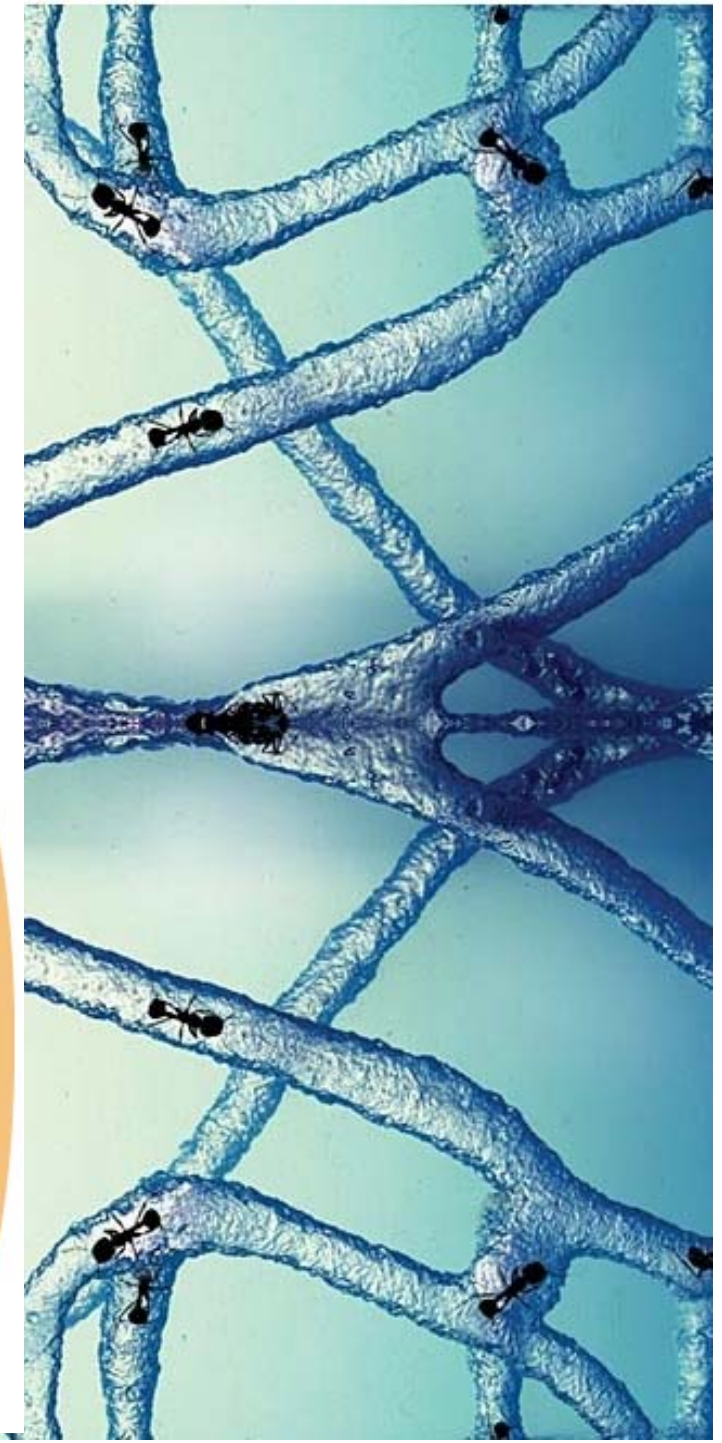
Net-ID 2007
Berlin

Privacy and Identity



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

Aim of this presentation

- To recap last year's main topics
- To build on them for a more detailed look at online privacy
- To sketch out some of the issues and challenges we will have to address as we go forward

- To answer this question:

Are we surfing naked on the information wave?

Topics

- Net-ID 2006 recap – Identity and Identity Theft
- Net-ID 2007 themes – Privacy and Identity
- Privacy in real life; privacy in the online world
- Some key questions
- Implementation options and issues

Net-ID 2006 (Identity Theft)

- Identity theft and identity fraud have a definable life-cycle;
- This life-cycle can be analysed in terms of the 'attack vectors' for each step;
- Simple models can also be constructed for
  - The Elements of Identity
  - The Lifecycle of Credentials
  - The 'Chain of Trust' on which authentication relies
- Identity theft prevention requires a set of related disciplines, including policy, technology, best practice and cultural measures.

Net-ID 2007 - Identity and Privacy

- As before, some simple models can help us analyse the problem;
- What significant differences are there between real-world and online privacy?
- What could/should we do differently?
- What are the current technical, implementation and cultural issues?

I'm pleased to make your acquaintance...

- I am a systems architect
- I work for Sun
- I am interested in identity, privacy and policy issues
- I live in England
- My boss is about 9000km away

- I like the music of Scarlatti
- I never eat offal (kidney, liver etc.)
- I think factory farming of animals is wrong
- I would probably like books by Arnaldur Indriðason

What's the difference...?

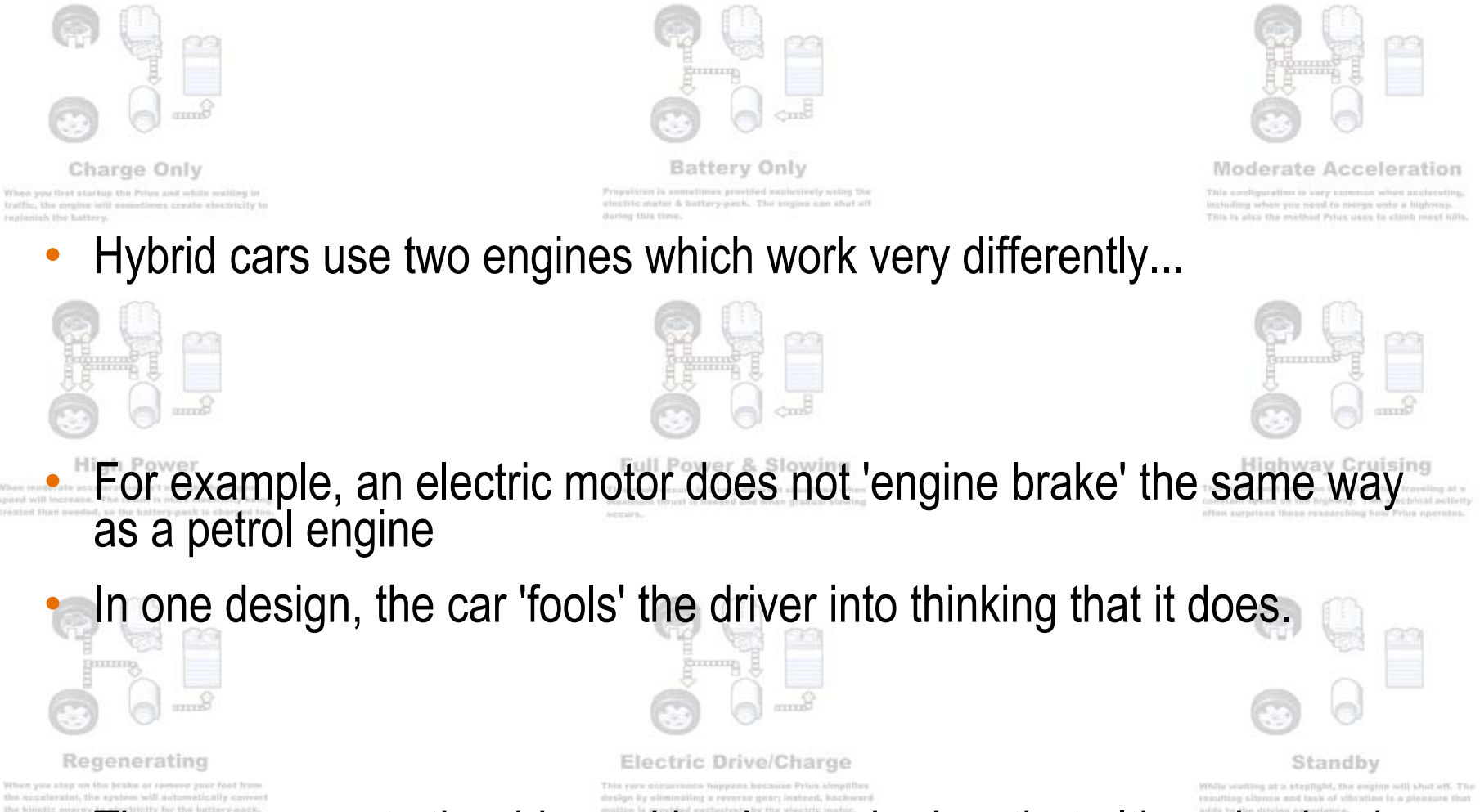
In real life:

- Information disclosure is often deliberate
- We tend to know when we are doing it, and to whom
- It usually generates feedback
- We adjust our behaviour accordingly over time
- Disclosure is contextual
- There is “friction” which acts as a brake on disclosure

Online:

- We may not be conscious that we are disclosing information, or to whom
- 'Behaviour' data is much easier to collect
- We get little or no feedback
- Bad behaviour seems to have no consequences!
- “Frictionless” transactions may mean frictionless disclosure

A (kind of) product plug



- Hybrid cars use two engines which work very differently...
- For example, an electric motor does not 'engine brake' the same way as a petrol engine
- In one design, the car 'fools' the driver into thinking that it does.
- The car presents the driver with a 'metaphor' so that although what is *really* happening is different, it appears to be working the same way.

The Challenge We Face

- The online world neither works like, looks like nor behaves like the real world;
- The online world often presents us with metaphors, but not ones which would help us overcome these differences.
- We therefore frequently base our behaviour on a flawed perception of risk.

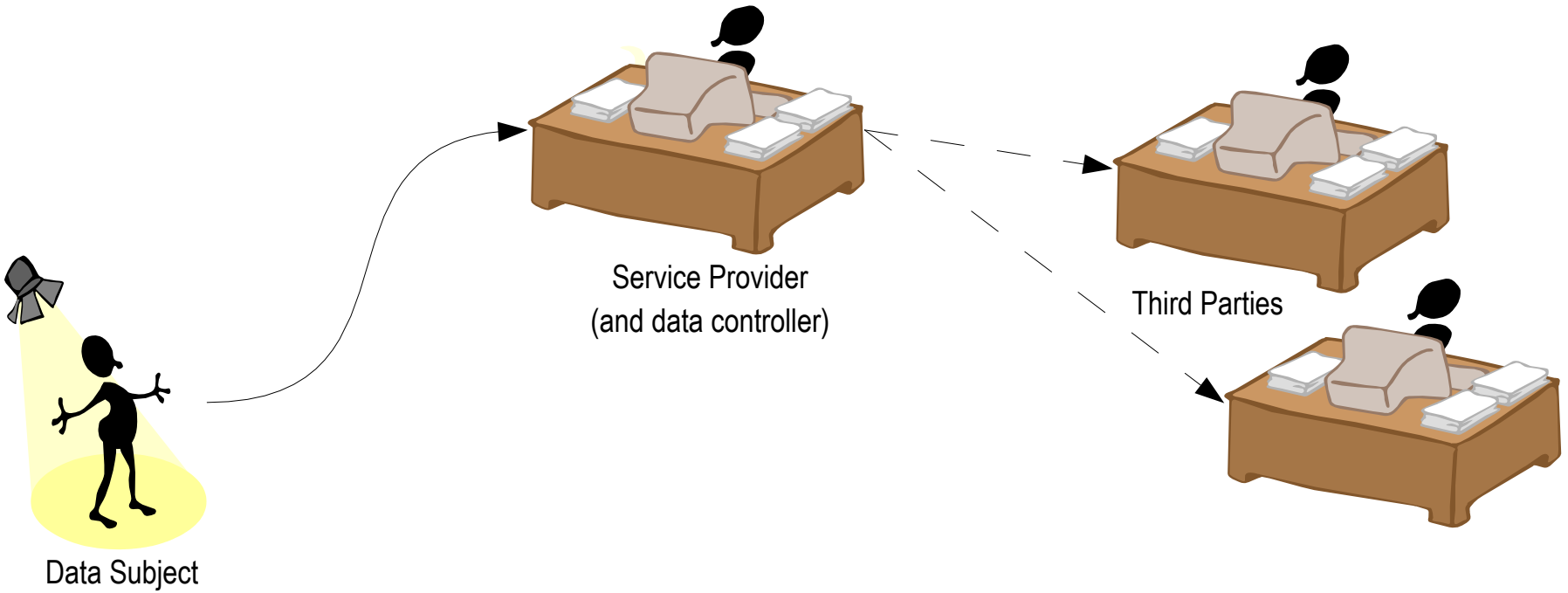
In other words, we could be surfing naked and not even know it. Brrr.

Some technical and design options

- The concept of a 'persona' may be useful:
  - A subset of identity/personal information which we choose to expose, according to context
  - This includes anonymity and pseudonymity... both of which can also have a 'dark side'
  - What PRIME refers to as a 'partial identity'
- Many of us already use personas on line:
  - Email addresses, user-names, avatars, etc.
- The ability to use a persona implies user consent and control over their identity data and its disclosure... whether that data is held by the user, or by some other party (such as an Identity Provider or an Attribute Provider)

In my view 'user centric identity' has more to do with this than with protocol flows and where the data is held.

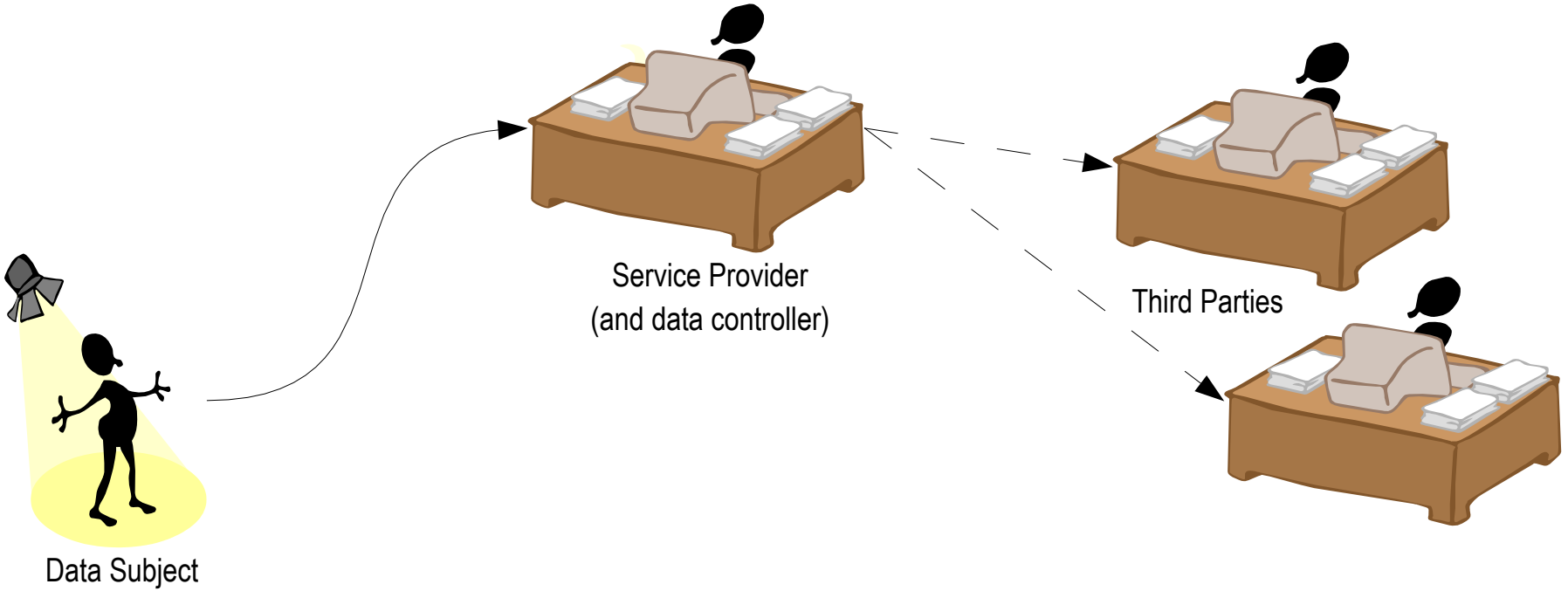
The issue of 'maintaining control'



Contractual Protection, Privacy Policy/Preferences	Non-technical Protection - discretionary?
Technical Protection, Policy Enforcement	Technical Protection - available?

Whether technically or contractually, policy is still not very 'persistent'...

Is a technical approach viable?

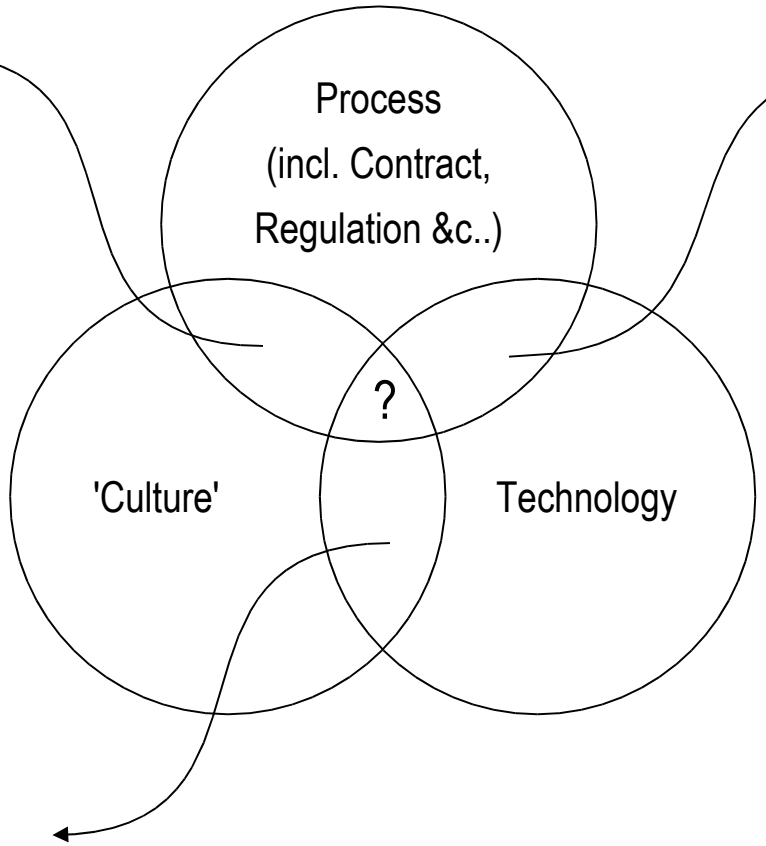


Privacy Preference Expression →	Privacy Preference Enforcement
Purpose of Use (or Disclosure) →	Purpose of Collection

However, Purpose of Use and Purpose of Collection are often expressed very differently...

Is there a privacy 'sweet spot'?

Consensual
(purely contractual
or best practice)



Compulsory
(e.g. User consent
is not sought)

“Bottom up” -
(e.g. User-generated
assertions)

Some Advantages of a Federated Approach

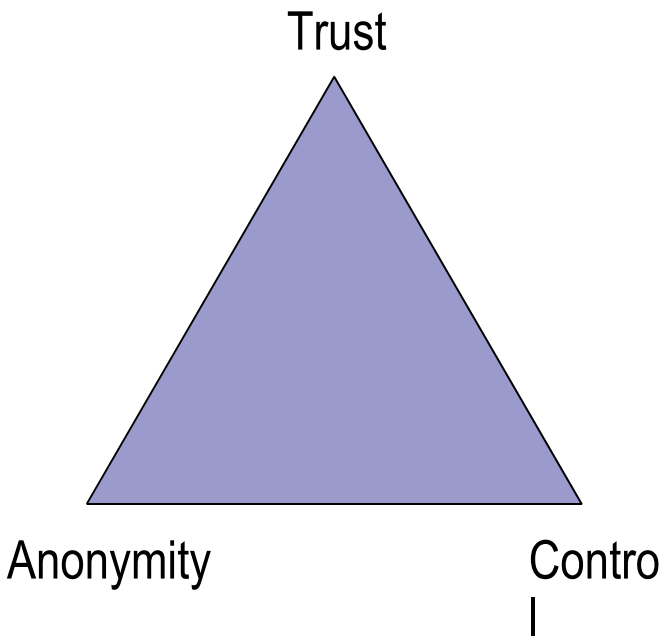
- Experience shows that multi-party federation only works if proper attention is also paid to the non-technical framework
- Permission-based exchange of user attributes (allows user consent and privacy to be addressed)
- Reduced need to move sensitive data from place to place
- The federated model provides a much better online analogue for 'real-world' trust relationships

But...

- More investigation is perhaps needed of 'policy persistence'

Some Closing Thoughts ...

- Consent
- Roles
- Personas



- *Most instances of identity theft happen when the subject's data is outside their control*
- *Third party 'assertions' are a key part of online interaction*
- *What happens when you remove someone's ability to have secrets?*
- *Just like identity theft, privacy requires a holistic approach:*
  - Legislation, Regulation, Best Practice, Technology, Process and User Behaviour are all factors

Net-ID 2007
Berlin

THANK YOU

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