Privacy & Security

Building User Trust in Technology

Intel seeks to ensure that Privacy and Security are essential building blocks of the new digital society, enabling User Trust in Technology.

The world is highly connected and the global flow of data is required for today's information economy. Information technologies enable virtually every aspect of our lives; how we work, play, socialize, and educate. With the opportunities that accompany this new digital society come new risks, including more sophisticated computer related threats, many of which directly affect user privacy. It is Intel's view that Governments, Industry and NGOs need to work together to further advance the level of security and respect for privacy, while at the same time stimulating economic growth and the free flow of information.

Triangle of Trust

Building Trust in technology is a complex challenge and clearly a shared responsibility. Governments, Industry and NGOs should work together in a "Triangle of Trust" centered around the Individual;

- **Government** establishes the base of the Triangle by creating a framework of compliance principles and rules, and by conducting robust, predictable and harmonized enforcement.
- **Industry** should build and share best practices which allow companies to improve compliance with laws and regulations.
- **NGOs** should, where possible, bring together industry best practices, educate individuals and privacy practitioners and provide dispute resolution with a clear path to government recourse.

Accountability and Compliance

Accountability and Compliance are two essential building blocks of a Triangle of Trust and major drivers of Intel's privacy and security work. We have comprehensive internal compliance programs as well as privacy and security requirements during the product design and development lifecycle. All employees are required to take annual privacy and security training, and this is further bolstered by constant internal awareness articles. In addition, employees share and apply their knowledge in community volunteering efforts, such as Data Privacy Day[1] and internet security educational outreach.

[1] www.intel.com/policy/dataprivacy.htm

Threat Innovation and the Role of Regulation

Threats to privacy and security are constantly evolving and it is critical that we allow engineers and project managers to innovate solutions at a pace that keeps up, or gets ahead of Threat Innovation. One lesson we have learned as an organization is that we are more successful when we describe well what the problem is, rather than providing detailed requirements on how to solve that problem. We must work on an approach that better prioritizes privacy and security problem-solving over imposing regulations that force technology developers to focus on rule compliance.

Review of the General Data Protection Directive

The cornerstone of the EU's protection of privacy as a fundamental right is the General Data Protection Directive – Directive 95/46/EC (hereafter "the Directive") which is an example of balanced legislation. The Directive addresses problems in a technology neutral manner that innovators have flexibility to solve in ways to best provide value for the individual. An example of this is the Directive's focus on malicious use of personal data, which allows privacy professionals to determine how best to protect the right of privacy. However, since its inception in 1995, increased modern communication and information technologies have brought significant benefits to consumers around the world while introducing some new challenges which warrant a new review of the Directive's functioning.

According to Intel;

- Issues of interpretation, implementation and communication of the Directive must be addressed, but the overall principles and model remain valid.
- Stakeholders must focus on eliminating unnecessary bureaucratic processes, which take resources away from the critical task of mitigating risk to individuals.
- Experience has shown that bureaucratic processes should not be replaced with detailed compliance regulations that will not stand the test of time and are aimed only at specific business or technology cases.

Increased global cooperation, and where necessary harmonization, is essential in providing a functional framework to build User Trust and address constant Threat Innovation.

Intel looks forward to continuing our engagement with all relevant stakeholders in helping to think about ways how to improve the effectiveness of the Directive and the overall protection of privacy and security.

In the event that you have any questions relating to Intel's views on Privacy & Security, please contact Christoph Luykx, christoph.luykx@intel.com.