

Butler Group Strategy Briefing  
June 3<sup>rd</sup> 2009  
London



# Information Security in an Economic Downturn

Robin Wilton

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

[mail@futureidentity.eu](mailto:mail@futureidentity.eu)  
+44 (0)705 005 2931  
<http://futureidentity.blogspot.com>

# Agenda

- Why me? - Future Identity's stakeholder engagement strategy
- Principles
- Policies
- Practicalities
- Problems to solve ...

# Why me?

- Future Identity Ltd: founded Jan 2009 on 25 years' experience
- Previous posts at IBM, JCP and Sun Microsystems
- Most recently Sun's Corporate Architect for Federated Identity
- Liberty Alliance Public Policy Expert Group (co-chair, '06-'08)
  
- Now consulting to public sector and Kantara Initiative
- Director of Privacy and Public Policy, Liberty Alliance
  
- Particular focus on privacy, and the policy/technology interface
  
- Laying the groundwork for Kantara Initiative's  
“Privacy and Public Policy Work Group” (P3WG)

# Future Identity's Stakeholder Engagement Strategy

- Key constituencies:
  - Policymakers
  - Adopters
  - Regulators
- The neat trick is often translating successfully between them

• Policymakers – define the privacy landscape we must inhabit and cross

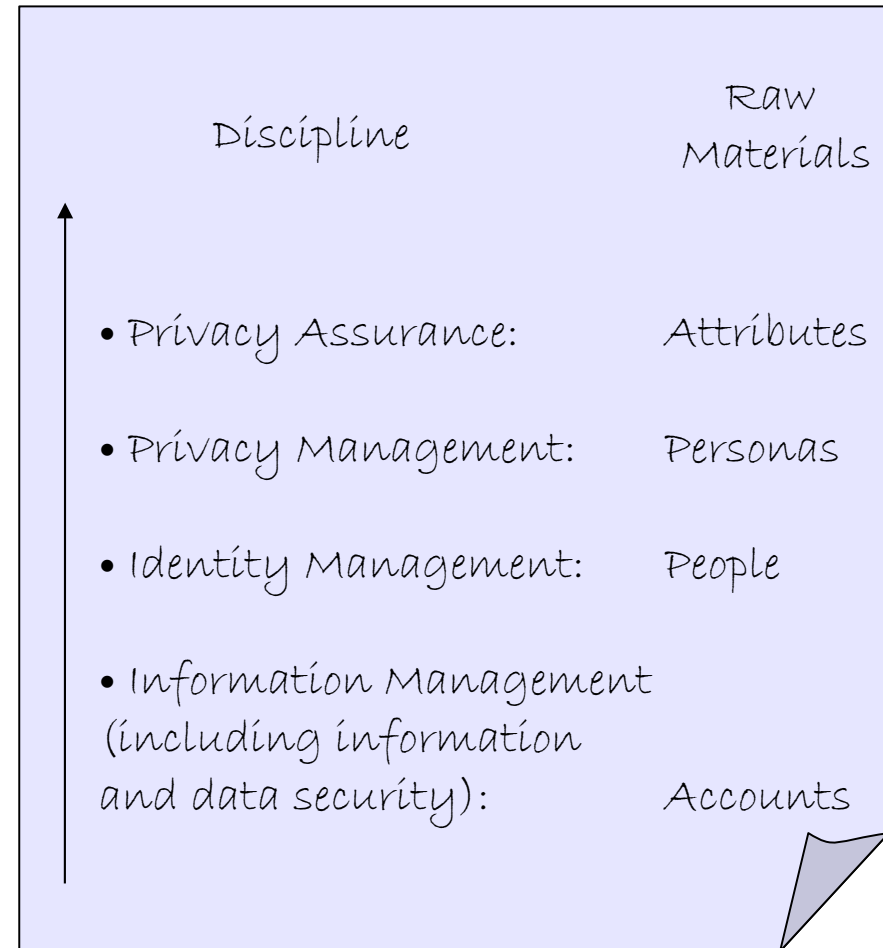
• Adopters – (CPOs, users...) – have to resolve the tension between motivation and risk

• Regulators – are our protection against poor policy, inadequate legislation and flawed adoption (including 'toxic' market forces)

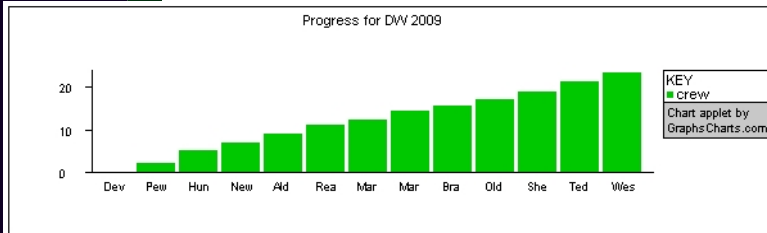
Ignoring any of these stakeholder communities leads to worse privacy outcomes ...

# What's the intersection between 'information security' and 'privacy'?

- A Maslovian hierarchy of information and disciplines:
- It's hard to address the upper layers without competence in the lower layers;
- In practice, “progress” usually means “unlocking the next set of problems”



# All else being equal...



## Progress for crew 529: Newman & Wilton (Dauntsey's School & Independent)

Location	Distance	Time	Elapsed time
Devizes	0	Fri 07:57:18	00:00:00
Pewsey	12	Fri 10:09:00	02:11:42
Hungerford	25	Fri 13:12:00	05:14:42
Newbury	34.5	Fri 14:59:44	07:02:26
Newbury	34.5	Sat 07:56:50	07:02:26
Aldermaston	43	Sat 10:00:00	09:05:36
Reading	54	Sat 12:01:00	11:06:36
Marsh	61	Sat 13:20:00	12:25:36
Marlow	70	Sat 15:10:29	14:16:05
Marlow	70	Sun 07:40:43	14:16:05
Bray	79	Sun 09:03:00	15:38:22
Old Windsor	87	Sun 10:37:05	17:12:27
Shepperton	97	Sun 12:22:00	18:57:22
Teddington	107.5	Sun 14:34:56	21:10:18
Teddington	107.5	Mon 06:33:00	21:10:18
Westminster	125	Mon 08:44:10	23:21:28

to westminster! [home](#) - browse by [class](#) or [team](#)

**2009 / 529** Alexander Newman & Anna Wilton  
Endeavour

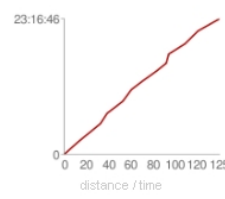


Times for Alexander Newman (Dauntsey's School) and Anna Wilton (Independent).

Location	Time	Distance	
Start	Devizes	Fri 07:57:18	0.0
	Pewsey	Fri 10:09:00	11.5
	Hungerford	Fri 13:12:00	29.0
	Newbury	Fri 14:59:44	34.5
Day 2	Newbury	Sat 07:56:50	34.5
	Aldermaston	Sat 10:00:00	47.0
	Reading	Sat 12:01:00	54.0
	Marsh	Sat 13:20:00	62.0
	Marlow	Sat 15:10:29	74.0
Day 3	Marlow	Sun 07:40:43	74.0
	Bray	Sun 09:03:00	82.0
	Old Windsor	Sun 10:37:05	84.0
	Shepperton	Sun 12:22:00	97.0
	Teddington	Sun 14:34:56	107.5
Day 4	Teddington	Mon 06:33:00	107.5
Finish	Westminster	Mon 08:44:10	125.0

**10th**  
23:16:46

**5.370 mph**  
average speed



a canoe/data mash up, curated by [mza](#) - all timings are provisional - official times and positions at [dwrace.org.uk](#)

- ... it is cheaper and easier to:
- Store vs. destroy (especially selectively)
  - Share vs. compartmentalise
  - Aggregate vs. segregate
  - Visualise vs. conceal

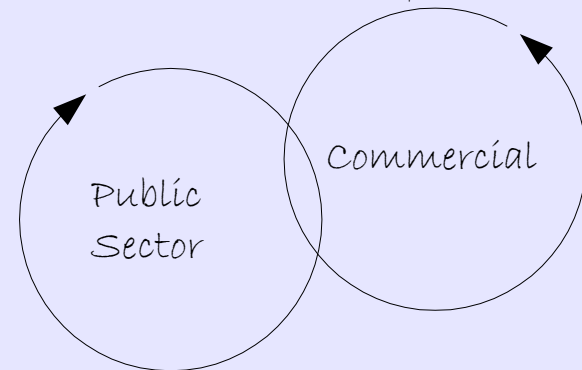
Technology tends to reinforce this trend.

*The principal counter-force is governance, which is people-intensive, and expensive, and suffers accordingly when money is scarce.*

# However, all else is not (currently) equal ...

- IT vendors and adopters are used to:
  - Decades of growth;
  - Sustained investment;
  - A “price/performance” equation to match;
  - The innovation “ecosystem” all this combines to create.
- We now have to adapt to:
  - Changed assumptions
  - Shifts in balance
  - New tensions

- Reduced commercial activity
- Reduced revenues
- “Sweat” assets – including personal data
- Pressure to reduce 'cost of compliance'



- Reduced economic activity
- Reduced tax revenues
- Pressure to reduce 'cost of collection'
  - CCTV parking fines
  - Speed cameras, ANPR
- Automate, and process only exceptions

None of these factors makes more, or better governance more likely ...

# The Balance of Technology and Governance

- Failures of process and culture take more sustained effort to address.
- A technical ('quick') fix is soon trumped.

Distorted cost/risk equation:

- Extracting 500 records from 25 million;
- Process for applying security technology;

vs.

- Disclosing all records.

Cost was immediate; risk was remote in time and place...

The screenshot shows the ComputerWeekly.com website. The main article is titled "HMRC data breach highlights need for data compliance" by Jeremy Smith, posted on 15:40 04 Jan 2008. The article text states: "The data breach at HMRC, which placed 25 million people at risk of identity theft, has brought information governance back to the fore. Early indications suggest that risk management procedural failures and human error were to blame." Below the article, there is a quote: "Those risk managers who fail to take data security seriously run the risk of being on the receiving end of heavy financial losses and often fines. Securing personal information is not just savvy commercial practice, but it is a legal requirement." The article is categorized under "Risk Management" in the "IT MANAGEMENT" section. A sidebar on the left lists various IT management topics, and a "SIGN UP TO" button is at the bottom. A logo for HM Revenue & Customs is visible on the right side of the article.



# Policy: how might it shape the landscape?

## ❖ Cost:

- One policy response is to offload cost (e.g. to industry)

## ❖ Risk:

- What happens to risk in this model? Who 'owns' the problem, and who *feels* responsible?

## ❖ Regulation:

- Regulatory picture changes from being centralised and 'internal' to being distributed among multiple (commercial) third parties.

## ❖ Technology:

- Heterogeneous, 'market led';
- Doomed if cost, risk and regulatory factors are not addressed.



The screenshot shows the BBC News website interface. At the top, the BBC logo is on the left, and navigation links for 'Low graphics' and 'Help' are on the right. A search bar is also present. Below the logo, the word 'NEWS' is displayed in large letters, followed by a 'LIVE' indicator and 'BBC NEWS CHANNEL'. The main content area features a navigation menu on the left with categories like 'World', 'UK', 'England', 'Northern Ireland', 'Scotland', 'Wales', 'Business', 'Politics', 'Health', 'Education', 'Science & Environment', 'Technology', 'Entertainment', and 'Also in the news'. The 'Politics' category is highlighted. The main article is titled 'Plan to monitor all internet use' by Dominic Casciani, a BBC News home affairs reporter. The article discusses the Home Secretary's decision to scrap plans for a database of internet contacts, instead focusing on modernising police surveillance tactics. A quote from a source is included: 'Communications data is an essential tool for law enforcement agencies to track murderers and paedophiles, save lives and tackle crime'. A small image of a Facebook logo is also visible on the right side of the article.

# Practicalities: Governance Revisited

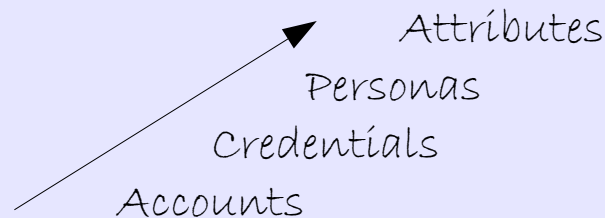
- Requirements may be:
  - Country-specific
  - Industry-specific
  - Cross-industry and cross-border
- Industry response is sometimes to pre-empt regulation (e.g. Binding Corporate Rule)
- Whether externally imposed or internally adopted, governance assumes healthy disciplines (technical, procedural, cultural...)
- As before, a hierarchy can be sketched out.

Discipline	"Raw Materials"
• Privacy Management:	Ethical principles
• Identity Assurance:	LoA, Risk, Contractual Frameworks
• Identity Management:	Joiners/Movers/Leavers, Roles
• Information Management (including information and data security):	Good practice e.g. BS7799, PIAs, Audit, Inventories of PII ...

# Exercises for the reader (there are still plenty to go round...)

- Balance of technology and policy

- Climbing the hierarchy:



- Managing contexts & relationships

- Metaphors, metadata and 'sticky policy'

- Requirements may be:
  - Country-specific
  - Industry-specific
  - Cross-industry and cross-border

- In the hierarchy, there's always something to aspire to...

- Some of these problems are yet to be comprehensively defined, let alone solved...

# Conclusions

- Principles:
  - Well-defined, or definable
  - Often philosophical/ethical in nature
  - Need to account for all the stakeholder groups
- Policy:
  - Likely to be tested by recession/recovery
  - Pressure will be on to cut (or outsource) cost
  - Governance measures will feel the pinch
- Practicalities:
  - Disciplines further up the hierarchy are still being developed (identity assurance, privacy management)
  - A road-map can be drafted, though
  - What is practical depends on context and adoption readiness
- Problems: still plenty of scope for innovation, if the economic climate permits it.





# Thank You

Oh... and that P3WG:  
Interested? See me...

<http://kantarainitiative.org>

Robin Wilton

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

[mail@futureidentity.eu](mailto:mail@futureidentity.eu)  
+44 (0)705 005 2931  
<http://futureidentity.blogspot.com>

