WITSA's Statement of Policy on Privacy, Security and Data Protection

September 2017

Document Purpose

This document has been prepared to provide policy guidance from the ICT industry to all stakeholders on the complex issues regarding cyber security, data privacy, trust and confidence etc. It can be used as a tool for the development of policy and to create opportunities for discussions with government officials and all appropriate stakeholders. It represents an extension to WITSA's publication: Policy Actions to Deliver the Promise of the Digital Age

Synopsis

Building and maintaining trust and confidence between all users of the Internet is one of the fundamental building blocks of the Digital Age. Trust and confidence are fragile concepts, often slowly formed, but rapidly destroyed when shown to be vulnerable, directly attacked or as an unintended consequence of other actions. All stakeholders have a role to play in building this trust ecosystem.

There is global concern about the adverse effect on trust and confidence arising from widespread commercial use of personal data, revelations of extensive electronic surveillance programs and efforts to undermine trust in ICT supply chain by governments, affecting both foreign and domestic citizens, corporations and individuals. This is additional to other recognized threats to the confidentiality, integrity and availability of information arising from hacking, fraudulent activities, viruses and other threats. Suggested responses by some governments, including proposals to localize ICT assets and server processing citizens' data within their jurisdictions, while superficially appealing, are nothing less than economic protectionism that threatens global growth. This localization also seriously diminishes the resilience of otherwise globally distributed systems.

WITSA advocates a principled approach, which recognizes information privacy as a fundamental human right, and seeks to balance this in context with equally important policy objectives of national security and data protection while maintaining the economic and social capability of digital information.

This approach highlights the importance of transparency and accountability within appropriate legal frameworks, information sharing of risks and vulnerabilities, and collaboration across jurisdictions.

Context

About WITSA

WITSA is a global consortium of leading ICT industry association members from over 80 countries/economies.

As the leading recognized voice of the global ICT industry, WITSA aims to drive transformation and grow the industry, given that ICT is the key driver of the global economy:

WITSA's members and stakeholders comprise national associations, multinational corporations, institutions and organizations, researchers, developers, manufacturers, software developers, telecommunication companies, suppliers, trainers and integrators of ICT goods and services. As such, they represent a large and obviously vital constituent group for whom the effective balancing of concerns and rights affecting the security, privacy and information capability provided by ICT products and services underpins business development and economic activity.

Privacy, Security and Data Protection in the Digital Age

The commercial use and development of the Internet since 1992 has generated the Digital Age in which we now live, based on the creation and sharing of information digitally, creating enormous capability. Five (of many) key elements critical to this development are:

- the ubiquity, global reach, resilience, standardization and redundancy of the Internet and its protocols;
- the invention and adoption of the World Wide Web built upon this network;

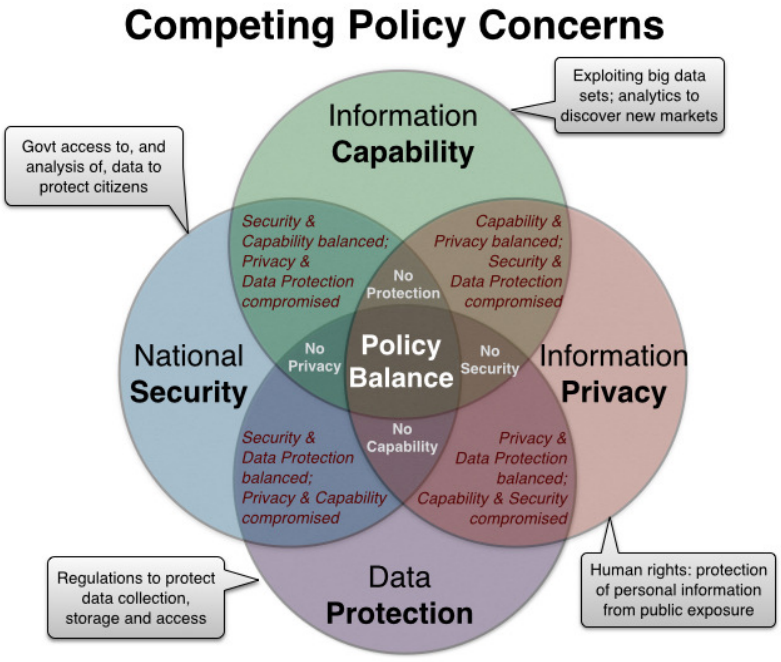
- an evolving, global system of governance and regulation based on open, multistakeholder structures and processes[1];
- the acceptance by virtually all organizations dealing with information derived from personal or commercially sensitive data, of the need for clear protocols to maintain the confidentiality and integrity of the information, while ensuring its availability to those authorized (the so-called "Confidentiality, Integrity, and Availability" triad (CIA triad)[2]" model of information security; and
- the creation and growth of trust and confidence between all users and organizations to enable transactions and the sharing of information over the medium.

Threats to, or failure of, any of these factors may have a profound impact on the others and, in turn, the ability to use the Internet as the modern basis for commercial, social and cultural exchange. However, the last – creating and maintaining user trust and confidence – is very subtle, and closely aligned to the psychological outlook and response of users at multiple levels in response to the visibility of the "Confidentiality, Integrity, and Availability" triad in particular circumstances:

- At one level, it is immensely personal – based on one's own perceptions and experience;
- at another, it is central to the fundamental reputation of organizations, critically reliant upon effective accountability structures and security processes that reflect best practices, universal ethics and principles; and
- at a third, it is underpinned by legal requirements;
- at a fourth, it is subordinated by judgments of "the greater good", whether driven for example by national security or medical emergency.

Hence, there is widespread disquiet regarding the current challenge to trust and confidence that has arisen as a consequence of public revelations of the nature and extent of government surveillance, not just of foreign governments, corporations and organizations, but also of domestic citizens and organizations.

This concern is further heightened by the rising number of reports of organized data intrusion, fraudulent use and theft affecting the information assets of corporations, organizations and government agencies together with theft of user credentials from a number of popular sites by "hacker" groups, in some cases instigated by state-sponsored entities. Widespread attacks such as Ransomware exploiting zero day vulnerabilities are using surveillance program data gone public,



In the Digital Age, trust and confidence is persistently challenged by the competing but fundamental goals that arise from the concerns of the key stakeholders regarding access to, and the use of digital information, perhaps best illustrated in the accompanying diagram. The public policy goal is to achieve the necessary policy intersect, seeking solutions that optimize interests, e.g. solutions that enhance both national security and individual privacy, and

[1] The multistakeholder model of policy development; multiple stakeholders may not always be the enforcement agent for these policies.
[2] http://www.techrepublic.com/blog/it-security/the-cia-triad/ (see also http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf)

recognizing that this is a dynamic, not static, equilibrium depending on circumstances, necessitating a range of compromises.

In developing this public policy guidance, WITSA (representing the global ICT industry) has sought to ensure even-handedness between the competing policy interests; indeed, determining the policy balance in any jurisdiction and event scenario requires constructive and cooperative multistakeholder engagement. Each stakeholder group – industry, government, consumer, civil society, technical community – has both rights and interests they rightfully seek to protect and the responsibility to ensure these are balanced against conflicting, equally valid public policy interests of others.

In recent years, a number of highly publicised events have underscored the need for all nations to focus on these issues, supported by human rights conventions and laws in many jurisdictions:

Information capability represents the extensive range of applications that can be made of data, especially data that is networked and shared by the Internet. This represents a benefit and asset, not just to suppliers of ICTs, but – most importantly – to users. It is this capability that drives productivity and efficiency, providing the information needed for decision-making as and when needed. This capability continues to grow exponentially, as ever more information is digitized and made available, and analytics software enables the ability to draw more and more inferences from the available data; the importance of metadata as both raw material, and a source of further privacy risk; and correlation and regression, inter alia, to identify relationships and predict outcomes. The challenge is that this can be both an opportunity and a threat.

Information privacy has been a concern since personal information relating to one's identity, medical and financial situation, or suggesting political status was first collected, stored and processed by third parties, such as governments and businesses. Different jurisdictions and cultures have developed different practices: in some countries, the information is collected unless an individual chooses to "opt out"; in others, the information should not be collected unless the individual has specifically chosen to "opt in" to the collection process. These differences were less of an issue until the advent of ICTs, which profoundly enhance the capability or organisations and individuals to collect, store and process information, heightening concerns about data breaches and misuse of sensitive information. At the same time, ICTs enable access to critical personal information at crucial times, e.g. health records, or to enable identification; we do want to authorize access to our personal information by certain classes of users at specific times. This issue is further confused by the growth of social media and other forms of personal information sharing, wherein citizens knowingly or unknowingly place personal information on systems that are accessible by third parties.

Data protection supports personal privacy, and has emerged as a particularly important requirement on those collecting and storing information in particular jurisdictions:

- *Transparency*, to ensure individuals have the right to be informed when their personal data is being collected, stored or processed;
- *Legitimate purpose*, meaning that personal data can only be processed for specified explicit and legitimate purposes, and not processed further in a way incompatible with those purposes;
- *Proportionality*, meaning that personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which the data are collected. The data must be accurate and, where necessary, maintained up to date, with inaccurate data removed or corrected; and destroyed when no longer needed.
- Data protection also incorporates the *principle of data minimization*, and the notion of retention periods; e.g. the practice of collecting personal data and retaining it indefinitely for future unknown uses.

Data protection regulations typically stipulate rules based on the principles above, regarding collection/use disclosure, security of information collected, and reporting of information losses. An emerging rule concerns data portability.

National security is a key issue given the emergence of digital information as a critical intelligence asset. Information surveillance technologies benefit from all the technical advances delivered by modern ICTs, thus raising concerns about privacy and the effectiveness of data protection rules when it comes to governments. Additionally, privacy and data protection rules generally contain a carve-out for matters of national security. Equally, citizens expect their governments to protect them from threats of harm, whether physical or in relation information assets. They also expect their governments to support their use of technology (e.g. encryption) to protect themselves, their communications and their data.

Statement of Policy Principles

Principles:

Principles should, as far as possible, be technology neutral so that rapidly evolving technology landscape with use of Machine Learning, AI, IoT, Cloud Computing, Blockchain etc. can be embraced.

Data Privacy:

1. *Privacy, security, and personal safety are fundamental human values*. Every person on Earth should have a right to privacy and the ability to communicate anonymously, which means to control access to themselves and information about themselves that maintains their dignity, self-determination (the ability to know if and when the decisions one makes are being constrained or directed by external agencies), security, property and privacy, unless law requires otherwise.
    a. All stakeholders should start from the assumption that an individual whose personal data is being collected for processing has rights over that data.
    b. Each individual has the right to request that information affecting their privacy be treated confidentially when circumstances require disclosure of such information to a third party.
    c. Third party controllers receiving such information have a fundamental obligation to maintain the security and confidentiality of such personal information shared with them, and only to share such information with the express permission of the organization sharing the information with third party.
    d. Any breach of the confidentiality of private information held must be immediately notified to the persons affected, and all reasonable steps taken to re-secure the information holdings henceforth. Affected organisations should take all reasonable steps to remedy the privacy impact.
    e. The only exceptions are those that arise in manifestly serious circumstances, such as an imminent risk to the health or safety of the person or others, national security or where there are overwhelming legal or societal interests.
    f. WITSA strongly supports the right of citizens to freedom of opinion and expression, to exchange data across borders, and the right to privacy as foundational underpinnings of human dignity. As such, we encourage all governments to respect Article 19 and 12 of the Universal Declaration of Human Rights.
2. *Governments must openly acknowledge and codify the privacy rights of their citizens and residents*, the importance of maintaining trust and confidence in the free flow of information

both within and across national borders, and avoid taking any actions that, without reasonable and specified cause, may undermine the confidentiality, integrity and availability of such information. Moreover, governments should respect the privacy of all individuals regardless of citizenship or residence.

3. *Industry must promote transparency about what data is collected and how it will be processed and handled*, as well as promoting compliance with data protection, security and privacy laws, establish good industry practices, promote privacy by design in all products and services, and educate consumers about the purpose and benefits of data sharing.

Data Protection & Cybercrime:

4. *Data protection does not mean data protectionism.* In seeking to protect privacy, data protection rules must recognize the importance of ensuring critical information flows freely between jurisdictions to enable economic activity and maintain communications. Data localization proposals, in particular, are ill-considered and are simply a new form of economic protectionism, with all the associated, proven damage to global growth of such mechanisms. Some countries promote data localization in name of national security, while others in name of citizens' privacy concerns.
5. *Threats to information security are best addressed by selected sharing of risks and remedies.* Collaboration is essential to create the informed communities of practice and effective emergency response strategies necessary to respond to cyber security threats[3].
6. *Public-Private Sector Collaboration*: To effectively combat cybercrime, governments must leverage multi-stakeholder partnerships to drive durable solutions and improve cooperation with industry and other stakeholders through information sharing initiatives, capacity-building programs, by employing responsible and equitable security vulnerability disclosure and remediation practices, and by jointly fostering technology innovations and investments that address global security challenges. The public and private sectors should also work towards greater adherence to established international cybercrime laws, harmonization of national laws as well as the universal adoption of key principles (Articles 1-9) of the Council of Europe 2001 Budapest Convention on Cybercrime[4]. Governments and industry should also work through international organizations, such as the World Economic Forum, the World Bank and others, to promote collective action to enhance the impact of private sector initiatives and local law enforcement to combat cybercrime.
7. *Industry must promote privacy by design and security by design in all products and services*, develop strategies to enhance security and limit loss due to data breaches or data corruption, as well as establish sound industry practices such as taking appropriate measures to ensure protection of data in storage and transmission, making available regular updating of security measures, and embracing new software and hardware technologies relating to authentication, identification and data access controls.
8. Where conflicts of laws arise across jurisdictions, governments must work together, reasonably and openly, to resolve them.
9. *Oppose Weakening the Security of Technology Products and Services*: Robust cybersecurity and data protection are essential to trust in technology products, services, and systems, and robust encryption is fundamental to building such trustworthy and reliable technology products, services, and systems. Governments must recognize the importance of strong encryption

[3] More information at: ISOC Collaborative Security approach: https://www.internetsociety.org/collaborativesecurity

[4] http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

technologies and refrain from mandating industry to implement "backdoor" decryption capabilities. It is essential that new technologies[5] are developed which continuously enhance secure systems that protect valuable, intimate information of our customers – including governments – to maintain their trust and confidence in these systems, and of the transactions, services and businesses based upon them. To solve legitimate national security and law enforcement concerns, WITSA encourages closer dialogue and cooperation with governments and law enforcement agencies. We need a 21st Century approach to a 21st Century problem.

10. *Governments must Embrace Openness and Global Markets to Enable Security Innovation and Interoperability*: Governments should support policies and practices that foster trust in technology products and services, promote global, market-driven product development approaches norms and protocols for security,
11. *Governments must work together to develop a robust, principled, and transparent framework to administer requests for data across jurisdictions* through mutual legal assistance treaties and should develop information sharing arrangements that are quick, procedural and respect rights.

National Security & Surveillance:

12. In order to maintain the rule of law, we acknowledge *governments need to undertake surveillance in an effort to detect and remove clear and present risks of terrorism and other criminal activity*, but this activity must be expressly limited in scope and scale, and should be articulated clearly and transparently in legal statute(s) reviewed through democratic processes. These activities must be expressly limited by their reasonableness, relationship, and relevance, i.e., that the surveillance contemplated:
    a. arises from generally accepted concepts of reasonable suspicion and due cause, based upon by independent judicial authorization;
    b. relates directly to that basis and purpose;
    c. is targeted; and
    d. is a relevant means of surveillance in the circumstances; and
    e. there is no viable alternative
13. The activities of intelligence and law enforcement agencies in conducting surveillance activities as set out above *should be undertaken within a transparent legal framework*, where actions are subject to timely, independent judicial review (or executive review, where applicable) to ensure full accountability of the agencies for their actions.
14. *All government surveillance policies and programs should be reported transparently, publicly and promptly* in terms of their frequency, mode of surveillance, timing and location etc. to restrict unauthorized surveillance. All requests for surveillance cooperation or access placed on corporations and organisations should similarly be reported promptly, and at least annually, and there should be no restriction on corporations and organisations themselves reporting on requests received in similar terms.

FURTHER READING:

- 2016 WEF Recommendations for Public-Private Partnership against Cybercrime (January 2016)

[5] Eg threat posed by quantum computing to the crypto codes that rely on factorization for crypto work factor.

- Council of Europe Convention on Cybercrime (2001)
- techUK: Trust in an Internet of Things Word (April 2017)
- ITI Global Guiding Principles for Trust, Technology and Government Access in the Digital Age (January 27, 2017)
- Outcome Document of The International Conference on Cyberlaw, Cybercrime & Cybersecurity (November 17-18, 2016)
- Internet Society Global Internet Report 2016
- AT&T Understanding the Cyber Threat: A Policy Guide for Legislators (2016)
- DIGITALEUROPE's views on Cybersecurity Certification and Labelling Schemes (March 23, 2017)
- INTERPOL GLOBAL CONFERENCE ON CYBERSPACE 2015 Chair's Statement
- DIGITALEUROPE Law Enforcement Access to Data in the European Cloud
- ISOC policy framework for an open and trusted Internet (June 22, 2016)
- Collaborative Security: An approach to tackling Internet Security issues (ISOC, April 12, 2015)