The Future of Privacy
Insights from the Internet technical community

Internet Governance Forum 2010 Workshop: The Future of Privacy
Presented by the Internet Society

www.InternetSociety.org
An ongoing project …

Collecting innovative, thought-provoking, forward-looking perspectives on the Future of Privacy from individuals, groups and organisations within the Internet technical community with expertise in Privacy, Data Protection, Identity Management and other related fields

Documenting them at www.isoc.org/privacyinsights
In the future, privacy will be redefined in response to changing social, technical, and regulatory realities. While the concept of privacy will remain contextual, individuals will become more actively engaged with the protection of their privacy by actively managing their identity and related personal data.

People will be more informed custodians of their personal data – able to help decide when the sharing of personal information requires explicit consent, and choosing appropriate levels of security and protection.

Internet-based solutions to support user-managed privacy protection are emerging, and the Internet Society is helping to provide clarity about their use to individuals, enterprise, and governments.

Internet Society (ISOC)  www.InternetSociety.org
The W3C, the IETF and the Internet community of privacy experts must work together to provide an online experience that conforms with user expectations of privacy and the emerging regulatory environment.

To keep up with the speed of innovation at the application layer, the IETF needs to develop privacy guidelines, building blocks and tools that are useful for an entire class of applications.

Technical work needs to be backed-up by providing incentives to incorporate privacy into system design and at the same time to keep the speed of innovation and the openness of the Internet intact.

The best technology will not help end users if it does not get implemented properly and deployed in a privacy friendly way.
As a universal, distributed application platform, the Web links personal data across individuals, organizations, and countries. New sensor APIs also give Web applications access to users' location and to their physical environment.

Everyday events – from the morning run to the credit card payment – are automatically brought online and shared online among friends and strangers.

Technology helps users defend against some intrusions, and it helps users understand who learns what about them. But when the data about preferences and habits that fuels the business models behind today's ecosystem of free services is gleaned from users' online interactions, the policy framework needs to encourage privacy friendly behavior.
The Kantara Initiative Privacy & Public Policy Work Group (P3WG) believes that it is important to support the open development of globally-applicable privacy standards, both technical and regulatory, in order to continue having confidence in the Internet ecosystem.

To do so, the P3WG actively engages with individuals, enterprises, policymakers, regulators and adoption communities on best practices and common solutions.

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

Only by multi-stakeholder collaboration will viable solutions emerge, be deployed, and maintained.
The state of privacy and information protection has changed substantially because of changes in technology, business models, and the role of the individual, bringing ever significant challenges to effective application of traditional privacy management.

Implementing policies for increasingly federated networks, systems and applications is a problem as typical policy expressions provide little insight into how to actually implement them, as well as the lack of standards-based technical privacy frameworks or reference models that can enable development and implementation of privacy and associated security requirements.

An effective solution would be a collection of privacy and security policy-configurable, IT-based, systematic behaviors that satisfy the requirements of privacy and security policies within a wide variety of contexts and implementation use-case scenarios.
The Internet provides us with more and more online services, virtualized online for our own convenience, which relieve us from cumbersome installation and configuration processes.

It is possible to write email, compose and share documents, virtually everything, without installing a piece of software in our computers beyond a web browser. However, as usual, such advantages also have a price to pay, in this case in terms of a potential privacy loss. For example, online email services usually scan and process our emails, sending us personalized advertisements and offering other potentially interesting (but usually undesired) services. …
Dr. Jose Manuel Gómez-Pérez  
R&D Director, Intelligent Software Components (iSOCO) S.A.

continued…

In general, the processes by which our own personal data are manipulated are often opaque to us, but citizens have the right to have knowledge of the logic involved in any process concerning their personal data (EU directive D 95/46).

These rights can only be enforced by a combination of legal but also automated means that analyze the provenance of the data [1] to support users in understanding such processes, are capable to determine what and by whom has been done with the data (attribution), and determine whether the processes are compliant with established contracts (accountability), while facilitating the analysis of the (potentially large and complex) processes by the users themselves (abstraction).

It is important to ensure that privacy is addressed as fundamental to the design and development of the ‘Future Internet’ as an aspect of maintaining the digital rights, dignity and sovereignty of the citizen.
Today, the need for Identity Management is present whenever the user needs to login or the provider needs information about the user.

Information, authentication and authorization should be consistent and act as the glue between the different applications the user interacts with.

This will be especially important in Network and Service Providers in relation to the user’s control of his/her identity and privacy.

In future Distributed Identity Management Platform the user should be able to deal with various services, specify the preferences regarding the information revealed, and especially within privacy policy enforcement with respect to usage of quest and with regards to the attribute provider’s privacy policy and user policies on what to disclose.
Antonio F. Gómez Skarmeta
Researcher, University of Murcia Spain UMU

- Future Identity Frameworks should provide privacy-enabled Future Internet using Identities such that user control is maximized at all layers

- User in the center of the control of its data and where they are stored and who use/access it

- More controlled privacy than today: Not letting technology dictate level of privacy (IP addresses in the network)

- The capability to establish zones of privacy as in real life

- Controlled linkability and identity disclosure for accountability

- Capability of “limited identities” for minors

- Identity, Privacy and Trust as a key enabler of a Citizen Living Use Case in Future Internet
Sam Coppens, Researcher and Ph.D. candidate in computer science and engineering at Multimedia Lab of Ghent

- Nowadays, the Internet has become such a big information space, people need technologies to filter out the information of interest. Examples are recommendation engines, RSS, social networks, etc.
- This leads to a situation where the Web has become a giant storage space for profile information on which the technologies rely to target the user with the information of interest.
- This profile information gets exchanged, even traded on the Internet like any other piece of information. People have no control anymore over this profile. The problem gets worse, because all this information is stored on a medium that has no expiration date. What ends up on the Internet, stays on the Internet. E.g., you can delete a photo on a certain social network, but chances are big it is already cached by some search engine, making it very hard to delete every trace of that photo.
- So, the users must recover full control over their profile information and this information, actually information in general, on the Internet should get an expiration date.
The Future of Privacy & Global Information Flows

- Substantive consumer protections facilitate global flows of information
  - Growing recognition that the opt-in vs. opt-out debate is insufficient.
  - Emphasis on the responsibilities of companies to comply with the full range of Fair Information Practice principles (FIPs).
  - Likely implementation of accountability programs, consumer access and control tools, and other mechanisms to both protect consumer privacy and encourage innovation.
- Recognition of these principles within the US and US government
  - US privacy bill is introduced and receives industry support
  - US Department of Commerce initiative emphasizes that privacy protections and global commerce and innovation are intertwined.
- Privacy protections should facilitate, rather than impede, free speech, the creation of user-generated content, and the proliferation of innovative platforms and services
Thank you

- Jon Peterson, Hannes Tschofenig and Bernard Aboba, Internet Architecture Board
- Rigo Wenning and Thomas Roessler, World Wide Web Consortium
- Kantara Initiative Privacy & Public Policy Work Group
- Gershon Janssen, OASIS (Organization for the Advancement of Structured Information Standards)
- Dr. Jose Manuel Gómez-Pérez, R&D Director, Intelligent Software Components (iSOCO) S.A.
- James Clarke, Program Manager / Project coordinator of INCO-TRUST, Waterford Institute of Technology, Future Internet Assembly ‘caretaker’
- Antonio F. Gómez Skarmeta, University of Murcia Spain UMU (RTSI ISG INS Partner) Identity and Access Management for Networks and Services (ETSI INS) ETSI Industry Specification Group (ISG)
- Antonio F. Gómez Skarmeta, Researcher, University of Murcia Spain UMU
- Sam Coppens, Researcher and Ph.D. candidate in computer science and engineering at Multimedia Lab of Ghent
- John Morris, Cynthia Wong, Alissa Cooper, Center for Democracy & Technology