ITAC SPEAKING NOTES FOR THE OCED PRIVACY CONFERENCE IN ISRAEL 25-26 OCTOBER 2010

PANEL IV – FOSTERING INNOVATION IN PRIVACY PROTECTION

> ***"This session will examine some innovative approaches being taken by organisations to provide individuals with appropriate and usable information to exercise control over their personal information and the challenges to making them effective. It will also consider the broader role of innovative approaches to privacy to address the current environment"*** [1]

Introduction

The Internet Technical Advisory Committee (ITAC)[2] to the OECD was officially recognised by the OECD Council on 15 January 2009. ITAC's main purpose is to contribute constructively to the OECD's development of Internet-related policies. ITAC primarily contributes to the work of the OECD Committee for Information, Computer and Communications Policy (ICCP) and its specific working parties such as the Working Party on Communications and Infrastructure Services Policy (CISP), the Working Party on Information Economy and the Working Party on Information Security and Privacy (WPISP).

Our members include the Internet Society (ISOC)[3], the Internet Architecture Board (IAB)[4], the Internet Engineering Taskforce (IETF)[5], the World Wide Web Consortium (W3C)[6], the Kantara Initiative[7] and the Organization for the Advancement of Structured Information Standards (OASIS)[8].

This group has been working together on privacy issues, not only for the OECD, but also for the United Nations Internet Governance Forum (IGF)[9].

ITAC representatives (Christine Runnegar and Trent Adams – Internet Society) also participate in the OECD WPISP Privacy Volunteer Group.

We aim to bring an Internet technical perspective to the discussion on how to foster innovation in privacy protection.

General principles

- The Internet is the ultimate transborder data conduit: it allows people all over the world to send and receive data from anywhere. The Internet is not controlled by a single country and has no geographical boundaries, though the technologies supporting it must be flexible to operate in various regulatory environments.

- Openly developed, globally-applicable privacy standards, both technical and regulatory, are important for widespread successful deployment of privacy-enhancing technologies.

- Only by multi-stakeholder collaboration and a holistic approach (ensuring value for all stakeholders) to privacy protection will viable solutions emerge, be deployed, and maintained.

- Transparent architectures that secure private information and enable information-sharing in a secure, privacy-enhancing manner are fundamental to effective privacy.

- Technological tools to protect privacy need to be usable, match users' expectations and adaptive to an evolving regulatory, economic and social landscape.

Panel discussion questions:

1. **What technical innovations offer promise for giving individuals easier access to and control over information about them?**

    - Many organisations working on Internet technologies are beginning to focus more explicitly on privacy. Supporting these efforts, standards-setting organisations are actively developing privacy-protecting patterns within their specifications.

    - In this effort, work within general standards-setting organisations such as the IETF (e.g. OAuth), W3C (e.g. STS), and OASIS (e.g. SAML, XACML) is finding common ground with organisations such as the OpenID Foundation[10], Information Card Foundation[11] and the Kantara Initiative that are focused more specifically on identity solutions. The commonality found across the many stakeholders is the growing understanding that users play an important role alongside government and enterprise in the protection of their privacy and personal data.

- Accompanying many efforts is a paradigm shift away from centralised command-and-control approaches relying entirely on cryptographic security as a means of handling and protecting personal data. The emerging focus is on providing **granular access** to specific personal data that may be **distributed** across multiple "authoritative sources".

- A promising new class of personal data management technologies is being called "Personal Data Stores". Technologies developed to support this class of operations empower users to be in control of their personal data for specific uses. Users can leverage existing and emerging identity management technologies such as U-Prove[12], Information Cards, OAuth[13], and User Managed Access (UMA)[14] to provide services with user-controlled access to their data maintained within a secure online repository.

- A simple component that will offer an important foundation upon which to develop effective solutions will be the support for a technical standard defining online notice (i.e. a common mechanism to encode and publish the policies governing usage of services.)

2. What are the incentives and barriers for innovating privacy tools and what are challenges to successful deployment?

- Incentives for innovating privacy tools include:
    i. Technology neutral privacy laws;
    ii. Technologically agnostic privacy frameworks capable of supporting different regulatory environments (e.g. in the area of Identity Management – Kantara Initiative *Identity Assurance Framework*[15]);
    iii. Open, interoperable building blocks supporting privacy-respecting technical solutions (e.g. OAuth – upon which UMA solutions can be built);
    iv. Open environments which support the bottom-up consensus driven development of technical standards and protocols (e.g. the IETF);
    v. Community investment in research and development of user-friendly privacy tools;
    vi. Raising awareness of the availability (or the potential availability) of tools to enable users to be more actively and directly engaged in protecting their privacy in the online environment – thereby driving demand;
        e.g. IdM Policy Audit System[16] (monitor website privacy policies), Ghostery[17] (detect and block web-based trackers), BetterPrivacy[18] (remove flash cookies), SpyBot-S&D[19] (detect and remove spyware)

vii. Recognition by business that privacy provides a competitive advantage and privacy-respecting approaches (e.g. data minimization practices) may lower their risk profile;
viii. Recognition by government that privacy tools can help support the effective implementation of privacy laws;
ix. A strong incentive is the recognition of the economic value that can be realised by enabling a user-managed flow of personal data. Providing privacy-respecting mechanisms to monetize data in a legitimate way will encourage innovation while improving security by adopting patterns of minimal collection and disclosure (data minimization).

- Barriers or disincentives for innovating privacy tools include:
  i. A lack of globally applicable privacy standards (technical and regulatory);
  ii. Insufficient government and/or business appreciation of the value of user-managed privacy tools in protecting privacy;
  iii. Lack of transparency in data handling architectures which allows organisations to continue to handle personal data without requiring them to adhere to structured observable privacy-enhancing models;
  iv. Current economic models that thrive by bartering personal data collected and aggregated by systems outside the user's specific control.

- Challenges to successful deployment include:
  i. Usability – Matching technology to users' capabilities – Noting that there is great variance across a population, what standard of usability is appropriate?;
  ii. Regulatory Environment – Where laws do not support deployment or are incompatible;
  iii. Technical Maturity – Privacy-enhancing technologies are emerging, but are not sufficiently complete at the current stage; additional support and resources are required;
  iv. Scale/Ubiquity – Until the technologies are available and widely deployed to support economic incentives, deployments will need to be incentivised by regulation and advocated for by users;
  v. Accessibility/Education – Even before the technologies are available for deployment, users need to be educated about the problems within the current model, then educated about emerging solutions. Once the solutions are more widely available, education about those new solutions will become the priority.

Note: Only by multi-stakeholder collaboration and a holistic approach to privacy protection will viable solutions emerge, be deployed, and maintained.

- Innovation in privacy tools should be encouraged by all stakeholders:
    i. Consumers of privacy tools can encourage innovation by clearly articulating their needs and expectations;
    ii. Governments can encourage innovation by providing a legal framework that supports the development and deployment of transparent architectures that secure private information and enable information-sharing in a secure, privacy-enhancing manner;
    iii. Business can encourage innovation by developing the market for privacy tools;
    iv. The Internet community can facilitate innovation in privacy tools on the application layer by developing open, interoperable Internet protocols and standards.

3. What is the role of technological innovation within a broader framework for privacy protection?

- Arguably, the Internet is the most remarkable technological innovation for the exchange of data – Further, it is constantly evolving and everyone connected to the Internet can participate in its innovation.

- The way the Internet has evolved – the Internet Model of development – can play an important role in inspiring the approach that governments take in reviewing, revising and/or developing legal frameworks for privacy protection.

- Internet Model is the term used to describe a common set of operating values shared among many of the key communities and organisations that have been central to the development and ongoing evolution of the Internet. These values include:
    i. Open technical standards;
    ii. Freely accessible processes for technology and policy development; and
    iii. Transparent and collaborative governance.

- The Internet's unprecedented success continues to thrive because the Internet model is open, transparent and collaborative. The model relies on processes and products that are local, bottom-up, and accessible to users around the world.

- To be successfully deployed and used, technological innovation should occur in tandem with other elements of a broader holistic framework for privacy protection.

- Technological innovation should be dynamic and adaptive to keep pace with a constantly evolving regulatory, economic and social landscape.

For more information regarding ITAC, please see http://www.internetac.org.

---

[1] OECD Privacy Conference (25-26 October 2010) Agenda – http://www.oecd.org/document/44/0,3343,en_2649_34255_45780844_1_1_1_1,00.html
[2] Internet Technical Advisory Committee (ITAC) – http://www.internetac.org
[3] Internet Society (ISOC) – http://www.isoc.org
[4] Internet Architecture Board (IAB) – http://www.iab.org
[5] Internet Engineering Task Force (IETF) – http://www.ietf.org
[6] World Wide Web Consortium (W3) – http://www.w3.org
[7] Kantara Initiative – http://kantarainitiative.org
[8] Organization for the Advancement of Structured Information Standards (OASIS) http://www.oasis-open.org/home/index.php
[9] Internet Governance Forum (IGF) – http://www.intgovforum.org/cms
[10] OpenID Foundation – http://openid.net/foundation
[11] Information Card Foundation – http://informationcard.net
[12] U-Prove – https://connect.microsoft.com/content/content.aspx?contentid=12505&siteid=642
[13] OAuth – http://oauth.net
[14] UMA – http://kantarainitiative.org/confluence/display/uma/UMA+Explained
[15] Kantara Initiative *Identity Assurance Framework* – http://kantarainitiative.org/confluence/display/idassurance/Identity+Assurance+Framework+v2.0
[16] IdM Policy Audit System – http://www.isoc.org/projects/idm_policy_audit_system
[17] Ghostery – http://www.ghostery.com
[18] BetterPrivacy – https://addons.mozilla.org/en-US/firefox/addon/6623
[19] SpyBot S&D – http://www.safer-networking.org/en/index.html