonstrating accountability, both internal to their organization and to external stakeholders.

Accountability is a well-established principle of data protection, having longstanding roots in many of the privacy and security components comprising global trust legislation.¹⁴ Though definitions of what is meant by “accountability” vary across these instruments, a useful approximation 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.¹⁵

But what does accountability mean in practice? We believe that a variety of accountability models can exist for different aspects of privacy and security but in general, such models are comprised of the following elements: 1) commitments which are interpreted from flexible and technology neutral laws, industry best practices and entity specific promises; 2) processes and procedures put in place to deliver on the commitments; 3) attestation by the entity demonstrating how it has fulfilled its commitments; 4) third party mechanisms (either regulators, certification authorities or NGOs) for measuring whether the commitments have been met. Although the focus of such accountability systems seems squarely on corporations, there are clear roles for the government and NGO “sides” of the Triangle of Trust to play here as

¹⁴

The accountability principle is included in:

- Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines)
- Asia Pacific Economic Cooperation Privacy Framework (APEC Privacy Framework)
- The European Union’s Directive on the Protection of Personal Data
- Canadian private-sector privacy law: The Personal Information Protection and Electronic Documents Act (PIPEDA), and
- The Safeguards Rule of the Financial Services Modernization Act of 1999, commonly referred to as the Gramm Leach Bliley Act.

¹⁵

Center for Information Policy Leadership, submission for Galway conference convened with the OECD in Dublin, Ireland.

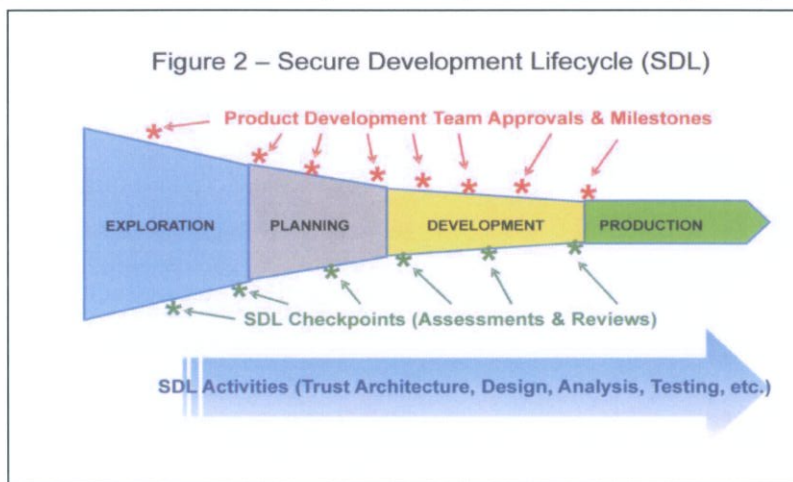
well. For example, robust, harmonized and predictable enforcement by regulators is critical to lend credibility to any accountability system, as citizens and regulators should not accept any system that relies on industry representations of accountability alone. All entities comprising the GDI have a need to show they are accountable. Such accountability must go beyond how organizations process personal data, and extend to their security measures and how they develop products, programs and services.

Demonstrating accountability internally

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 into the GDI that have been vetted through processes such as development lifecycles which have privacy and security integrated as

Accountability & The Galway Project

The Galway Project, an increasingly recognized effort to push accountability beyond the principle phase, crisply articulates how this concept might best be demonstrated or measured. As per the Galway guidance, “an accountable organization demonstrates commitment to accountability, implements data privacy policies linked to recognized external criteria, and implements mechanisms to ensure responsible decision-making about the management and protection of data.” The essential elements of such an accountability system as proffered by the Galway Project are: 1 – *Organizational commitment* to accountability and adoption of internal policies consistent with external criteria (as demonstrated via an organization’s structures, processes, etc.); 2- *Mechanisms* to put privacy policies into effect, including tools, training and education; 3 –*Systems for* internal, ongoing oversight and assurance reviews and *external verification* (including assessments by privacy enforcement or third-party accountability agents); 4- *Transparency* and mechanisms for individual participation (beyond mere privacy notices) 5- Means for *remediation and external enforcement* (acknowledged as ultimately resting with local legal authorities). (See CIPL Galway Paper, cited at fn. 15).



foundational elements.¹⁶ Intel and other like-minded companies are currently committing significant resources to “being accountable” in this way now. But industry must do more, in a systemic and systematic way, to demonstrate accountability processes, than to simply say, “Trust us – we’re accountable.” Adoption and implementation of a “privacy by design”¹⁷ process

¹⁶ See, *infra*, discussion of SDL at section IV. See also Figure 2 above.

¹⁷ Privacy by Design ... Take the Challenge, by Ann Cavoukian, 2009.

and integrating security into the development lifecycle are two mechanisms by which companies can demonstrate accountability in the development of technologies to regulators and policymakers, who have been actively debating this concept.

Demonstrating accountability externally

Demonstrating accountability externally is therefore equally important and arguably more challenging for corporations and governments alike. Ultimately, regulators are responsible for ensuring that risks have been managed appropriately. This responsibility is why regulators are unlikely to simply defer to industry best practices in this area, but instead should play a role in commenting on global best practices and then in using them as enforcement guidance. Yet due to resource constraints and other factors, governments will still need additional mechanisms to enforce accountability. Third party certification is one such additional mechanism that has been used previously in the areas of privacy and security.

However, third party certification may be counter-productive, if it:

(a) is so detailed that it slows the ability of innovators to be able to get products/services/programs to market, or

(b) requires the certifying entity to have such detailed knowledge of the product or business processes that such certifying entity would not be able to acquire the right content expertise in a cost effective way to cover the great variety of participants in the GDI; or

(c) uses siloed geographic certifications without mutual recognition.

This is why third party certification mechanisms need to comprehend the processes by which an organization is ensuring it is accountable, including processes which check for common problems that may lead to a lack of trust (e.g. checking software code for known vulnerabilities or checking to make certain access controls are set appropriately). Some of this verification can be done by the organization itself, which can then subject itself to the authority of third parties for enforcement and dispute resolution (e.g. similar to the way corporate officers annually attest to compliance with the EU – US data transfer safe harbor principles). The key is that to accomplish the needs of the GDI, these attestations or certifications must be to globally recognized principles or best practices. Governments should begin work to help foster the development of such certification organizations, including providing public funding to underwrite such efforts.

Privacy by Design & Accountability

Over the past several years, regulators in multiple jurisdictions have called for more formalized and widespread adoption of Privacy by Design. The consensus view of these regulators – including the Art. 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. (See, e.g., FTC Commissioner Harbour's speech at the last FTC Roundtable.) Intel believes that a Privacy By Design principle should encourage the implementation of accountability processes in the development of technologies. 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.

IV. Intel's Accountability Model and Ecosystem Role

Intel has long been at the center of the growth of the GDI, and takes seriously its role as a provider of building blocks for the digital infrastructure. Increasingly, Intel is working to ingrain the responsibility to build a reliable and trusted environment into our internal policies and practices. Yet building trust in technology is a complex challenge. We look to the various elements associated with trust and ensure we are making advances in all of them, as privacy or security breaches can have serious long-term effects on the individual. Put another way, Intel is putting accountability into practice, by building out layered internal accountability systems.

a. Internal Accountability Structures

Intel is investing in solutions to the difficult challenge of building trust directly into platforms, whether it's a PC, Server, smart phone, or networking equipment. Trusted hardware is the foundation upon which the market will build trusted operating systems, applications, networks, and services.

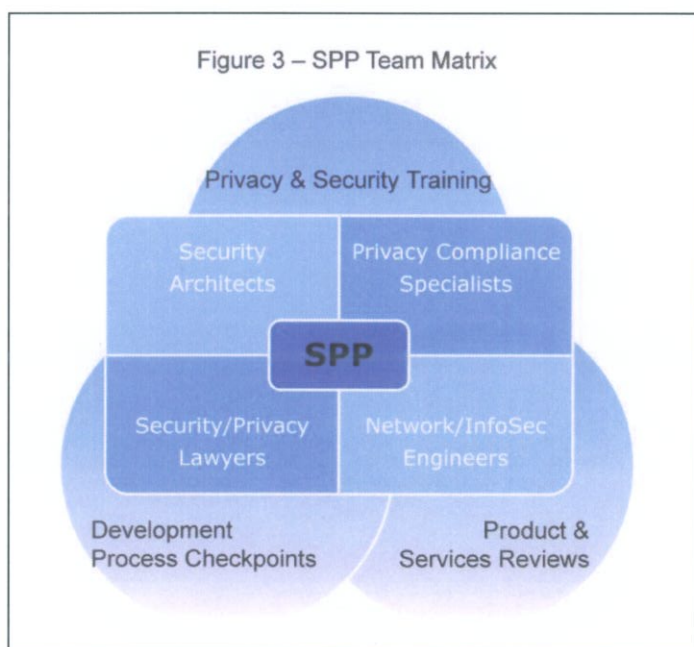
Trust Innovation. Building trust via designing in privacy and security is now an integral part of Intel's entire innovation pipeline, from concept to product. We are actively engaging with "white hat" communities, striving to stay one step ahead of an escalating threat model, and doing fundamental research on novel trust mechanisms. Increasingly we are introducing new hardware based cryptographic mechanisms that can protect data through secure bus structures, secure memory, secure application execution environments such as trusted virtualization, and secure I/O to protect against attacks such as keyboard logging.

Intel is committed to the fundamental human right of privacy and providing robust security, and so it takes seriously its role in developing technologies which help to ensure the protection of data. Intel's goal in this area is to minimize potential threats to data in order to develop a sufficient level of trust in digital devices to enable innovation and economic growth. At the same time, malicious actors are constantly introducing new threats that put this data at risk. Intel focuses on bringing together the brightest minds globally to tackle this difficult problem to help ensure the rate of security innovation keeps pace with developing threats. Some of these brightest minds work in the government, which is just one of many reasons Intel works with multiple governments to increase the security robustness of our products. Yet some government entities have expressed concern that higher levels of security in products may make it more difficult for law enforcement to acquire access to information necessary to accomplish critical law enforcement missions. Intel respects these law enforcement mission needs, and believes sound GDI-Policy should take into account that provisions allowing governments to gain access to the data they need via robust lawful due process mechanisms will continue to be necessary. However, Intel does not believe law enforcement is well served by introducing security weaknesses into hardware and software products as a further mechanism by which to access such data.

Trust Policy. Intel has developed a comprehensive set of processes, tools, and policies to provide security and privacy. To better demonstrate accountability on a policy level, Intel has created organizational structures focused on bringing security and privacy expertise to individual product reviews, including the Security and Privacy Policy (SPP) organization. (See Figure 3). SPP has established a structure and processes which can draw upon hardware security

architects, network and information security engineers, privacy compliance specialists and security/privacy lawyers:

- SPP has built several internal processes to facilitate this focus on security and privacy - as an example, Intel employees are required to complete both privacy and security related training tailored to their job positions, and which complements employees' familiarity with processes they use every day.
- SPP has also instituted several steps in the development of each Intel product to ensure the company is not only building great security products, but that these products enhance user privacy.
- Out of this development process, SPP creates project teams to review individual products, programs or services. In these reviews, SPP looks at how personal data is collected and processed, unique platform identifiers and their linkage to personal data, and how remote privileges are managed.



Security Assurance in Development and Manufacturing.

Product complexity and platformization¹⁸ add new challenges for Intel and its customers. To better demonstrate development and manufacturing accountability, Intel is increasingly focused on security assurance and has undertaken significant initiatives aimed at increasing security assurance processes across the company, including establishing the Security Center for Excellence (SeCoE). One SeCoE-led initiative is “Design for Security,” which is focused on building a capability in each and every engineering team to develop secure products. A central aspect of this

initiative is educating engineers to design for security and privacy. Another example is the Intel Secure Development Lifecycle, which defines the actions, deliverables and checkpoints a project team follows to engineer in security/privacy and then assure we meet the expectations of the product and market.

a. External Trust Policy Efforts

Externally, Intel has already taken numerous actions to support development of a GDI-Policy.

¹⁸ 'Platformization' is the combination or bundling of standard hardware and software technologies, capabilities, services and tools in an integrated product.

Trusted Government Partnership. Intel has made significant efforts on global technology public policy by acting as a trusted advisor to governments on a number of different topics, and is expanding these relationships in emerging areas such as security assurance.

For example, governments around the world are increasingly concerned with Critical Infrastructure Protection (CIP) issues, and they regularly call on Intel to discuss these issues. Intel also partners with governments to share information and data regarding threats to the security of the GDI and the critical infrastructure, and helps government organizations develop better processes with respect to internal information security processes.

Industry Cooperation and Coordination. As a leading global ICT company, Intel is helping build the GDI-Policy by coordinating with other industry leaders and facilitating discussions and cooperation with and amongst governments – this is an example of how we are working to encourage the development of the Triangle of Trust.

Intel has been particularly active in external policy efforts concerning security assurance, not only to address growing government concerns regarding global supply chain security, but by participating with other leaders in the field to promote security assurance processes and awareness, and by helping to drive our industry partners to invest in security assurance.

Additionally, peer review and academic research are playing more important roles in security assurance processes – Intel along with others in industry increasingly share technologies with universities, researchers, and other peers, affirming the principle that openness is the preferred way to test security. Intel is also taking a leadership role in the important area of trust verification. Specifically, Intel has been working with others in industry as well as the certification labs in an attempt to improve the current common criteria certification scheme, to make sure it addresses the concerns various governments have expressed in currently proposed regulations, while addressing the concerns of industry to make certification more timely and cost-efficient.

Education and Outreach Leadership. As mentioned above, one of the mechanisms needed to give life to the concept of accountability is

Data Privacy Day

First celebrated in 2007, Data Privacy Day is an international event founded to spread awareness about privacy and data protection. Data Privacy Day is aimed at educating the individuals most impacted by the security and privacy issues raised by the GDI (e.g. children). Data Privacy Day notably provides a forum for dialogue among all of the stakeholders in the GDI – businesses, individuals, government agencies, non-profit groups, academics, teachers and students – to look more thoroughly at how advanced technologies affect our daily lives. The number of participating countries and stakeholders continues to expand each year, with an increasing number of government entities from around the globe participating in this education and awareness-raising effort. This endeavor is designed to promote understanding of privacy best practices and rights. Intel and a growing number of corporations participate to help demonstrate their common concerns, and to share how what they are doing to address such concerns demonstrates the accountability of their own organizations. Outreach efforts like Data Privacy Day need to be more than just corporate activities. This is why Intel is now working with The Privacy Projects (TPP), a leading Privacy Policy NGO, to have TPP coordinate industry, government, NGO and academic participation in the annual event. Data Privacy Day truly symbolizes what can happen when companies step up to help make the “triangle of trust” operational – it is evidence that working together will increase the trust and confidence in the GDI. More information about Data Privacy Day can be found at www.dataprivacyday.org.

increased public awareness regarding the security and privacy problems threatening to undermine the functioning of the GDI (from both a technology and policy standpoint). In addition to highlighting the measures companies are taking to address these concerns (from processes to products), Intel has taken a leading role in furthering perhaps the most prominent cross-border, multi-stakeholder educational effort in this space: Data Privacy Day.

V. Conclusion and Recommendations

The data empowered world has brought enormous benefits to businesses, consumers and society as a whole. At the same time, the exponentially growing amount of data being processed on a global scale is accompanied by increased risks. All entities working within the GDI need to innovate solutions to provide security and protect privacy, while at the same time increasing the rate of economic growth and technological innovation. These interests can best be served by focusing policy efforts on the primary technological characteristics that have driven the GDI's growth – openness, interoperability, and enabled economic growth.

A more cohesive global digital infrastructure policy should be further developed. The underpinnings of such a sensible GDI-Policy are already in existence today:

- The 'Triangle of Trust,'
- Flexible technology neutral laws and regulations;
- International cooperation and global standards; and
- Accountability systems.

Yet enabling these GDI-Policy mechanisms in a meaningful and comprehensive way requires continuing the global dialogue between industry, governments and NGOs who are working to address the challenges of building trust in the global digital infrastructure. Collaboratively, we can build meaningful and attestable accountability into our organizational structures, technology development processes, and cooperative efforts and policies.

The current environment presents an unprecedented opportunity for technology policy collaboration not only between governments, corporations, and NGOs, but between the technical and policy communities, and between the privacy and security communities. Intel is committed to fostering these bridging efforts – by continuing to innovate in the technology sphere, by providing the solutions that build trust in the GDI, and by working with other stakeholders to innovate in the policy sphere. We offer up a vision of what we believe the contours of a GDI-Policy should look like, and provide our own accountability practices as a model for consideration, in an effort to encourage not only dialogue, but action.

As part of that effort, Intel specifically recommends the following five actions to further the GDI-Policy:

1. Put an end to import, export and use restrictions on cryptography for COTS and public research;
2. Hold international discussions involving all stakeholders in the Triangle of Trust regarding decreasing cyber attacks, with the goal of an intergovernmental accord limiting the proliferation of such attacks;

3. Increase understanding and implementation of accountability practices amongst public and private sector organizations to an accepted global framework or standard, increase international government funding of NGOs as certifying agencies, and develop robust, harmonized, coordinated and predictable enforcement mechanisms against noncompliant entities;
4. Deepen government/private sector partnerships and international collaboration on cybersecurity research, including increased government funding;
5. Promote the widespread adoption of a unified certification process and global standards for product assurance and product security to ensure a secure platform for the GDI. More specifically, we recommend improving the reliability and cost effectiveness of Common Criteria by adopting a tiered approach to certifications (allowing companies to attest to compliance with an accepted global standard for certain levels of products, and for third parties to verify company attestations), expanding Common Criteria to development processes, and broadening the international mutual recognition of Common Criteria.

###

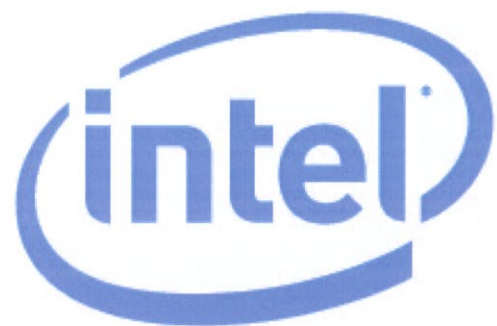
This paper is intended as a discussion draft, and will be updated over time. Please take part in an open dialogue on these issues by submitting comments at <http://blogs.intel.com/policy>.

Acknowledgements

David Hoffman, the Director of Security Policy and Chief Privacy Officer for Intel Corp., leads Intel's Security & Privacy Policy Team. John Miller is Senior Counsel and Policy Strategist in Global Public Policy, and a member of the Security & Privacy Policy Team.

The creation of this paper was a collective effort, and the authors would like to thank many Security & Privacy Policy Team members and others for their significant substantive and editorial contributions and support. We are greatly indebted to Jun Takei, who first articulated the concept of the Global Digital Infrastructure, in the form described in this paper, and who also spent considerable time helping us apply the concept to our policy ideas. Audrey Plonk and Christoph Luykx were selfless with their time to help us reshape the paper and contributed several of the included concepts and examples, and Audrey tirelessly reviewed and carefully edited numerous drafts. Several other members of the core and extended Security & Privacy Policy team provided substantive comments that helped make this a better paper, including John Kincaide, Claire Vishik, Scott Uthe, Kai Chen, Hitesh Barot, George Thompson, David Rose, David Doughty, Brian Huseman, Jonathan Weeks, Stuart Tyler, Brian Willis and Donald Whiteside. For further information on many of the contributors, please see the author biographies at <http://blogs.intel.com/policy>.

Finally, we would like to thank Marty Abrams, Director of the Center for Information Policy Leadership, for generously taking the time to review the paper and provide thoughtful comments,



Sponsors of Tomorrow.™

**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.¹ 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

¹ 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.

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.² 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.

² 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.³

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.

³ 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.⁴ 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.⁵

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.⁶

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

⁴ 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.

⁵ 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.

⁶ 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. 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.⁷

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

⁷ 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,⁸ 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.

⁸ See www.donotcall.gov.