The Evolution of Network Confidence
and Internet Society Trust and Identity Initiatives
INET Morocco – 10 May 2011
Lucy Lynch (lynch@isoc.org)
Tussles, Tensions, and Interdependence

The Internet was created in simpler times. Its creators and early users shared a common goal—they wanted to build a network infrastructure to hook all the computers in the world together so that as yet unknown applications could be invented to run there. All the players, whether designers, users or operators, shared a consistent vision and a common sense of purpose.

Perhaps the most important consequence of the Internet’s success is that the common purpose that launched and nurtured it no longer prevails. There are, and have been for some time, important and powerful players that make up the Internet milieu with interests directly at odds with each other.

“The Tussle in Cyberspace: Defining Tomorrow’s Internet”, Clark et al
The ISOC Trust and Identity Initiative

• The Internet Society's Trust and Identity initiative recognizes that in order to be trusted, the Internet must provide channels for secure, reliable, private, communication between entities, which can be clearly authenticated in a mutually understood manner.

• The mechanisms that provide this level of assurance must support both the end-to-end nature of Internet architecture and reasonable means for entities to manage and protect their own identity details.

• A trusted Internet takes into account security, transaction protection, and identity assertion and management. Trust must be a primary design element at every layer of the architecture, and in some cases, existing elements may need to be redesigned or improved to meet emerging requirements.
The Initiative includes three programs

• **Identity and Trust:**
  • Elevating "Identity" to a core issue in network research and standards development

• **Architecture and Trust:**
  • Implementing open trust mechanisms throughout the full cycle of Internet research, standardization, development and deployment

• **Operationalizing Trust:**
  • Mitigating the social, policy, and economic factors that may hinder development and deployment for trust enabling technologies
Internet Society and Network Confidence

• **Internet Society Objective:**

To actively promote and support standards and technologies that enable trust from the network layer to the application layer; encouraging policies that enable, extend, and strengthen confidence within the chain of network trust; and sustaining a culture of innovation and openness to create value for all stakeholders.

• **Trust & Identity Activities Supporting the Objective:**
  • **Understanding** the Trust Ecosystem
  • **Supporting** Open, Trust-Enabling Solutions (technical and policy)
  • **Advocating** for User Empowerment in Trust Exchanges
  • **Building** on Trust to Improve Network Confidence
Defining “Confidence” in the Network

• Confidence is:
  • The **belief** that one can have **faith** in or rely on someone or something.
  • **Self-assurance** arising from an appreciation of one’s abilities. The telling of private matters or secrets with **mutual trust**.
  • A secret or private matter told to someone under a condition of **trust**.

• Confidence in a network …
  • … results from **trust** developed through **positive interactions** experienced **over time**.
Requirements: Building the Trust Ecosystem

- A strong foundation built on open technologies, best common practices, and proven methodologies.
- All system participants cooperating as valued stakeholders.
- Operational transparency with integrated feedback loops allowing flexibility in fluid environments.
- Coordinated responses to emerging issues from all participants in the ecosystem.
- Functional frameworks that support deployments in varied markets and jurisdictions and across multiple platforms.

Effective expectation management:
- What is expected and what is delivered must match.
- A mismatch (in either direction) can be a disaster.
Achieving the Network Confidence Balance:
A Healthy Trust Ecosystem

Confidence in a functioning network requires balancing:

- **Security**
  - Transmission | Storage | Access | Usage
- **Privacy**
  - Agreement | Scope | Context | Consent
- **Transparency & Accountability**
  - Openness | Verifiability | Remediation
- **Exchange Value**
  - Generative | Authoritative | Minimizing Risk
- **Evolution**
  - Responsive | Flexible | Open to Innovation
The Classic Tussle:

Security VS Privacy
Cybersecurity (noun) ~

The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

http://oxford dictionaries.com/
Online Privacy...

... is not:

• secrecy or anonymity

... is:

• the ability to **selectively share** information within a specific context
• about the **appropriate handling** of information being shared
• highly influenced by **individuals’ expectations**
• fundamentally **contextual**, governed by societal norms, **often encoded** by law
• protected using **various tools** such as laws and technology
Online Privacy: *In Short*

Sharing (data) in an explicit *context* with an expectation of *scope*. 
Online Privacy: One Level Deeper

• Shared Data:
  • Provided Data (user-supplied, service delivered, co-created)
  • Observable Data (IP addresses, domain names, geo-location, etc.)
  • Hardware & Software Data (mac addresses, browser / OS details, etc.)

• Explicit Context:
  • Bounded Relationships (may require authentication, consent, etc.)
  • Terms and Conditions (transparency of use, notifications, etc.)
  • Limitations on Use (by first party and extended uses)

• Expectations of Scope:
  • User Settings (e.g. privacy controls, profile data, delegation, etc.)
  • Service Agreements (e.g. exchange models, monetization, etc.)
  • Portability (e.g. to transfer data, extract contacts, profiles, etc.)
Online Privacy: A Timely Topic

The rise of social networks and the growing use of data gathering and correlation to target users for both economic and security reasons has led to increasing concern.

Hot Topics for International Regulatory Bodies:

“Right to be Forgotten”
“Privacy by Design” & “Privacy by Default”
“Transparency” & “Informed Consent”
“Identification” vs. “Correlation”
“Data Minimization”
“Data Protection”
“Jurisdiction of Origin & Use”
“Online Activity Tracking”
“Defining Personal Data”
Online Privacy & User-Managed Identity

• **Users are key stakeholders** in the continued growth, utility and health of the Internet.

• Users engaged in the management of their identity helps ensure a high level of **confidence in the network**.

• **Key concepts** in user-managed identity include:
  • Distributed personal data – *a user’s data isn’t all in one place*.
  • Constrained data access – *users decide who sees what data*.
  • Delegated authorities – *users allow agents to act for them*.
  • Controlled privacy – *ability to manage levels of privacy protection*.
Privacy Overview: *International ISOC Member Survey*

- **Regional Differences Emerged, Including:**
  - **Societal** – Responses from Asia tended to focus on security of personal data.
  - **Regulatory** - Responses from countries with well-established privacy laws tended to be more specific with policy suggestions.
  - **Priority** - Respondents in countries with low Internet penetration prioritized connectivity over privacy concerns.
Privacy Overview: International ISOC Member Survey

• Emerging Challenges Included:
  • Data Durability – How to effectively manage long-lived personal data.
  • Economics of Privacy – What is the value of personal data, and how to balance the transborder flow of legal economic activity & privacy.
  • Ownership, Control and Responsibility – Who owns what data, how is it controlled, and who is the responsible party.
  • Surveillance – How to protect individuals from intrusive observation from governments and enterprise.
  • Transparency and Understanding – How to ensure adequate understanding of how personal data is collected and used.
  • Unauthorised Access and Use – How to address issues related to the illegal and/or unauthorised access to or use of personal data.
Network Confidence: Returning to the Balance

To balance privacy issues, we need many of the building blocks of basic security (data protection) to achieve our online privacy goals.

In the same way, usable security will depend on both flexible privacy protections for the user and verified network and browser exchanges.

The same holds true for reliability - In each case, we need to solve the tensions to reach ease of use.
Thank you.

Questions? Comments? Send them to:
Lucy Lynch (lynch@isoc.org)

The Internet Society:
- InternetSociety.org
- info@InternetSociety.org
Goals for the Trust and Identity work

• End users understand their options for identity management and demand appropriate tools and services to support the full range of use cases.

• Developers think in terms of trust, interaction, and sustaining global reach (end-to-end) when designing the next generation of reliance technologies and standards.

• ISOC continues to support the open, transparent, bottom up nature of Internet development and is an active partner in the standards process as the Internet Model expands.

• ISOC acts as a primary advocate for architectural issues that support and increase the value of the Internet as well as an active promoter of "best current practices" for the deployment of key Internet technologies.