Burton Group Catalyst Conference
San Diego, July 2009

Privacy: How to have a productive multi-stakeholder discussion

Robin Wilton

Director, Future Identity Ltd
Director of Privacy and Public Policy, Liberty Alliance

kantara INITIATIVE™

Future identity

“Of Ladders, Onions, and Surfing Naked...”

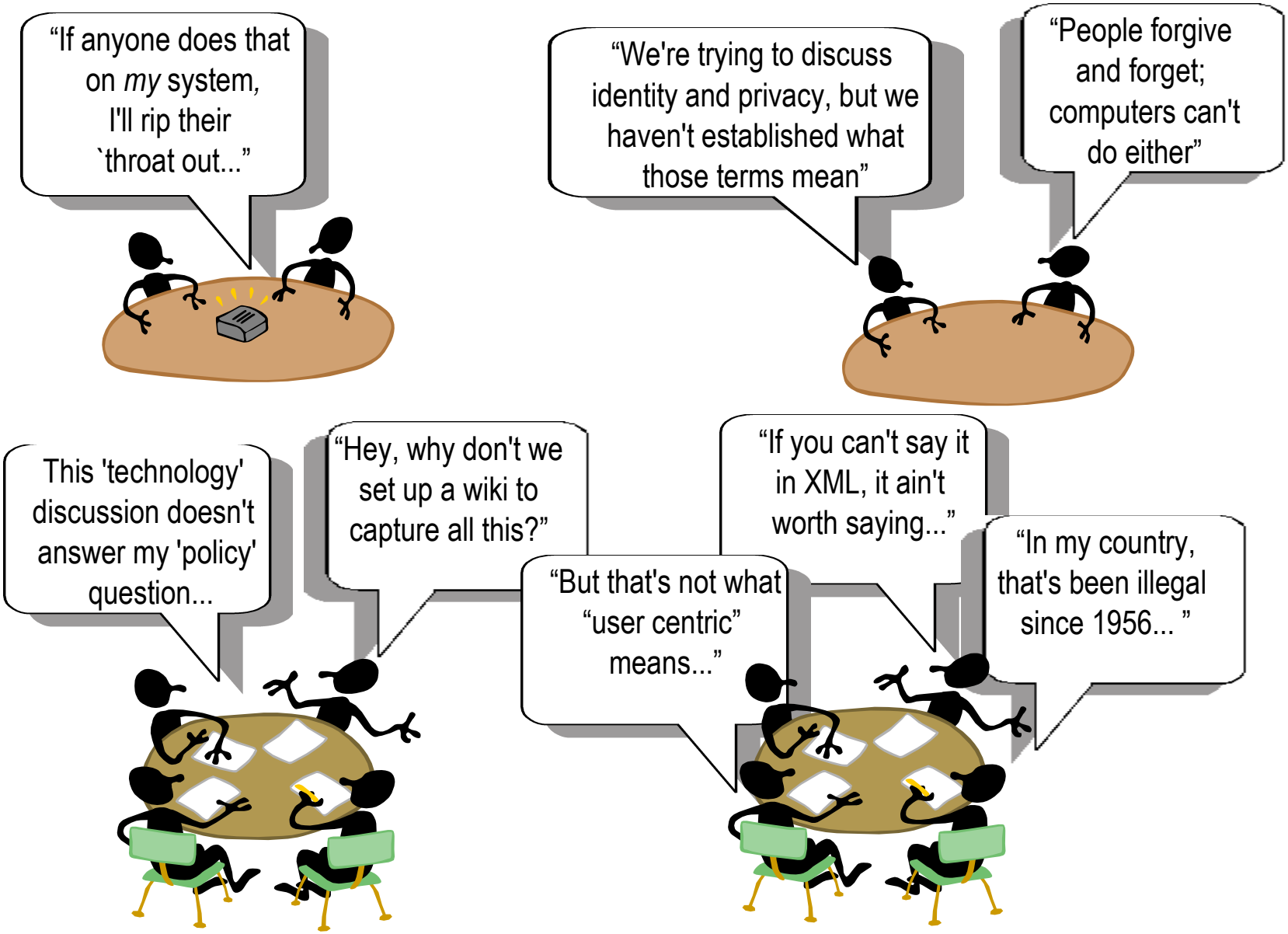
Objectives for this session:

- What is privacy anyway, and why is it important?
- What's the “multi-stakeholder” problem?
- How can your organisation overcome it?

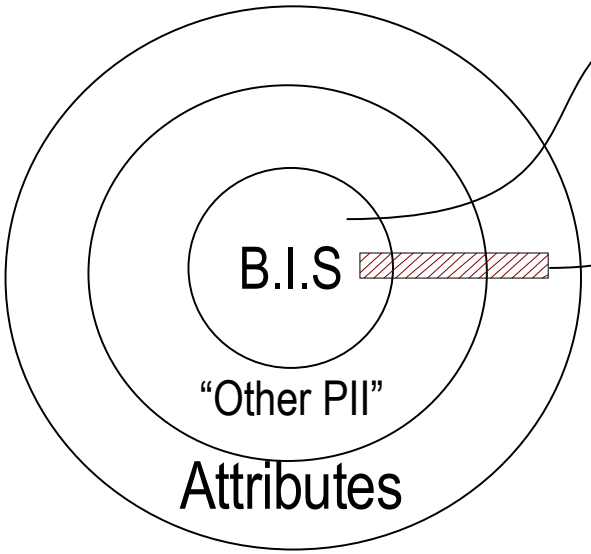
A note of gratitude: this presentation is only possible because of the generous input of participants in the Liberty Alliance Privacy Summit programme -

My sincere thanks to all of them

Does any of this sound familiar?



How are identity and privacy related? (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
- One 'good practice' approach to digital credentials suggests that they should 'gravitate' towards the centre – i.e. not be overloaded with attribute data, but provide the means to link to it.

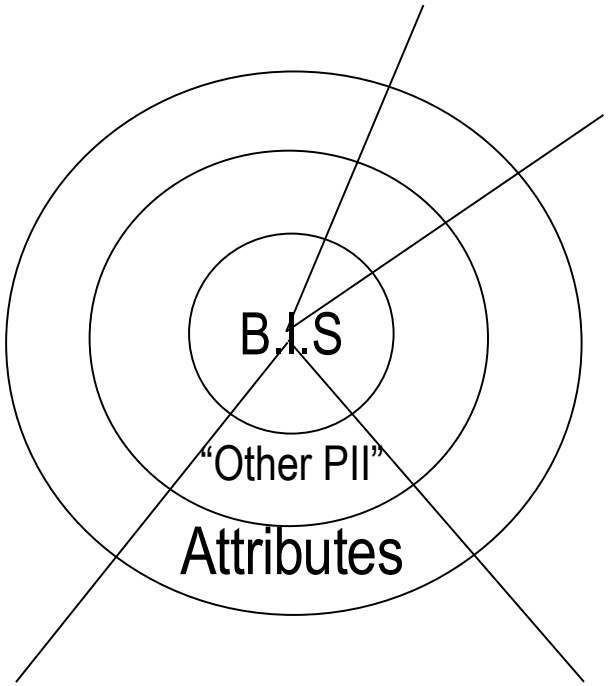
Credentials are not privacy-neutral

- e.g. Using a driver's license to prove your age reveals more than your age;
- By their nature, credentials tend to make transactions 'linkable';
- Privacy-enhancing systems will (must) be better at attribute-level disclosures, or better still, "Yes/No" answers to attribute-level questions.

(cf. Dave Birch's paper on the "Psychic ID" metaphor)

How are Identity and Privacy related? (2)

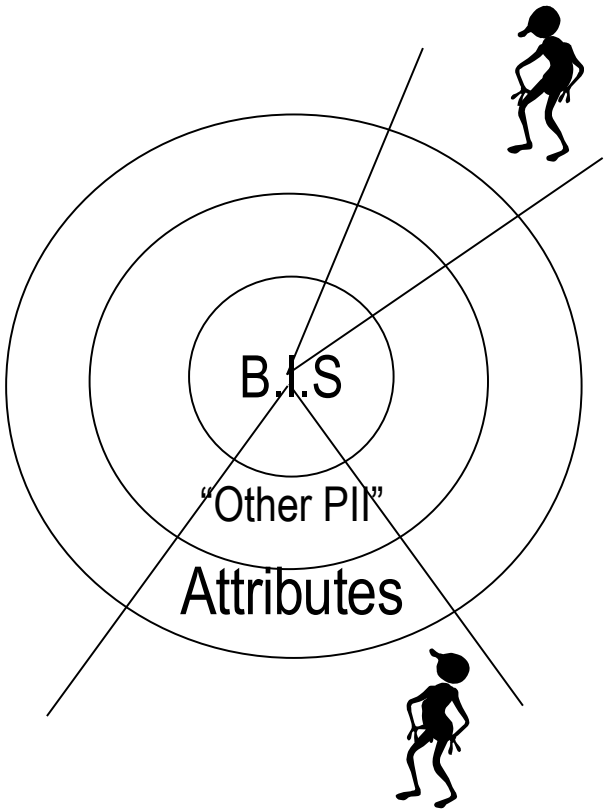
There's no such thing as a shared secret...



- A 'segment' of the onion may correspond to sector-specific data (healthcare, tax, employment...).
- Some sectors are entirely 'informal' – such as the separation between your Flickr and MySpace accounts.
- Others, you might prefer to keep strictly separate.
- 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)*

We become uneasy if our personal data shows up 'out of context'...

What risks does this model suggest?

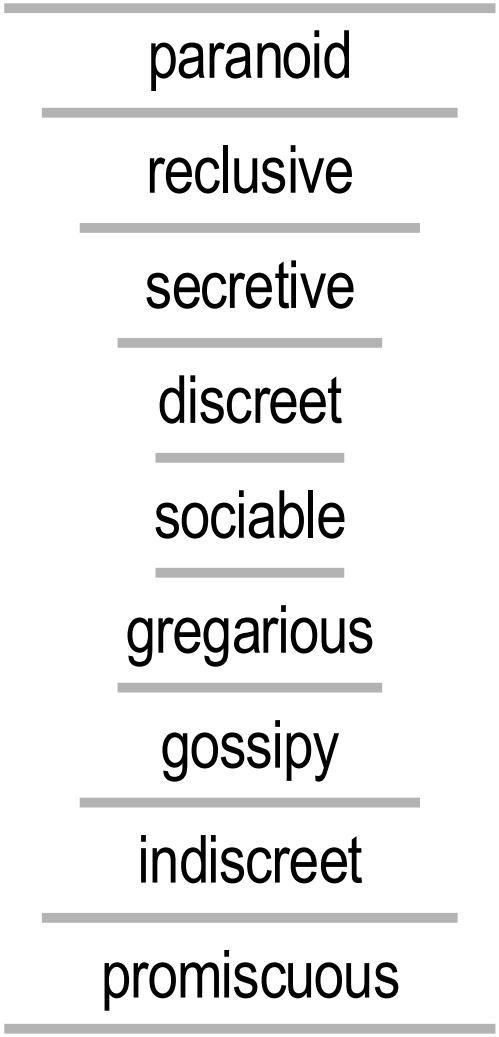


- Privacy is not a 'state': it's a relationship, often involving multiple parties;
- Like any relationship, it involves conflicting interests and motivations:
- What we tell different people often depends on context;
- Like any relationship, there are rules – mostly implicit:
- When third parties exchange (your) personal data, is that co-operation or collusion?
- Like any relationship, without maintenance and management it may go awry.

Intuitively we know all these things, because humans are social animals...

and yet ...

The Great Privacy Experiment



- Most humans are effortlessly sensitive to many kinds and qualities of social interaction;
- We manage our real-life relationships accordingly;
- We (often implicitly) rely on contextual factors...

In "social networking", we often ignore all that expertise and carry on regardless...

Conclusion:

- You can have 'social interaction' and 'networked interaction'... but if you behave as if they are the same, you're fooling yourself...

Flawed Perceptions

- The online world neither works nor behaves like the real world;
  despite occasional appearances to the contrary...
- The online world often presents us with metaphors, but not ones which would help us overcome these differences.
- We therefore frequently – and willingly - base our behaviour on a flawed perception of risks and the reality which gives rise to them.

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

Getting the Privacy 'Big Picture'

- “Privacy management” implies being aware of relationships and contexts, and acting accordingly;
- It means taking diverse, legitimate stakeholder perspectives into account;
- It needs a new set of metaphors, which help build a privacy-enhancing culture: 'protocol rules' are not the same as 'social rules';
- It will involve privacy-enhancing technologies, but those are doomed without a privacy-enhancing ecosystem of governance, adoption and behaviours which, largely, remain to be developed ;
- That's hard to do, if you're not talking to the stakeholders...

Privacy is not about secrecy: it's about disclosure...
but disclosure with consent and control
appropriate to the context.

Why is data privacy hard? (The Stakeholder Model)

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

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

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

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

And a changing picture of over-arching problems -

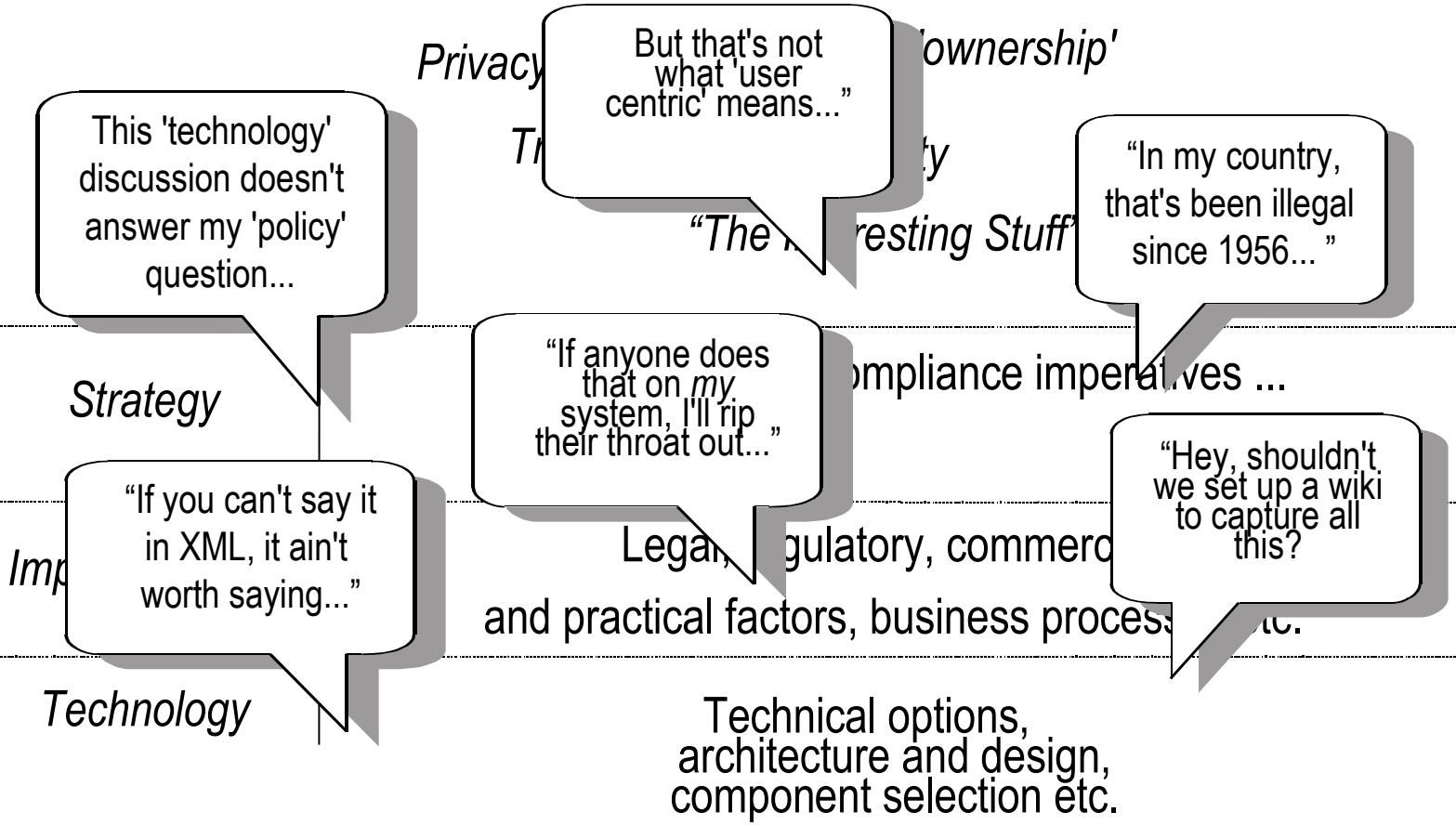
- *Legacy of "over-collection";*
- *Increased linkability;*
- *Economic pressure to 'sweat the information asset';*
- *'Variable' appetite for regulatory compliance.*

Why are privacy discussions difficult? (The "Ladder" Model)

Philosophy	*Data 'ownership'* *Privacy* *Identity* *Culture* *Trust* *"The Interesting Stuff"*
Strategy	Policy, Business, Compliance imperatives ...
Implementation	Legal, regulatory, commercial and practical factors, business processes etc.
Technology	Technical options, architecture and design, component selection etc.

- *There's a great deal of work and progress in all of these lower layers... although stakeholder engagement and communication are often patchy.*
- *It's all too easy to fail because of fractures or constraints from layer to layer.*
- *It's healthy to remember that only a minority of the stakeholders are technologists.*

Using the 'Ladder' to manage contributions to the discussion



- *Some causes of frustration in multi-stakeholder discussions:*
  - *"Right contribution, 'wrong' moment..."*
  - *"Giving a 'technology' answer to a 'policy' requirement..." (or vice versa)*
- *Record such contributions at the appropriate 'layer' and come back to them in context.*

Next Steps...

- Break out of 'monoculture' discussions;
- Manage diversity in your stakeholder engagement;
- Prepare to do a great job of mapping “human” privacy onto the online world!

And remember...

- There are proven ways of approaching these issues, and Kantara's Privacy and Public Policy group is there to help -

http://kantarainitiative.org/confluence/display/WGPRIV/Home

Burton Group Catalyst Conference
San Diego, July 2009

Thank you...
... any questions?

Robin Wilton
Director, Future Identity Ltd
Director of Privacy and Public Policy, Liberty Alliance

futureidentity@fastmail.fm
+44 (0)705 005 2931

http://futureidentity.eu
http://futureidentity.blogspot.com

Future identity