The Public Policy Expert Group's Privacy Summit Programme

Robin Wilton
Corporate Architect (Federated Identity)
Sun Microsystems
robin.wilton@sun.com
+44 705 005 2931
http://blogs.sun.com/racingsnake
Objectives for this session:

- To review the Privacy Summit programme so far;
- To present some simple models of identity and privacy;
- To describe some of the knotty problems which remain...

A note of gratitude: this presentation is only possible because of the generous input of the Privacy Summit participants ... my sincere thanks to all of them, past and future.
The Privacy Summits have been hosted by the Public Policy Expert Group – one of four in Liberty:

- PPEG
- Technology Expert Group
- Identity Assurance EG
- Business and Marketing EG

Summits so far:

- Berlin (Feb 2007)
- Brussels (Apr 2007)
- Washington DC (June 2007)
- London (Feb 2008)
- Basel (Mar 2008)

Summits planned for Tokyo and Stockholm in 2008

The rationale is consistent, wherever we are:

- Today's (and tomorrow's) problems of digital identity and privacy cannot be solved by a 'single stakeholder' approach;
- The Summits gather people from the academic, legal, policymaker, technology and privacy spheres (and others), and enable each to contribute their perspective in an open and privacy-respecting forum.
Why is privacy such an issue, anyway?

- Identity data is a monetisable commodity.
- It is easy to transport.
- It makes crimes possible which cross borders and jurisdictions.
- The 'at risk behaviour' and the adverse consequences are often remote from one another in time and place.
- The internet is now often, by default, an indelible medium.

Interviewer: “Why do you rob banks?”
Interviewee: “Because that's where the money is”
Attributed (apparently apocryphally) to Willie Sutton* (1901-1980)

*Two interesting things which are true about Willie Sutton:
- He made frequent use of disguises in his robberies
- He later advertised a bank's 'face card' as an anti-theft measure
... so he clearly had a shrewd grasp of identity management

And a slightly more recent headline:

“Google resolve crumbles on 'cookies' pledge”
Financial Times front page, 21/4/2008
How to leave a permanent mark (C20\textsuperscript{th} version)

- The Politics
- The Economy
- The Technology
- The Atmosphere (none)
In the 21\textsuperscript{st} Century:

- It no longer takes a moon-shot to leave a permanent footprint...

... but we often assume that we are leaving no trace.
How to leave a permanent mark (C21st style):
... just nip out to the shops.

(I collected this free newspaper while approaching what is probably the most heavily surveilled public space in Europe...)
Why is digital privacy hard? (The Stakeholder Model)

Policymakers express frustration that privacy can't just be “built in at the technology layer”

Technologists are often unpleasantly surprised by regulatory/legal requirements which affect the solution

The rights and interests of the data subject can often seem to be very low down the list of priorities...

Implementers can't see why so much time, effort and money still fail to address the actual issues...

Digital identity and privacy raise complex, multifaceted issues with a multiplicity of stakeholders
Why are privacy discussions difficult? (The Ladder Model)

Privacy

Data 'ownership'

“The Interesting Stuff”

Trust

Legal, regulatory, commercial and technical implementation factors

Basic terms and conceptual framework

Technology

- There's a great deal of work and progress in all of these lower layers... although stakeholder engagement and communication is often patchy.
- It's all too easy to fail because of fractures or constraints from layer to layer...
So What Is 'Identity Data'...? (The Onion Model)

- The BIS (Basic Identifier Set) is what usually suffices to provide 'proof of uniqueness'.
- Credentials usually encapsulate data from multiple 'rings' of the onion.
- There is usually a further index value (such as an Identity Number) which may merit specialised treatment, legally, technically or both. It probably should not be treated as a credential...

One 'good practice' approach to digital credentials suggests that they should 'gravitate' towards the centre of the onion – i.e. not be overloaded with attribute data, but provide the means to link to it.
The “Onion” model (2)

- A 'segment' of the onion may correspond to sector-specific data (healthcare, tax, employment ...)
- Sectors often have their own credentials (passport, driving licence)
- Some sectors are entirely 'informal' – such as the separation between your Flickr and MySpace accounts
- One way to look at privacy is as the preservation of “contextual integrity” between sectoral data sets. (*With thanks to Piotr Cofta of British Telecom*)
- *If that's the case, then privacy is usually not a 'state', but a relationship – involving multiple parties.*
Technology and policy: a fluid borderline (The Silo Model)

One-way hashing function

"Global" ID

"Sectoral" ID #1
"Sectoral" ID #2
"Sectoral" ID #3
"Sectoral" ID #4

Context

Data-sharing Context

© Copyright Sun Microsystems March 2008
The Privacy Paradox

• It turns out that what we often mean by “privacy” is actually “disclosure”... but disclosure within a certain context, and with specific assumptions about consent and control;

• It's hard to exercise consent and control if you think you are just 'leaving a sandprint on the beach'...

• *Either* it no longer takes a moon-shot to leave a permanent footprint... *or*, put another way, we all have the means to do our own 21C moon-shot.
Further exercises for the reader...

However, there's still a lot to be investigated further:

- Protection 'beyond first disclosure'
  - Privacy preference expression and enforcement
  - Ephemerisation of data
- Technical convergence vs. semantic interoperability
- Improving contextual integrity, consent and control

In other words -
How can we make it easier for data subjects to understand and manage their digital footprints?
Summary

- The Liberty Alliance Privacy Summits are an ongoing programme;
- Some progress to date has already been documented – more Summit reports are still to come;
- There are still substantive questions to address;
- The 'Ladder', 'Onion' and 'Silo' models help get a productive discussion going;
- So far, the Ladder has always led somewhere interesting.

- Here's where to go for more information – or please email me with comments/queries/suggestions.
  http://www.projectliberty.org/liberty/public_community/privacy_summits
Thank You

Robin Wilton
Corporate Architect (Federated Identity)
Sun Microsystems
robin.wilton@sun.com
+44 705 005 2931
http://blogs.sun.com/racingsnake