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

By John Miller and David Hoffman

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

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

# Contents

*Case Studies and Additional Information*

*Graphics/Charts*

## I. Executive Summary

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

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

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

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

- openness[2],
- interoperability, and
- enabled economic growth

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

[1] http://www.intel.com/education/isef/

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

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

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

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

## II. Introduction

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

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

## III. Toward a Global Digital Infrastructure Policy

### *a. GDI Components*

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

- Openness,
- Interoperability[3], and
- Enabled economic growth[4]

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

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

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

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

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

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

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

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

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

## Network Fragmentation Risks

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

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

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

**Enabled Economic Growth.** Companies worldwide need to be able to work with each other to bring innovative solutions to the global market. In the technology sector it is rare when one company can work in isolation, whether they are creating hardware components, portions of the software stack, or services layered on top of the hardware and software. Companies need access to the best available people, processes and technology, irrespective of country of origin, to continue the innovations necessary to drive the GDI, and remain competitive in the global marketplace. At the same time, in addition to these technical preconditions, building trust in the digital economy is an essential component of driving the GDI forward. Building a trusted global environment in a systemic way not only benefits consumers and increases their trust in the use of GDI technologies, but is vital to the sustained expansion of the Internet and future ecommerce growth.

## Internet Policy

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

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

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

### a. GDI-Policy Mechanisms

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

(1) Individual countries increasingly and in isolation pass laws endeavoring to 'regulate' different aspects of the GDI; or

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

[5] Some examples include:

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

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

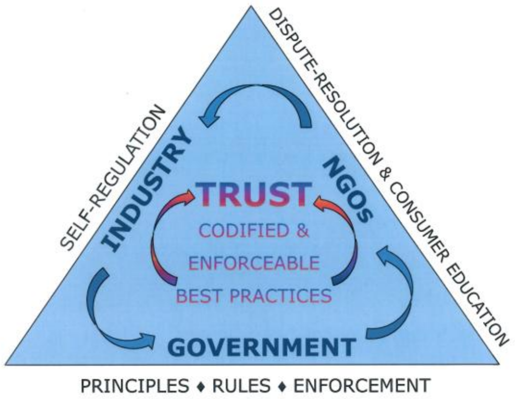
Navigating the increasingly confusing and non-harmonized patchwork of global legislation with respect to privacy and security to extract elements common across cultures presents challenges. There are efforts to harmonize around central standards or legislative approaches (the EU 95/46 Directive is a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

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

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

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

Figure 1 - Triangle of Trust



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

### Cybersecurity R&D

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

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

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

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

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

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

[7] EU Directive 95/46/EC, Art. 17(1).

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

We can look both to past efforts such as the key escrow scheme considered by the U.S. in the 1990s[9] and ongoing regulatory efforts in the encryption area in a number of jurisdictions to provide further support for this concept. Currently, encryption laws and regulations in the U.S., China, Russia and other countries variously impose regulations ranging from limited export controls to import authorization/declaration requirements for ICT products with cryptographic technology to restrictions on distribution, sales and use of such products (including R&D and manufacturing in some cases).[10] Some of these regulations have the impact of requiring the adoption of certain country specific standards and technologies, which run the risk of mandating a particular technology as the innovation that must be deployed. Even the application of more limited encryption export controls by the US is increasingly creating burdens and supply chain instabilities, since the substantial liberalization of the controls a decade ago are now being outpaced by the pervasiveness of encryption capability in ICT products. Such

### Cryptography

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

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

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

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

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

proscriptive technology focused regulations are forcing companies like Intel and its customers to attempt to preserve the ability to functionally disable (fuse off) innovative security technologies in products sold in some countries. If not for these regulations, these security enhancing features would be deployed globally. Fusing off this technology creates portions of the GDI that operate in a less secure environment and over time will frustrate interoperability and international transactions, as well as creating manufacturing inefficiencies that could hinder innovation. GDI-Policy solutions should encourage technical innovation, collaboration and openness rather than proscriptive security measures or the imposition of standards which require the adoption of a particular technology.

### Smart Grid

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

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

**3. International Cooperation and Global Standards**. Just as the GDI itself is a network of networks – and requires hardware and software working together to create a trusted stack – governments must work together to create a networked regulatory framework – a policy and legal infrastructure which promotes continued innovation and enabled economic growth. In developing solutions to the privacy and security problems threatening the GDI, we should avoid creating geographically siloed regulations that may impede the global interoperability and network connectivity that have spurred the growth of the GDI. Governments would also be well-advised to avoid taking confrontational action which may provoke country specific regulation. While some coordinated efforts have been carried out such as the effort led by the Spanish Data Protection Agency (which resulted in the Joint Proposal for a Draft of International Standards with regard to the processing of Personal Data),[11] and the Council of Europe's Convention on Cybercrime,[12] additional efforts are needed as more policymakers at various other national governments continue to draft legislation, in areas such as cybersecurity, with little to no attention paid to cross-border realities.

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

[12] http://conventions.coe.int/treaty/en/treaties/html/185.htm

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

## Government Procurement & Assurance

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

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

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

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

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

## Cyber Crime ~ Cyber Attacks

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

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

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

> *Accountability is the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations. Accountability goes beyond responsibility by obligating an organization to be answerable for its actions.*[15]

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

[14] The accountability principle is included in:

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

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

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

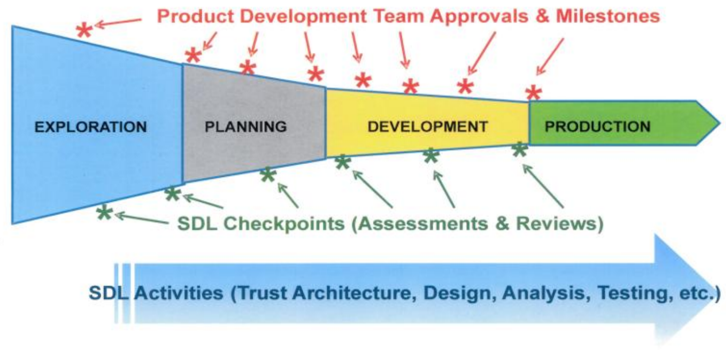
## Accountability & The Galway Project

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

### *Demonstrating accountability internally*

Accountability requires an organization to make responsible, disciplined decisions regarding privacy and security. It shifts the focus from an obligation on the individual to have to understand complicated privacy notices to an organization's ability to demonstrate its capacity to achieve specified objectives. The accountable organization complies with applicable laws and then takes the further step of implementing a program ensuring the privacy and protection of data based on an assessment of risks to individuals. For example, companies can demonstrate accountability by innovating to build trust, such as by developing and selling more secure and privacy-enhancing component parts into the GDI that have been vetted through processes such as development lifecycles which have privacy and security integrated as foundational elements.[16] Intel and other like-minded companies are currently committing significant resources to "being accountable" in this way now. But industry must do more, in a systemic and systematic way, to demonstrate accountability processes, than to simply say, "Trust us – we're accountable." Adoption and implementation of a "privacy by design"[17] process

Figure 2 – Secure Development Lifecycle (SDL)


Product Development Team Approvals & Milestones
EXPLORATION
PLANNING
DEVELOPMENT
PRODUCTION
SDL Checkpoints (Assessments & Reviews)
SDL Activities (Trust Architecture, Design, Analysis, Testing, etc.)

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

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

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

### *Demonstrating accountability externally*

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

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

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

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

(c) uses siloed geographic certifications without mutual recognition.

### Privacy by Design & Accountability

Over the past several years, regulators in multiple jurisdictions have called for more formalized and widespread adoption of Privacy by Design.  The consensus view of these regulators – including the Art. 29 Working Party, the FTC and the European Data Protection Supervisor – has been that the voluntary efforts of industry to implement Privacy by Design have been insufficient.  (See, e.g., FTC Commissioner Harbour's speech at the last FTC Roundtable.)  Intel believes that a Privacy By Design principle should encourage the implementation of accountability processes in the development of technologies. To achieve its objective, the principle should avoid mandatory compliance to detailed standards, or mandatory third party detailed product reviews, as this would decrease time to market and increase product costs. This would be particularly the case when it is unclear whether third parties would have the appropriate resources or skill sets to effectively review the technology.  Instead, a Privacy by Design accountability model should focus on making certain privacy is included as a foundational component of the product and service development process.

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

## IV. Intel’s Accountability Model and Ecosystem Role

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

### a. Internal Accountability Structures

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

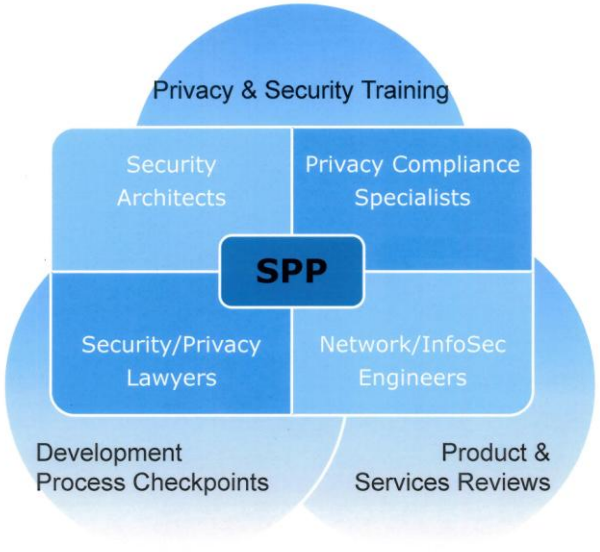
**Trust Innovation.** Building trust via designing in privacy and security is now an integral part of Intel’s entire innovation pipeline, from concept to product. We are actively engaging with “white hat” communities, striving to stay one step ahead of an escalating threat model, and doing fundamental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

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

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

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

Figure 3 – SPP Team Matrix


Privacy & Security Training
Security Architects
Privacy Compliance Specialists
SPP
Security/Privacy Lawyers
Network/InfoSec Engineers
Development Process Checkpoints
Product & Services Reviews

**Security Assurance in Development and Manufacturing**. Product complexity and platformization[18] add new challenges for Intel and its customers. To better demonstrate development and manufacturing accountability, Intel is increasingly focused on security assurance and has undertaken significant initiatives aimed at increasing security assurance processes across the company, including establishing the Security Center for Excellence (SeCoE). One SeCoE-led initiative is "Design for Security," which is focused on building a capability in each and every engineering team to develop secure products. A central aspect of this initiative is educating engineers to design for security and privacy. Another example is the Intel Secure Development Lifecycle, which defines the actions, deliverables and checkpoints a project team follows to engineer in security/privacy and then assure we meet the expectations of the product and market.

**a.** <u>External Trust Policy Efforts</u>

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

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

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

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

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

Intel has been particularly active in external policy efforts concerning security assurance, not only to address growing government concerns regarding global supply chain security, but by participating with other leaders in the field to promote security assurance processes and awareness, and by helping to drive our industry partners to invest in security assurance. Additionally, peer review and academic research are playing more important roles in security assurance processes – Intel along with others in industry increasingly share technologies with universities, researchers, and other peers, affirming the principle that openness is the preferred way to test security. Intel is also taking a leadership role in the important area of trust verification. Specifically, Intel has been working with others in industry as well as the certification labs in an attempt to improve the current common criteria certification scheme, to make sure it addresses the concerns various governments have expressed in currently proposed regulations, while addressing the concerns of industry to make certification more timely and cost-efficient.

## Data Privacy Day

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

**Education and Outreach Leadership.** As mentioned above, 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.

## V. Conclusion and Recommendations

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

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

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

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

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

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

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

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

# # #

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

# Acknowledgements

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

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

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

intel®

Sponsors of Tomorrow.™