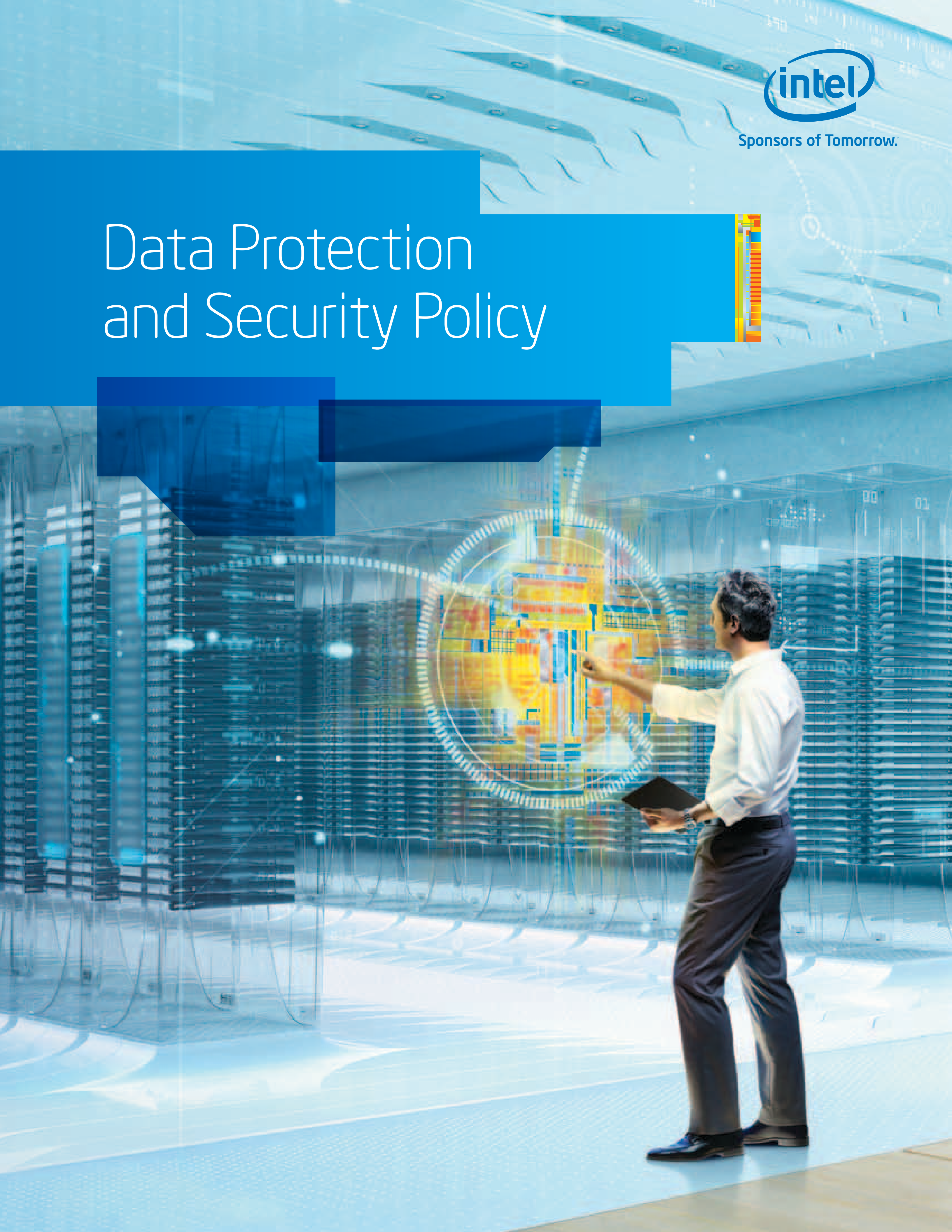
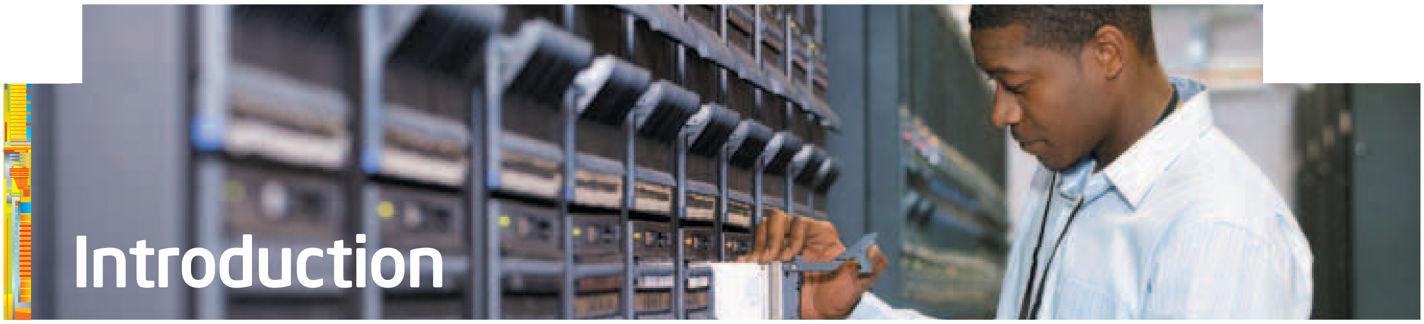
Sponsors of Tomorrow.

Data Protection and Security Policy





Introduction

TABLE OF CONTENTS

Letter from Intel's Director of Security Policy and Global Privacy Officer

The past two decades have seen a tremendous rate of innovation in the way that data is used. The benefits of this innovation hold tremendous promise for our economy and to aid the lives of individuals. People are using a great number of Internet connected devices to manage this data and the applications that use the data. We refer to this spectrum of devices (e.g., PCs, laptops, tablets, smartphones, connected televisions, etc.) as the Compute Continuum. The use of these connected devices, and the numerous applications which run on them is transforming the way we work, socialize, and spend time with our families. However, along with these benefits come concerns of privacy and security. It is critical we address these concerns, so individuals continue to have confidence in their use of technology.

David Hoffman,
Director of Security Policy and
Global Privacy Officer

As a result, a burgeoning profession has emerged to help manage these issues. Ten years ago there were relatively few individuals who considered themselves "privacy professionals." There were lawyers, professors, IT managers, engineers, and marketers who worked on privacy issues, but there were likely very few who would consider themselves "privacy professionals." Fast forward to 2011, and there is a starkly different environment. There is an International Association of Privacy Professionals (IAPP) with over 9,000 members. The IAPP offers a Certified Information Privacy Professional (CIPP) certification, which thousands of individuals have obtained. Most of the Fortune 100 have Chief Privacy Officers, who oversee staffs of "privacy professionals." Online privacy is now also at the forefront of public attention: Congress has held hearings about online privacy, data breaches have exposed the personal information of millions of consumers, and Congress is considering several pieces of privacy legislation.

Similarly, the importance of data security professionals has greatly increased during the last several years. We have seen both the number and complexity of threats increase. Malicious online attacks have morphed from mischievous hackers to sophisticated criminal organizations intent on stealing intellectual property, damaging infrastructure and obtaining sensitive personal information. In response, many companies now employ large numbers of cyber security professionals.

In this environment, Intel works hard to create trust in the use of new technologies. We are investing significantly in developing innovative security technologies which gain the benefit of operating in both hardware and software. We are also working with other stakeholders to determine better ways to share threat and vulnerability information, and to use that information to better secure the digital infrastructure. Last, but not least, we are committed to being an accountable organization. Intel utilizes Privacy by Design and the Secure Development Lifecycle to develop products with both privacy and security in mind. Intel also works to educate consumers about the importance of online data protection, and it is a proud founding sponsor of Data Privacy Day.

For several years, Intel has recognized the increasing interrelation between privacy and security, as two components which can both increase trust. I am proud to lead our Security and Privacy Policy Team of outstanding legal, policy, and technical professionals. I hope that the following papers help to explain Intel's views on privacy and security. We look forward to working with all interested parties in promoting strong trust in the use of the great diversity of devices that comprise the Compute Continuum.

Sincerely,

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

Intel's Vision: Security and Privacy for Today's Global Digital Infrastructure

What is the Global Digital Infrastructure?

The global digital infrastructure (GDI) consists of the foundational information and communications technology products that make up and enable the Internet and modern communications. The GDI is predominantly composed of interoperable hardware and software products which do not vary significantly amongst individual countries and are deployed worldwide. Together, these products allow networks to communicate with each other. The components make up the central nervous system of not only innovation, but economic development and social interaction.

As individuals and businesses increasingly rely on the GDI, they place a corresponding value upon the security of the network and the protection of data traversing the network. Yet this need for trust in the security and privacy provided by the GDI is increasingly challenged by the rapid increase of malicious attacks (such as hackers and malware) to the network and data. It is critical that the GDI continues to promote innovation of security and privacy measures at a pace equal to the development of these threats.

Intel acts as a trusted advisor to governments on a number of different topics, and is expanding these relationships in emerging areas such as security assurance.

GDI-Policy

To help provide for the innovation of new security and privacy technologies needed to ensure that the GDI continues to thrive, Intel believes another type of innovation is necessary: policy innovation, and the development of a global digital infrastructure policy (GDI-Policy). New information and communications technology (ICT) innovations are frequently stalled and sometimes blocked by a confusing and often conflicting array of country specific laws and regulations. A unified GDI-Policy informed by cross-border policy cooperation provides an opportunity to enable continued innovation and economic growth.

GDI-Policy Principles

Intel believes that a successful GDI-Policy should build off of the following common components that have helped the GDI flourish and become ubiquitous:

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 web filtering requirements, and local standards regarding data protection. 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 the seamless operation of networks irrespective of geographic borders. This ability of systems or components to exchange and use information has been largely enabled by global technical standards. However, the current policy environment is increasingly creating barriers to interoperability which threatens to undermine the benefits of these standards. Recent legislative proposals and enacted country-specific laws create inefficiency and harm interoperability, preventing innovators from focusing on meeting the needs of the entire GDI. A GDI-Policy helps ensure interoperability, allowing innovators to focus on meeting the needs of the entire GDI.

ENABLED ECONOMIC GROWTH. For the ICT sector to continue its rapid growth, companies worldwide need to be able to work with each other to bring innovative solutions to the global market. Companies need access to the best available people, processes, and technology irrespective of country of origin to remain competitive in the global marketplace. In addition to these technical preconditions, building trust in the 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 e-commerce growth.

> Intel believes that the best way to ensure continued innovation and economic growth is to pursue multi-jurisdictional efforts that are as global in scope as the GDI.

GDI-Policy Mechanisms

Policymakers worldwide increasingly realize 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. Numerous countries and jurisdictions are considering new privacy legislation, information security legislation, or country-specific certification schemes (i.e., to assess certain products for known security flaws). The question is which one of two divergent paths the change will follow:

- Individual countries increasingly pass isolated, and sometimes conflicting, laws endeavouring to "regulate" different aspects of the GDI; or
- Governments and industry work together to coordinate multi-jurisdictional and transborder standards.

Intel believes that the best way to ensure continued innovation and economic growth is to pursue multi-jurisdictional efforts that are as global in scope as the GDI. High-level principles which have gained broad acceptance over the past 40 years can provide insight into the best way to structure GDI-Policy. Additionally, 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.

The following four current mechanisms can provide the foundation for a more productive policy environment:

1. Public-Private-NGO Partnerships
2. Flexible, Technology-Neutral Laws and Regulations
3. International Cooperation and Global Standards
4. Accountability Systems

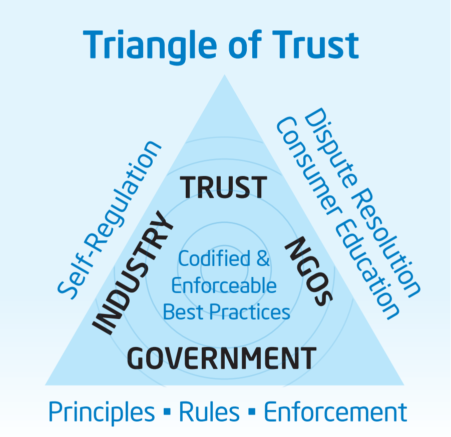
1. Public-Private-NGO Partnerships: The Triangle of Trust.

One policy mechanism upon which to build GDI-Policy is the public-private-NGO partnership. No single entity can achieve the goal of building trust in the GDI; it is clearly a shared responsibility. Governments, Industry, and Non-Governmental Organizations (NGOs) all benefit by working together to form a "triangle of trust."

Governments 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–including advocacy groups, academics, think tanks, and civil society—form the final "side." They assist both government and industry in codifying best practices, handling dispute resolution to free up scarce government enforcement resources, and helping educate individuals and privacy/information security professionals. It is important to note the "length" of this side of the triangle will vary based on circumstances, including the specific country, economy, or issue involved.



Governments and industry should work together to develop a policy and regulatory environment informed by the principles of openness, fairness, and flexibility. Industry best practices can play an important role in developing robust, context specific implementation guidance of laws and regulations. Governments can play a significant part in this process by being "impatient conveners" of industry best practice discussions and by providing predictable enforcement of laws and regulations. NGOs can then assist by documenting this enforcement guidance and helping to 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 trusted NGOs as indispensable partners in the efficient and trustworthy functioning of the GDI.

Key Escrow – A Cautionary Tale

In the 1990s, the US conditioned 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 U.S. attention to make certain its technology neutral and market driven aspects continue to apply to COTS that are increasingly integrating more powerful cryptography.

2. Flexible Technology-Neutral Laws and Regulations.

Sensible regulation of the GDI need not require the creation of new laws or principles. Ample flexibility exists in many current laws, principles, and regulations dealing with aspects of data protection, privacy, and security.[1] Indeed, the EU Data Protection Directive, OECD guidelines, and U.S. privacy laws all lack detailed regulations which 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.

However, this technology-neutral and market-driven regulatory approach, which has largely stayed in place for approximately twenty years, is currently in danger of eroding. The use of increasingly powerful encryption technologies has become more pervasive in widely available software and hardware products. Current encryption laws and regulations in the U.S., China, Russia, and other countries impose regulations ranging from limited export controls; import authorization/declaration requirements for ICT products with cryptographic technology; and restrictions on the distribution, sale and use of such products (including R&D and manufacturing in some cases).[2] Moreover, restrictive government procurement guidelines for purchasing custom hardware or software and local technology certification guidelines may effectively weaken government systems by splitting them off from the Commercial-Off-The-Shelf (COTS) products driving the GDI as a whole.

Some of these regulations have the impact of requiring the adoption of certain country-specific standards and technologies, effectively mandating a particular technology. Even the application of more limited encryption export controls by the U.S. is increasingly creating burdens and supply chain instabilities, as encryption capabilities are now pervasive in ICT products. Such proscriptive, technology-focused regulations are forcing companies and their customers to preserve the ability to functionally disable (fuse off) innovative security technologies in products sold in some countries. This prevents security enhancing features from being deployed globally and creates portions of the GDI that operate in a less secure environment, frustrating interoperability and creating manufacturing inefficiencies that could hinder innovation.

While many countries are understandably worried about cyber threats, country or technology specific policies are counterproductive. Proposals discussed by policymakers in India, the U.S., and elsewhere—including demands for access to encrypted data or the encryption technology itself—would represent several steps backward to the encryption debates of the 1990s and threaten to undermine security across the GDI. Intel believes that the best way to mitigate the security risks threatening economic growth is with robust, peer-reviewed, public encryption ciphers and internationally interoperable cryptography standards. 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.

[1] For example, the OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data contains a Security Safeguards Principle stating, 'Personal data should be protected by reasonable security safeguards' [OECD 'Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data' 23 September 1980 Principle 5, at [11]. The EU Data Protection Directive contains a similarly flexible Article regarding security, providing that 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 [Article 17(1)].

[2] 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.

3. International Cooperation and Global Standards.

To create an effective and efficient GDI-Policy for the 21st century, 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 privacy and security problems threatening the GDI, governments should avoid creating geographically-siloed regulations that may impede the global interoperability and network connectivity that have powered the GDI. Governments would also be well-advised to avoid taking confrontational action which may provoke country specific retaliation.

While some coordinated efforts have so far been carried out, such as the effort led by the Spanish Data Protection Agency and the Council of Europe's Convention on Cybercrime, additional undertakings are needed. Worryingly, policymakers at various national governments continue to draft legislation in areas such as cybersecurity with little to no attention paid to cross-border realities.

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 APEC's Data Privacy Pathfinder Project. Also notable is the proposal to design privacy into products, services, and business processes known as privacy by design. Designing in privacy includes a flexible set of principles allowing for technology companies to honor local traditions.

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 secure development lifecycles. Security assurance—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. There is great potential value in multi-lateral certifications for security like the Common Criteria. GDI-Policy efforts should focus on how we can improve the reliability and cost effectiveness of these processes while providing 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 that GDI-related standards can play an increasingly prominent role. They can be particularly useful in developing security policy areas such as security assurance, as an alternative to uncoordinated recent major legislative efforts in the U.S., China, and elsewhere.

No single entity can achieve the goal of building trust in the GDI; it is clearly a shared responsibility. Governments, Industry, and Non-Governmental Organizations all benefit by working together to form a "triangle of trust."

Intel predicts that the number of connected devices will grow from 4 billion in 2011 to 15 billion by 2015.

4. Accountability Systems.

Private sector companies should work together with all stakeholders—governments, NGOs, and users—to create and increase trust. The primary means by which they can do so is by demonstrating accountability, both internally to their organization and externally to stakeholders.

Accountability is a well-established principle of data protection, having longstanding roots in many of the privacy and security components comprising legislation in the U.S., EU, OECD, APEC, and Canada. 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.[3]

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:

- Commitments which are interpreted based on flexible and technology-neutral laws, industry best practices and entity specific promises;
- Processes and procedures put in place to deliver on the commitments;
- Attestation by the entity demonstrating how it has fulfilled its commitments; and
- 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, the government and NGO "sides" of the Triangle of Trust have clear roles to play here as well. For example, robust, harmonized, and predictable enforcement by regulators is critical to lend credibility to any accountability system.

Demonstrating accountability internally requires an organization to make responsible, disciplined decisions regarding privacy and security. It shifts the focus from an obligation on individuals to understand complicated privacy notices to an organization's ability to demonstrate its capacity to achieve specified objectives.

[3] Galway Project, 'Data Protection Accountability: The Essential Elements' (October, 2009).

The accountable organization complies with applicable laws and 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 into the GDI that have been vetted through processes such as the Secure Development Lifecycles (SDL).[4] Designing in privacy should occur during the entire innovation pipeline, from concept to product, and can include introducing new hardware based on cryptographic mechanisms. Intel and other like-minded companies are currently committing significant resources to "being accountable" in this way. But industry must do more, in a systemic and systematic way, to demonstrate accountability processes than to simply say, "Trust us—we're accountable."

Ultimately, regulators are responsible for ensuring that risks have been managed appropriately, so regulators are unlikely to simply defer to industry best practices in this area. Instead, regulators should comment on global best practices and use 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 get products/services/programs to market;

(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.

Rather, third-party certification mechanisms need to comprehend the processes by which an organization ensures that 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 third-party enforcement and dispute resolution (similar to the way corporate officers annually attest to compliance with the EU—U.S. data transfer safe harbor principles). The key to accomplishing the needs of the GDI is to make these attestations or certifications 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.

The Way Forward

The worldwide nature of the GDI necessitates a global solution. Intel cannot achieve this vision of a GDI-Policy alone, so we invite readers and policymakers alike to join a constructive dialogue around the most effective ways to ensure continued innovation and economic growth.

[4] The SDL defines the actions, deliverables and checkpoints a project team follows to engineer in security/privacy at a foundational level, and then assures the market that product expectations are met.

Privacy and Security Topics

Why Intel Cares About Privacy and Security

Consumers and businesses increasingly use connected devices—laptops, tablets, smartphones, etc.—to store and access sensitive information, such as financial and health records. Consumer and business trust in the security and privacy of online information is central to the continued growth of e-commerce, the telecommunications sector, and Intel's business. If consumers and businesses do not trust their online information is private and secure, then they will buy fewer computers or other products that contain Intel components. Recent studies and surveys have found not only do consumers care deeply about the privacy and security of their electronic information, but privacy and security concerns may impede the growth of e-commerce. Many consumers also falsely believe that current laws and regulations afford them greater privacy protections than is actually the case.

> "Since Internet commerce is dependent on consumer participation, consumers must be able to trust that their personal information is protected online and securely maintained."[5]
>
> *— U.S. Department of Commerce*

Several recent studies and polls have shown that consumers care deeply about online privacy. In a survey published in 2010:

- 68% of respondents thought that there should be a law that gives people the right to know everything that a web site knows about them;
- 92% supported a law requiring web sites and advertising companies to delete all stored information about an individual;
- 86% strongly agreed or agreed that "generally speaking, anyone who uploads a photo or video of me to the Internet where I am clearly recognizable should first get my permission;" and
- 63% of respondents also stated that they often or sometimes erase Internet cookies.[6]

A separate poll of mobile users found that:

- 98% consider having some access to mobile privacy controls important;
- Privacy and security were the two most frequently listed primary concern of mobile users (38% and 26%, respectively);
- 74% of respondents do not like advertiser tracking;
- 85% would like the choice to opt in or out of targeted mobile ads;
- 77% don't want to share their location with app owners; and
- When asked about the importance of privacy when using a mobile device, 79% said it was extremely or very important.[7]

Consumers also care about online security. A recent study found that:

- 60% of Americans back up their information electronically, with 75% of these backing it up at least every month;
- 65% of consumers stopped visiting a web site after receiving a security alert message about potential risks of the site; and
- When asked how the possibility of becoming a victim of cybercrime changed their behavior, if at all, 36% say they only visit web sites they are familiar with, 15% stopped or limited online purchases, and 8% stopped or will not do online banking.[8]

Worryingly, consumers are becoming increasingly concerned about the security and privacy of their electronic information. A 2009 study found that 67% of those polled strongly agreed or agreed that "Consumers have lost all control over how personal information is collected and used by companies."[9] A study one year later found that 55% of participants are more concerned about privacy issues on the Internet now than they were five years ago; only 6% were less concerned.[10] A poll of smartphone users in 2011 found that only 37% of respondents agreed or strongly agreed with the statement "I feel in control of my personal information when using my mobile device."[11]

[5] NOI, 75 Fed. Reg. at 21227.

[6] Chris Hoofnagle, et al, "How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?," April 14, 2010, http://ssrn.com/abstract=1589864

[7] TRUSTe, "Mobile Privacy: A User's Perspective," April, 2011, http://www.truste.com/why_TRUSTe_privacy_services/harris-mobile-survey/index.html

[8] NCSA and Symantec, "2009 NCSA / Symantec Home User Study," October 2009, http://www.staysafeonline.org/sites/default/files/resource_documents/Home%20User%20Study%20FINAL.pdf

[9] Joseph Turrow et al, "Americans Reject Tailored Advertising and Three Activities that Enable It," September 2009, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214?

[10] Hoofnagle, et al, "How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?"

[11] TRUSTe, "Mobile Privacy: A User's Perspective."

Additionally, consumers are showing increased concerns about the security of their online information. "Consumers have expressed an increased awareness in many types of threats they face online each day," and many are worried about sharing their personal information due to security concerns.[12] A survey conducted in 2009 found that 62% of respondents were more concerned about online security now than two years earlier. Another poll, carried out in 2011, found that 36% of American adults are not confident, or not at all confident, in the security of online transactions while 37% are uncomfortable, or not at all comfortable, using their credit cards for online purchasing.[13] Moreover, only about one third of consumers believe most web sites are safe for shopping, an 11% decrease from two years ago. The same survey found that 84% of online consumers continue to have some level of concern when providing personal information online.[14]

Reflecting their concerns, Consumers are willing to pay for greater privacy and security. Over 90% of Americans have antivirus software installed on their primary home computer, of whom almost half purchased antivirus software separately.[15] A separate study by Carnegie Mellon examining online purchasing found that participants made significantly more purchases from sites rated "high privacy" (47.4%) than participants buying from sites rated "no privacy" (5.6%). The study even found that consumers were willing to pay additional money to buy products from vendors that offered better privacy protection.[16]

Consumers are right to be concerned about online privacy and security threats. According to the FTC, "many companies—both online and offline—do not adequately address consumer privacy interests."[17] A recent Wall Street Journal survey of 101 popular mobile apps found that 45 did not have privacy policies, and "56 transmitted the phone's unique device ID to other companies without users' awareness or consent. Forty-seven apps transmitted the phone's location in some way. Five sent age, gender and other personal details to outsiders."[18] Moreover, online security threats are growing daily. McAfee now collects roughly 2 million new malware samples every month, and total malware samples in McAfee's database have almost doubled in the 18 months from Jan 2010 to June 2011.[19]

Despite growing and widespread concerns about online and mobile privacy, many consumers falsely believe they have stronger privacy protections than they actually do. For example, one study asked consumers five simple questions about Internet privacy (such as: "if a company wants to follow your Internet use across multiple sites on the Internet, it must first obtain your permission"). Overall, 30% answered zero correct, 45% 1-2 correct, 22% 3-4 correct, and only 3% correctly answered all five.[20] Another study found that "American consumers believe (albeit mistakenly) that an array of strong laws prohibit companies from sharing or selling data about them."[21] As consumers become more aware of how weak the legal and regulatory regime protecting their privacy is, they may participate less in e-commerce.

In fact, there is evidence that privacy and security concerns may already be beginning to negatively impact consumer trust in the Internet. In 2010, a study found that 56% of respondents had changed their minds about buying something online because of a privacy or security concern. Additionally, 88% refused to give information to a business or company because they "thought it was not really necessary or was too personal."[22] Privacy fears appear to be especially serious in the mobile space. For example, a recent poll of smartphone users found that 85% say they've restricted some type of mobile information sharing on mobile applications.[23] Additionally, a 2011 survey found that one-third of the smartphone users that don't use geolocation apps did not use them because of privacy concerns. [24]

> Consumer trust is vital to the continued economic growth of e-commerce and the telecommunications sector.

Consumer trust is vital to the continued economic growth of e-commerce and the telecommunications sector. Consumers are becoming increasingly aware of online security and privacy concerns. They expect companies and government to work together to protect consumers. Intel believes that best way to ensure this trust is through the adoption of strong, technology-neutral legislation and international standards.

[12] RSA, "RSA 2010 Global Online Consumer Security Survey," 2010, http://www.rsa.com/products/consumer/whitepapers/10665_CSV_WP_1209_Global.pdf

[13] Rasmussen, "57% are Still Confident in Online Security," April 2011, http://www.rasmussenreports.com/public_content/lifestyle/general_lifestyle/april_2011/57_are_still_confident_in_online_security

[14] McAfee, "McAfee Survey Reveals that Confidence in Online Retailers has Fallen Since 2009," August 18, 2011, http://www.mcafee.com/es/about/news/2011/q3/20110818-01.aspx

[15] NCSA and Symantec, "2009 NCSA / Symantec Home User Study."

[16] Online Consumers Willing to Pay Premium for Net Privacy," ScienceBlog, 11 July 2011, http://scienceblog.com/46176/online-consumers-willing-to-pay-premium-for-net-privacy/

[17] FTC, "Protecting Consumer Privacy in an Era of Rapid Change," December 2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

[18] Yukari Iwatani Kane and Scott Thrum, "Your Apps are Watching You," *The Wall Street Journal*, December 17, 2010, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html

[19] McAfee Labs, "McAfee Threat Report: Second Quarter 2011, McAfee," 2011, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2011.pdf

[20] Hoofnagle, et al, "How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?"

[21] Turrow et al, "Americans Reject Tailored Advertising and Three Activities that Enable It."

[22] Hoofnagle, et al, "How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?"

[23] TRUSTe, "Mobile Privacy: A User's Perspective."

[24] Jamie Beckland and Will Reese, "Lost in Geolocation: Why Consumers Haven't Bought it and How Marketers Can Fix It," White Horse, Spring 2011, http://www.whitehorse.com/uploadedFiles/World/Reports/Lost%20in%20Geolocation%20Report(1).pdf

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. At Intel, we strive to put accountability into practice by building out layered internal accountability systems.

Internal Accountability Structures

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

> 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.

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 from 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 against this difficult problem to help ensure the rate of security innovation keeps pace with developing threats.

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 realizes that there are certain legitimate law enforcement needs for data access. However, Intel does not think 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. Intel 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.

Intel has several internal processes to facilitate this focus on security and privacy—for example, Intel employees are required to complete both privacy and security related training tailored to their job positions. Intel's Security and Privacy Policy team (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. SPP has also developed a set of privacy principles that guide product development and Intel's use of personal data.

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 platformization[25] 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 integrate security/privacy and then assure we meet the expectations of the product and market.

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

TRUSTED GOVERNMENT PARTNERSHIP. Intel acts 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, Intel frequently discusses Critical Infrastructure Protection (CIP) issues with governments around the world. Intel also partners with governments to share information regarding threats to the GDI and critical infrastructure.

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

INDUSTRY COOPERATION AND COORDINATION. Intel is helping to encourage the development of the Triangle of Trust by helping build GDI-Policy. Intel coordinates with other industry leaders and facilitates discussions and cooperation with and amongst governments.

Intel has been particularly active in external policy efforts concerning security assurance. These efforts have included addressing growing government concerns regarding global supply chain security, participating with other leaders in the field to promote security assurance processes and awareness, and 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 both government security concerns and the industry need for a timely and cost-efficient process.

EDUCATION AND OUTREACH LEADERSHIP. One of the mechanisms needed to give life to the concept of accountability is 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.

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) and to promote understanding of privacy best practices and rights. It also 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.

Intel and a growing number of corporations participate to help demonstrate their common concerns, share what they are doing to address such concerns, and demonstrate the accountability of their own organizations. Intel is also working with The National Cyber Security Alliance, to help coordinate 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. Data Privacy Day 2012 is January 28th. More information about Data Privacy Day can be found at **www.dataprivacyday.org**.

The Computing Continuum and Data

The world is witnessing an explosion of connected devices, or those devices which can communicate with each other, usually through the Internet. Intel predicts that the number of connected devices will grow from 4 billion in 2011 to 15 billion by 2015. As part of this increased connectivity, Intel believes individuals will be able to seamlessly move their data between devices, with individuals having the same user experience across different devices. We call this seamless connectivity between devices the computing continuum.

In addition to increased connectivity, the computing continuum will utilize an expanding array of hard and soft sensors to enable a multitude of new uses. Hard sensors, such as GPS, and soft sensors, such as user preferences and calendar information, will be combined to deliver new functionality. For example, soon an individual's smartphone will be able to communicate with his or her car. The GPS function 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 their phone in a car. If the driver gets a text message, the message would not be displayed on the phone. Instead, the speakers of the car could 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 will again display text messages on its screen. Additionally, while en route the user's smartphone could combine information from his or her calendar, GPS location, and traffic information. It could use this combined information to determine that the user is going to their next calendar appointment and reroute them around road construction.

The computing continuum has the ability to bring huge benefits to individuals, businesses, and governments. A seamless connection that "just works" can increase productivity, save money, spur innovation, and decrease frustration. The computing continuum will allow more developers access to more devices—increasing competition and leading to better products. As technology continues to develop, individuals will use a variety of devices to access and manage their data, from traditional desktop and laptop computers to small form factor and even embedded devices. It will be critical for individuals to be able to share data and applications between these devices.

Intel's Role in the Compute Continuum

In order for the computing continuum to thrive, connected devices ranging from cars to phones to computers must be able to securely and easily communicate with each other. A common computing ecosystem built on a common architecture with consistent software is vital to the operation of the computing continuum. As a principal hardware supplier of the Global Digital Infrastructure, Intel is uniquely positioned to help provide this common architecture. Intel® architecture can play a key role in helping to accelerate and enable the computing continuum, delivering a common architecture with uncommon performance.

Privacy and Security for the Computing Continuum

Security and privacy are key to the success of the computing continuum. Devices that are part of the computing continuum will increasingly gather sensitive data through hard and soft sensors, such as location and life style habits. The computing continuum will also lead to the transferring of this information among multiple devices. Consequently, users will expect strong privacy and security controls to protection their data.

Intel believes that one of the best ways to protect users' privacy and security on the computing continuum is through comprehensive privacy legislation. Intel supports the passage of comprehensive U.S. privacy legislation that would ensure companies follow a baseline of privacy. Such legislation should also include provisions for robust security, as privacy is reliant on security. Additionally Intel has several recommendations for how to make privacy legislation in the EU more effective.

Another way to help ensure the security and privacy of users' data is through privacy by design and the secure development lifecycle. Companies that adhere to these two principles build products with security and privacy considerations in mind at every stage of the development process. This results in final products that are more secure and have stronger privacy protections.

Intel's corporate vision is to create and extend computing technology to connect and enrich the lives of every person on earth.

Common Standards

In order for the compute continuum to function, devices will need to be able to talk to each other. Common technology standards are vital to this communication. Intel encourages all companies and countries to work towards the continued development of common, interoperable standards. The compute continuum will also allow business models where companies in multiple countries could hold a user's data. Since data can be combined in new, useful ways to deliver services, countries should coordinate interoperable laws that allow data to move freely across borders without delay or legal restrictions. Such a free flow of data will enable continued innovation and economic growth.

Vision

Intel's corporate vision is to create and extend computing technology to connect and enrich the lives of every person on earth. Intel hardware can play a key role in making this future possible by enabling and accelerating the adoption of the compute continuum. In order to reach their full potential, the computing continuum will need to incorporate strong privacy and security and be subject to interoperable, global standards.

Privacy and Security: A Two Way Street

As part of a new corporate strategy in 2010, Intel concluded that security is the third pillar of computing, along with energy-efficient performance and Internet connectivity. Intel believes that online privacy and security are interrelated. Privacy makes up an essential component of Intel's security framework.

In order to be effective, electronic privacy needs security. As evidenced by the numerous data breaches that have taken place recently, malicious actors are targeting personal data for financial or political reasons. While the data breaches have exposed the personal data of millions of people, countless other attacks have been prevented due to robust security. Without robust security, malicious actors would be able to steal huge amounts of personal data that could be used to defraud, embarrass, or discriminate against individuals.

Likewise, strong privacy helps provide sound security. Intel's Privacy Standards are based on the widely-respected Fair Information Practices, and several of these have the additional benefit of promoting security. "Data minimization" states that only the minimum amount of data necessary to accomplish a goal should be collected in the first place. "Retention," meanwhile, holds that sensitive or personal data should only be retained for as long as the purpose for which it was collected. Finally, "transfer" specifies that privacy and security requirements must be complied with when transferring data to a third party.

In addition to providing strong privacy protections, these three Privacy Standards also help increase security. By reducing the time period and amount of data that Intel maintains, minimization and retention decrease the potential losses due to a data breach. Therefore, if there is a data breach, less personal data is able to be compromised. Similarly, transfer ensures that even if personal data is shared with third parties, it is still subjected to high security and privacy standards.

> In order to be effective, electronic privacy needs security.

Intel believes privacy and security are significantly interrelated. Strong security is necessary to protect private information and, strong privacy protections are beneficial for security.

U.S. Privacy Legislation

Recent data breaches and online security threats have spurred renewed Congressional interest in privacy legislation. Congress is currently considering several different approaches to best protect consumers' privacy in the modern world while ensuring continued technology innovation. Intel believes that the most effective way to balance the need for strong consumer privacy and continued innovation is through comprehensive privacy legislation.

The Need for Legislation

Intel has worked hard to understand what consumers want out of technology and why. We consistently hear that consumers have different ideas about what information deserves to be private. Consumers want to control information that is important to them; they want to be able to choose what, when, and with whom to share certain information. After having made choices about how to protect this information, they do not want to be surprised by how the data will be used.

The Commercial Privacy Bill of Rights Act of 2011

Intel believes that this bill, co-sponsored by Senators John Kerry and John McCain, deserves robust discussion. Importantly, the Kerry-McCain bill is technology neutral, encourages privacy by design, gives consumers choices about sharing their personal information, and provides strong security protections for personal data. Intel supports discussion of the Kerry-McCain Commercial Privacy Bill of Rights Act of 2011, as it supplies an excellent framework to provide consumers with the controls and protections they want.

Technology provides a significant opportunity for individuals to make choices about how their online information is shared and used. In order to exercise this control, the companies that create hardware, software, and online services must develop user experiences that allow individuals to understand what can be done to protect access to data. However, individual choice will also have its limits, as technology users likely will not have time to constantly be asked whether they consent to a specific use of their data. A system is necessary to determine what are the specific uses of data which require affirmative consent, and in what situations should consent be implied from the context (e.g., I implicitly consent for an online retailer to send my address to a shipping company when I pick that shipping company as the fulfillment option online). For this system to work, U.S. federal privacy legislation must be enacted, and there must be a backstop of government enforcement to hold companies accountable when they mislead people about how technology will operate.

> Intel believes that the most effective way to balance the need for strong consumer privacy and continued innovation is through comprehensive privacy legislation.[29]

The best way to ensure that consumers can manage their information is comprehensive privacy legislation. Such legislation would create baseline protections that apply to all actors in the marketplace. Comprehensive privacy legislation would also provide important statutory guidance to companies. It would provide companies with a predictable standard, allowing them to design new products with the specific standard in mind.

Elements of Legislation

Intel feels strongly that baseline privacy legislation should be focused on the principles and concepts laid out in the Organization for Economic Cooperation and Development's (OECD) Fair Information Practices (FIPs). The FIPs are internationally recognized privacy principles that, due to their high level, will stand the test of time in an environment where technology is rapidly evolving. They include:

- **COLLECTION LIMITATION PRINCIPLE –** There should be limits on 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.
- **DATA QUALITY PRINCIPLE –** Collected personal data should be relevant to the purposes for which they are to be used.
- **PURPOSE SPECIFICATION PRINCIPLE –** The purposes for which personal data are collected should be specified not later than at the time of data collection.
- **USE LIMITATION PRINCIPLE –** Personal data should not be used for purposes other than those specified in the purpose of data collection except: (a) with the consent of the data subject, or (b) by the authority of law.
- **SECURITY SAFEGUARDS PRINCIPLE –** Personal data should be protected by reasonable security safeguards.
- **OPENNESS PRINCIPLE –** There should be a general policy of openness about developments, practices, and policies with respect to personal data.
- **INDIVIDUAL PARTICIPATION PRINCIPLE –** An individual should have the right: (a) to obtain confirmation of whether or not the data controller has data relating to him or her; (b) to receive, from the data controller, information about what data is collected about him or her; (c) and to challenge data relating to him/her and, if the challenge is successful to have the data erased, rectified, completed, or amended.
- **ACCOUNTABILITY PRINCIPLE –** A data controller should be accountable for complying with measures which give effect to the principles stated above.

Privacy legislation should also be guided by other fundamental principles. Firstly, it should be technology neutral and not mandate the adoption of specific technologies. This is a key provision because technology changes rapidly, and the proscription of specific technical solutions can hinder the adoption of new and more effective technologies. Secondly, privacy legislation should encourage privacy by design, the principle that companies should build technologies with privacy in mind.

Consumers and businesses increasingly realize the privacy risks threatening their personal data and care deeply about exercising control over their personal information. Building a trusted online environment 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 e-commerce growth. Intel strongly believes that comprehensive U.S. federal privacy legislation that follows the above principles is a key mechanism for building this consumer trust in the Internet and e-commerce.

New Data Protection Legislation in the European Union

Computing technology has advanced significantly since the European Council and Parliament passed EU Directive 95/46 in 1995, and Intel supports efforts to update this Directive. Intel agrees with the European Commission that two central elements to any legislative proposal on data protection in the EU should be:

(a) Ensuring respect for the fundamental rights to data protection which leads to increased trust; and

(b) Enhancing the global and internal market dimension and facilitating the free flow of personal data.

Any legislative proposal should focus on the outcomes rather than the prescriptive means to achieve them. The principles as enshrined in the current Directive should be maintained as they are still valid. Additionally, it is essential that the principle of technology neutrality is respected in the new legal framework.

Increased Harmonization

Intel feels it is necessary for the new legislative framework to continue harmonization efforts within the EU. Greater focus is required on limiting Member States' specific customization of the legal framework in order to provide greater clarity of individual rights and to simplify the implementation of operational measures. For example, widely varying requirements for providing access to personal data should be avoided.

One of the best ways to achieve more clarity and harmonization is to base the legal framework on a home country principle. Under this principle, if an organization has multiple establishments within the EU, it would be the Data Protection Authority of the main establishment that would be the lead authority. Under the current legal regime, organizations that are established in multiple EU markets need to comply with the data protection regimes in each of those markets, which sometimes have divergent obligations. This compliance with multiple regimes imposes significant compliance costs on the organization—and not always with any corresponding benefit in terms of enhanced user protection. Such a principle would reduce the administrative burdens for any organization involved while providing more legal certainty.

In addition to greater harmonization within the EU, it is clear that there is an increasing need for simple, consistent and practical data protection standards that can be understood and followed globally by international organizations. Such global rules would not lower the standard of privacy protection, but instead would provide a visible and realistic future for data protection compliance. Intel encourages all countries, including EU member states, to help drive harmonized, international data protection standards.

Accountability

Intel promotes the inclusion of an accountability principle in any new legislation. Accountability has been summarized as "the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations" and as going "beyond responsibility by obligating an organization to be answerable for its actions."[26] Accountability tools should be added and the overall system should be used in a more coherent, harmonized, and predictable fashion. Demonstration of accountability should also provide benefits such as in the area of international data transfers and reduction of administrative burdens.

Industry must do more, in a systemic and systematic way, to demonstrate accountability processes, than to simply say, "Trust us—we're accountable." To ensure accountability, Intel supports the inclusion of a privacy by design concept if it is technology neutral, flexible, and focuses on the processes instead of imposing prescriptive procedures. Intel also supports the creation of a privacy profession and voluntary Data Protection Official (DPO) model with harmonized requirements for Europe. DPOs should not be personally liable or potentially criminally responsible, except for cases of clear and intentional fraud towards the DPA. Introducing specific criminal liability regimes will hamper the nascent growth of a privacy

[26] "Data Protection Accountability: The Essential Elements A Document for Discussion" from the Center for Information Policy Leadership (CIPL) - October 2009.

culture. Moreover, Intel promotes Privacy and Security Impact Assessments (PIAs) as a tool to ensure an organization has the right internal processes in place, if this remains technology neutral, and flexible.

Voluntary third-party certification can be a useful mechanism to demonstrate accountability and if connected to a reduction of administrative requirements. However, this can only be effective if it avoids: (1) being too detailed, (2) requiring too much detailed knowledge by the certifying authority, and (3) using siloed geographical approaches—these attestations or certifications must be to globally recognized principles or best practices.

To further strengthen accountability, Intel supports the concept of accountability as a driver of international transfers. International data transfers have grown in complexity, despite the lack of a practical mechanism for compliance and the absence of a culture of accountability amongst organizations of varying types and sizes. If an organization, regardless of its size, provides adequate protection and accountability measures, transfers of personal data should be able to take place without complex, lengthy, and costly administrative processes. Adequate protection should not be interpreted as equivalency to the Directive, but instead should focus on whether the core principles of the Directive are met. Binding Corporate Rules (BCRs) can play an important role in this process, and further work is required to simplify the processes for drafting and ratifying BCRs and to encourage organizations to adopt them.

Intel encourages the simplification of the current notification and registration regimes. Current global data flows, combined with bureaucratic procedures, have made this system overly burdensome, costly and largely ineffective. One way to streamline the current system would be to establish a one-stop shop regime in which an organization would only be required to notify only in specific and limited situations and in one Member State based on the lead DPA model. However, it should be avoided that any new obligations come into place, such as prior consultation obligations, which would undermine the efforts in reducing administrative burdens.

Finally, Intel urges governments and organizations to develop best practices. Best practices can be a useful tool for supervisory authorities to help interpret the high-level principles of the Directive and can have an important role to play in the facilitation of awareness and understanding towards individuals.

Increasing Consumer Trust

Education is vital to continued consumer trust in the privacy and protection of their electronic data. Intel calls for more awareness raising and education by providing more support for civil society, NGOs, professional associations, and other organizations that have privacy awareness and education as their primary mission and that regularly report on their progress to the general public. Additionally, Intel supports the view that improvements to privacy notices are needed but cautions against strict standardization and calls for flexibility.

> Intel feels it is necessary for the new legislative framework to continue harmonization efforts within the EU.

U.S. Cybersecurity Legislation

Intel is committed to creating trust in the use of technology products, including providing robust security assurance, and protection of individual privacy. Consequently, Intel feels cybersecurity legislation should:

(a) Protect the computer systems of governments, companies, and individuals;

(b) Support innovative security research and development; and

(c) Allow industry the agility to innovate novel security solutions.

Cybersecurity legislation should foster long-term security solutions and allow U.S. companies to continue to lead the world in innovation.

Technology Mandates

U.S. cybersecurity legislation should avoid overly proscriptive mandates on the ICT sector and instead empower voluntary codes of conduct and industry best practices. Proscriptive legislative mandates that specify certain security measures can actually decrease security by hindering the adoption of innovative new security approaches. Given the rapidly evolving technology and security landscape, the best way to provide robust security is through government and industry collaboration. By combining their expertise, government and industry can develop flexible standards that protect both security and innovation. Already-existing industry best practices and voluntary codes of conduct can provide the basis for these new standards.

Global Norms

U.S. cybersecurity legislation should also be consistent with global norms and standards. U.S. ICT companies sell their products globally, and country-specific regulations are a significant threat to rapid and continued innovation. Non-harmonized and country-specific regulations could impose considerable costs on companies, potentially forcing companies to build different products for different markets. Such additional costs would substantially curtail companies' ability to create innovative new technologies and security solutions. By enacting cybersecurity legislation that is harmonized with existing global standards, the U.S. could set a powerful precedent of international cooperation for other countries to emulate. Conversely, siloed and country-specific U.S. cybersecurity legislation would encourage other countries to follow suit. The Common Criteria (CC), an international security certification scheme, provides a strong framework for international coordination and cooperation on harmonized security standards, and if properly modernized can be an effective tool for establishing trust in the use of technology.

Critical Infrastructure

To increase security, any definition of critical infrastructure should be specific and exclude most Internet-connected technologies and networks. Several potential cybersecurity bills contain definitions of "critical infrastructure" (CI), infrastructure that, due to its importance, is subject to additional regulations. There is clearly some infrastructure, such as the equipment controlling nuclear reactors, that is significantly more critical than most infrastructures. However, if the definition of CI is too broad, then government and industry will not be able to focus finite security resources and expertise on protecting the most important systems; strong protection of the most important systems will be traded for lesser protection of many systems.

A broad definition of CI would also impose additional reporting certification costs on numerous companies, reducing their competitiveness against international competitors and depriving them of funds to invest in new, innovative security solutions. Many in government have already realized the importance of focusing scarce resources on protecting the most important systems. To ensure that the most important pieces of infrastructure receive the best protection possible, the definition of CI should be limited to entities whose failure could lead to a mass casualty event, a significant national security incident, or a catastrophic halt to economic markets.

COTS Products

Cybersecurity legislation should also affirm that commercial off the shelf (COTS) products are not subject to onerous federal government procurement policies. COTS products are the standard technology products (such as the software and hardware) produced for the entire consumer market. Many COTS products can be used in sensitive, government systems; for example, COTS expense tracking software could be used to track classified expenses. When the federal government buys new products, it specifies the requirements (for security, reliability, etc.) in Federal Acquisition Requirements (FARs). FARs are frequently time-consuming and expensive. Consequently, forcing COTS products to undergo FARs would slow the pace of innovation by imposing significant delays and costs on companies. COTS products should therefore not be subject to burdensome FARs, and instead these requirements should be carefully used for the most sensitive government systems.

Breach Notification

Intel supports preemptive federal data breach legislation, and believes that such legislation should be based on global norms. Currently, almost every U.S. state has its own data breach law, and these laws are frequently inconsistent. This patchwork of state laws makes compliance expensive and burdensome. Consequently, Intel encourages preemptive federal data breach legislation that creates a single, federal data breach notification standard. Given the global nature of the internet and ICT products, the federal government should develop a global strategy and framework for security breach notification that is developed with international partners.

Intel also believes data breach legislation should include the following key components. First, such legislation should clearly define security breach notification objectives while avoiding mandates dictating the specific technologies and processes that must be used to accomplish those objectives. Second, data breach legislation should also encourage and fund the research, development, and use of safe harbor technologies and processes. These technologies should 1) render unauthorized accessed data practically unusable, unreadable, or indecipherable and 2) be widely accepted as effective industry practice in the global marketplace. Finally, Intel promotes policy efforts to proactively mitigate the risks to individuals caused by unauthorized access to personal information, including support for stronger authentication methods and technologies.

> Intel is committed to creating trust in the use of technology products, including providing robust security assurance, and protection of individual privacy.

Security Assurance and Common Criteria

Governments around the world are understandably concerned about the security of information and communications technology (ICT) products and networks. The best way to address these concerns is through an internationally recognized product assurance and evaluation regime. Common Criteria (CC) is the best such regime and should be updated to increase its effectiveness.

The Environment

Today's dynamic threat environment is marked by increasingly sophisticated attacks targeting both government and civilian critical infrastructure, such as Stuxnet. These attacks are perpetrated by an array of malicious actors across the globe with varying motives. Organizations, consequently, are justifiably concerned about the security of ICT products and networks. To better secure their nation's networks, many governments are increasingly interested in finding ways to evaluate the security features of ICT products.

The vast majority of the hardware and software that make up the Global Digital Infrastructure are sold globally and based on international technology standards that only vary modestly between individual countries and geographies. Given the global nature of ICT products and networks, any security evaluation scheme should be internationally harmonized. International harmonization allows innovators everywhere to have access to global markets for their ICT products, thereby increasing potential investment and the total available market for companies. This, in turn, spurs innovation and leads to more secure products.

Why Common Criteria?

Intel believes a modernized CC is the best mechanism to provide governments with reasonable security assurances while simultaneously allowing innovation to flourish. CC is a common language that allows for the evaluation of security features and assurance parameters of ICT products. Under CC, licensed independent labs evaluate the security requirements of ICT products and specify a level of security assurance against certain attacks.

CC is the only internationally recognized product assurance evaluation and certification scheme for hardware, firmware, and software. Since CC is mutually recognized by 26 countries, a company can receive a security evaluation in one country that can be used in many others. This process dramatically cuts down on red tape and costly delays to market, which allows companies to focus on innovating and developing products for the global market.

Additionally, CC has been in use for over 10 years. It is well understood by the stakeholders in the vendor community who have worked with the certification labs and schemes over time. CC is also scalable to many different types of products and fulfills many different requirements for security assurance. Finally, CC provides a structured review process for developing more secure products that incorporates sufficient flexibility to address new and emerging threats.

> Given the global nature of ICT products and networks, any security evaluation scheme should be internationally harmonized.

Proposed Changes to Common Criteria

In its present form, CC has several drawbacks and should be reformed and extended. Currently, receiving a CC evaluation is a long and expensive process. This lengthy and bureaucratic process can impact product lifecycles and time to market for vendors' products. Additionally, CC lacks consistent objective results across evaluating laboratories. Finally, CC does not have a sufficiently transparent governance process that represents all stakeholders including vendors, labs, and national schemes.

To make it more effective, Intel believes CC should be modified in several ways. Specifically, Intel recommends CC:

- Establish and work through broad technical communities to collaboratively develop security assurance targets. These technical communities should include government and industry representatives and maximize the recognition of targets across borders and technology areas (i.e., only one for operating systems);
- Improve the efficiency and consistency of evaluations;
- Expand the scope of CC to address manufacturing process integrity aspects of the supply chain; and
- Provide vendors and schemes an appropriate format for collaborating on CC reform.

Additional Principles

Intel feels that several other high-level principles should also guide the implementation of security assurance around the world. Governments around the world should:

- Avoid dictating private sector security standards. Government mandates will hamper innovation, increase costs, and result in less secure products;
- Avoid addressing supply chain concerns through government procurement guidelines. Such guidelines will result in less secure products as they slow government adoption of new and innovative security features; and
- Promote cybersecurity solutions that take into account the global nature of cyberspace and ICT products. For example, government procurement guidelines should not exclude products based on the geographic origins of suppliers, vendors, or manufacturing facilities.

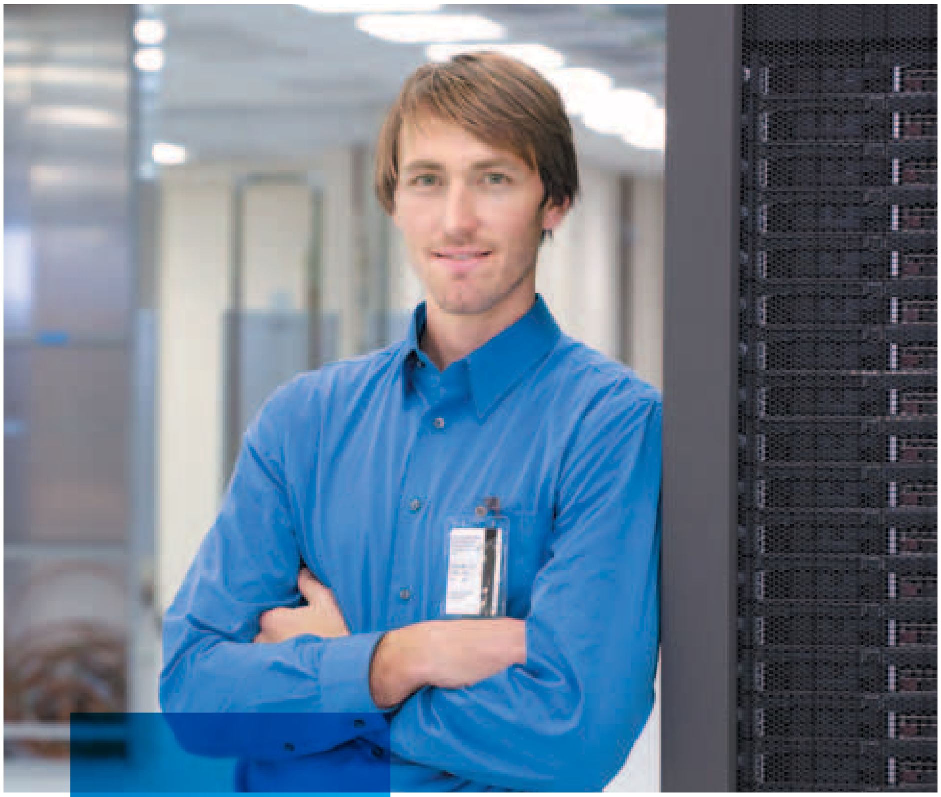
The Path Forward

Several countries around the world are considering geographically siloed approaches to security assurance. Intel feels that such an approach will fragment the market, resulting in less secure products for everyone. Rather, Intel believes the best way to provide security assurance is through solutions that take into account the global nature of cyberspace. CC, as one of the most widely-used security assurance mechanisms, can play a key role in providing governments and organizations with the security assurances they are increasingly asking for. To make it more effective and efficient CC should be reformed and extended.

ECPA Reform

In its current form ECPA is unable to appropriately address today's technology, not to mention tomorrow's innovation.

The Electronic Communications Privacy Act (ECPA), the U.S. statute that governs government access to electronic information, was enacted 25 years ago. When it was passed, ECPA was a cutting-edge piece of legislation. The pace of technological innovation has left ECPA outdated, however, and it urgently needs reform.



ECPA was designed to deal with the technology of a 1986 world, where cell phones cost thousands of dollars and were the size of bricks, the Internet was confined to a handful of labs and military facilities, and GPS technology had not even been invented. Computing technology has undergone tremendous growth since the inception of ECPA, and it will continue to evolve rapidly. The world is witnessing an explosion of connected devices, and within the next few years billions of additional devices will be connected to the Internet. As part of this increased connectivity, Intel believes individuals will be able to seamlessly move their data between devices. Individuals having the same user experience across different devices in what we call the computing continuum.

However, in its current form ECPA is unable to appropriately address today's technology, not to mention tomorrow's innovation. In fact, ECPA is in danger of impairing future technological progress, like the compute continuum. For example, under ECPA e-mail is subjected to different legal standards when it is being typed, opened, and stored by an Internet Service Provider. Additionally, law enforcement does not need a warrant to read the e-mail or personal electronic documents of a suspect, but does need a warrant to read the physical mail of a suspect. ECPA has also been interpreted inconsistently by courts across the country, leading to law enforcement and industry confusion. Such inconsistencies decrease consumer and business trust and create uncertainty in the market.

Consequently, ECPA desperately needs to be reformed. Intel, along with other members of the Digital Due Process coalition, has called for a number of specific reforms for ECPA. A reformed ECPA should incorporate the following components:

- Technology and platform neutrality, so that a particular piece of information receives the same level of protection regardless of the platform or technology used to create, store, or send it;
- Continued law enforcement access with appropriate judicial oversight;
- Equal legal protections for transiting and stored data;
- Consistency so that the content of communications is protected by a court order based on probable cause, regardless of how old the communication is and whether or not it has been opened;
- Simple and clear rules; and
- Recognition of all existing exceptions (such as disclosure to the government in emergency situations).

ECPA reform would greatly benefit consumers, the government, and industry. With a reformed ECPA, consumers would gain the assurance of consistent and clear privacy protections. Law enforcement would also have clear rules to follow and would avoid wasting precious resources interpreting and using unclear provisions of ECPA. Industry too would gain by having clear and consistent rules to follow, freeing up resources to spend on innovation.

Cloud Computing

Data usage is growing at a tremendous rate: in 2010, more data was transmitted over the Internet than in the entire history of the Internet through 2009. Moreover, data usage is set to continue to grow at an incredible rate. Intel estimates that one billion additional users will become netizens (internet users) and over 10 billion additional devices will become connected to the Internet between 2010 and 2015. All these additional users and devices will strain traditional computing resources. Cloud computing can make possible this massive growth while delivering cost savings.

The Cloud

Cloud computing can be defined as the delivery, over the Internet, of information technology infrastructure, applications, and services from remote, third-party managed, data centers. While cloud computing has existed for decades in one form or another, recently there has been a dramatic increase in the options available to businesses and individuals.

Cloud computing offers users—individuals, enterprises, and governments—significant benefits. It allows users the flexibility to access and pay for IT infrastructure, applications, and services on a scalable, use-by-use basis. This model allows organizations to save money on IT infrastructure costs, and increases innovation and competition by allowing start-ups avoid expensive overhead. Cloud computing is also more energy efficient, resulting in a more environmentally friendly footprint. Moreover, cloud computing makes possible new business models and new jobs. Finally, cloud computing can also help facilitate the growth of the compute continuum. As billions of additional devices are connected to the Internet, cloud computing can help share data and applications among devices.

Cloud 2015

In 2010, Intel established a "Cloud 2015" vision that specifies three goals for cloud in 2015: federated, client-aware, and automated. By 2015, Intel envisions a world of interoperable, federated clouds that can share data securely across public and private clouds. Additionally, the vision calls for the cloud to be composed of device-savvy client-aware clouds that organize services based on device capability (i.e., that know what processing should take place in the cloud or on your laptop, smartphone, or other device). Finally, the cloud should enable the automated movement of software applications and resources so that IT can focus more on innovation and less on management.

Privacy and Security in the Cloud

Privacy and security are fundamental to the success of cloud computing and Intel's Cloud 2015 vision. Since cloud computing involves the remote storage of data, individuals and organizations need strong assurances that their data is protected and confidential. Data breaches or other breakdowns in security could cause many users' data to be exposed. Both companies and governments can contribute to building trust in cloud computing.

Intel believes that governments can support the growth of cloud computing in several ways. Government laws and regulations should remain technology neutral by not prescribing the adoption of any specific technology. Technology neutrality allows the private sector to develop and deploy innovative new solutions. In the U.S., Intel supports the adoption of comprehensive privacy legislation and does not believe that such legislation needs cloud specific language. Baseline privacy legislation in the U.S. can provide companies with a predictable standard while ensuring consumer trust in the privacy and protection of their personal data. Intel also supports the reform of the U.S. Electronic Communications Privacy Act (ECPA). This legislation is severely outdated, and Intel backs the efforts of the Digital Due Process Coalition to update ECPA to take into account modern technologies. Intel has also submitted specific recommendations to the EU on updating the EU's Data Protection Directive, EU 45/96.

The private sector too has an important role to play in promoting trust in cloud computing, and companies should work hard to be accountable organizations. Two of the most important ways that companies can demonstrate accountability are by following the principles of privacy by design and the secure development lifecycle (SDL). These processes ensure that companies design products with both security and privacy in mind during every stage of the development process. The result is more secure products with stronger privacy protections.

> Privacy and security are fundamental to the success of cloud computing.

Common Standards

Interoperable and harmonized standards are essential to cloud computing. Since the global digital infrastructure is distributed around the world, a user may live in country A, store their personal data in country B, and store their work data in country C. Consequently, governments should coordinate interoperable laws that allow data to move freely across borders without delay or legal restrictions. Such a free flow of data will allow continued innovation and enable economic growth.

Additionally, infrastructure location should not be a requirement for market access. Such a requirement would be very difficult to operate as data could conceivably fall under multiple jurisdictions. Infrastructure location requirements would also be costly for businesses, which need the ability to quickly move data across national borders. Such a requirement would also harm economic growth, as companies would likely move their data center operations to countries that do not have location requirements.

Industry too plays a vital role in promoting common standards. Intel is proud to serve as the technical advisor to the Open Data Center Alliance, a group of several hundred companies that works to ensure seamless interaction between data centers and an open marketplace.

The Path Forward

The rapid growth of data will require new solutions. Cloud computing can be an integral part of managing the data created by billions of new connected devices and a billion new Internet users in the next few years. Cloud computing can also be a major driver of innovation and economic growth. Both industry and government should work together to foster the growth of cloud computing.

Applications

Since their inception in 2008, applications, or apps, have been an engine of economic growth. Apps are now available for devices including smartphones, tablets, netbooks, and smart TVs. Developers have created apps to help users learn new languages, find places to eat, and play games. Robust privacy and security protections are essential to allow this fledgling industry to reach its full potential.

The Landscape

Consumers have downloaded billions of apps, and the one millionth unique app is expected to be developed in 2011. Apps have, almost overnight, created a market worth billions of dollars. The continued development of this market should be encouraged.

Incidentally or purposefully, many of these apps collect sensitive information such as geolocation or personal information about individuals. In some cases the collected information is needed to perform the functions of the app. In other cases, the collected information provides advertising revenues or the purpose of the information collection is unclear. Much of the information collected by apps is especially sensitive since many apps are on mobile devices, and the owner of the device can be effectively located along with the device. Moreover, this link between the device owner and the device itself provides an opportunity for personal behavioral patterns to be deduced from location data.

Recent studies, newly discovered malware targeting apps, and congressional hearings have all highlighted the growing concerns around current app privacy and security protections, especially for mobile apps. One study found that one out of three smartphone users that don't use geolocation apps do not use them because of privacy concerns.[27] Another poll of mobile users found that privacy (38%) and security (26%) were the two highest primary concerns listed when using mobile apps.[28]

App Privacy and Security

While consumers are excited about apps, privacy and security concerns are hindering the ability of the app marketplace to reach its full potential. Robust privacy and security protections can give consumers trust that they have control over their personal information and that their personal information is secure. With robust protections and controls, consumers will be more likely to trust companies with their personal information, allowing for new business models and services to be created.

Robust privacy and security protections should contain several elements. App developers should provide users with a notice explaining what information they collect, usually in the form of a privacy policy or short form notice that contains a link to the full privacy policy. Notices should: provide notice at the time of collection; be easy to find and read; explain how the collected data is used; and whether the information is shared with anyone else. Additionally, app developers should collect and retain only the personal information required for a specific purpose and keep it no longer than needed to satisfy the purpose. Users should have reasonable access to their personal information and developers should obtain explicit opt-in consent to transfer a user's personal information to third parties. Finally, developers should provide reasonable security measures for the storage and transfer of users' personal information.

These privacy and security safeguards can greatly reassure consumers, allowing the app marketplace to realize latent potential.

Privacy and security concerns are hindering the ability of the app marketplace to reach its full potential. Robust privacy and security protections can give consumers trust that they have control over their personal information and that their personal information is secure.

[27] Jamie Beckland and Will Reese, "Lost in Geolocation: Why Consumers Haven't Bought it and How Marketers Can Fix It," White Horse, Spring 2011, http://www.whitehorse.com/uploadedFiles/World/Reports/Lost%20in%20Geolocation%20Report(1).pdf

[28] TRUSTe, "Mobile Privacy: A User's Perspective," April, 2011, http://www.truste.com/why_TRUSTe_privacy_services/harris-mobile-survey/index.html

Smart Grid

The Smart Grid, a next generation electricity distribution system that utilizes digital devices and services to improve energy management from production to consumption, holds a great deal of promise. Privacy and security are vital to the success and widespread implementation of the Smart Grid.

The Smart Grid can enable individuals to reduce their energy consumption, annual energy costs, and greenhouse gas emissions. Through the use of self-purchased services/devices or Home Energy Management Systems, individuals can monitor and manage their energy usage. However, this promise will only be fully realized if individuals trust that robust security and privacy protections are in place. For example, consumers will want strong protections to keep their usage data private so that potential burglars cannot use energy usage to determine when houses are unoccupied. Moreover, individuals should have sufficient access to data about their own energy use, energy sources, and pricing. Finally, individuals should have the ability to control and manage their own energy usage.

Intel believes that comprehensive U.S. privacy legislation can establish a baseline of consumer trust and protection that will enable the Smart Grid to thrive in the U.S. Such legislation should include requirements for privacy by design and accountability. Privacy by design will ensure that vendors creating Smart Grid products or services will incorporate privacy protections as an essential early step in the development process. Accountability will make certain that vendors collecting an increasingly granular view of data from individuals' homes will put in place mechanisms, policies and structures to make certain the data is managed appropriately no matter where the data is processed. It is also important that any new laws are sufficiently technology neutral, flexible, and in accord with global norms, so that companies creating Smart Grid products and services can innovate both to reduce energy consumption and to increase the level of privacy and security provided for the data.

For more information, current developments, and to participate in the discussion please visit **http://blogs.intel.com/policy**

Also, follow Intel’s policy team on Twitter at **@IntelPolicy**

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.

0112/BH/HBD/PDF 326536-001US

Sponsors of Tomorrow.