

Identity and Privacy Personal Data Guardianship

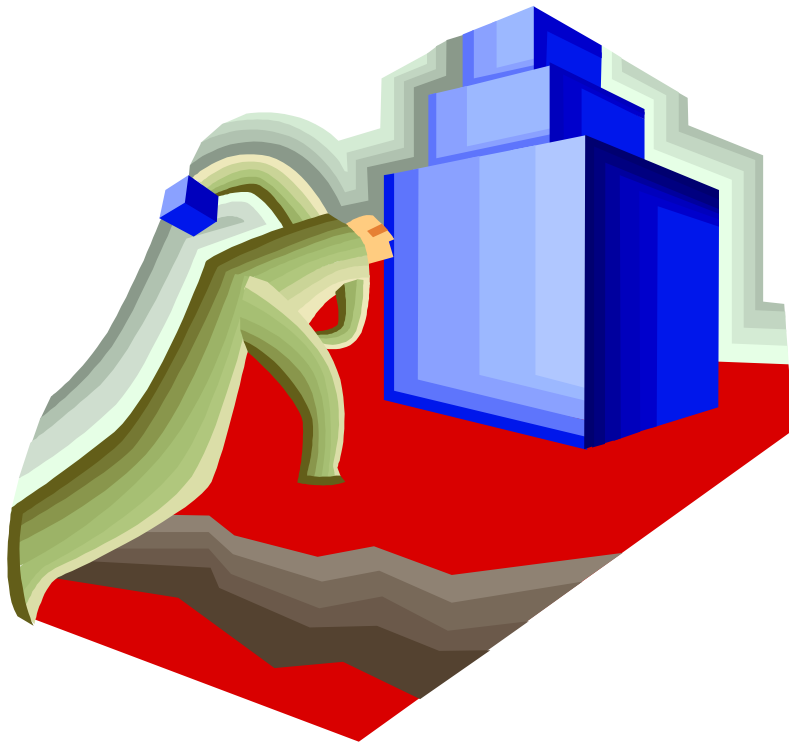
14 May 2009

Louise Bennett

Three questions

1. What is private data in the electronic age?
2. What is the place of identity management in good data guardianship?
3. How will people behave if they understand data guardianship?

Privacy in the electronic age



1. Practical obscurity has gone
2. Your electronic footprint is impractical to erase
3. Context is all important with regards to privacy

Context and data linkage



1. Privacy is compromised by linkage
2. Address and job, when linked can make you a victim of activists

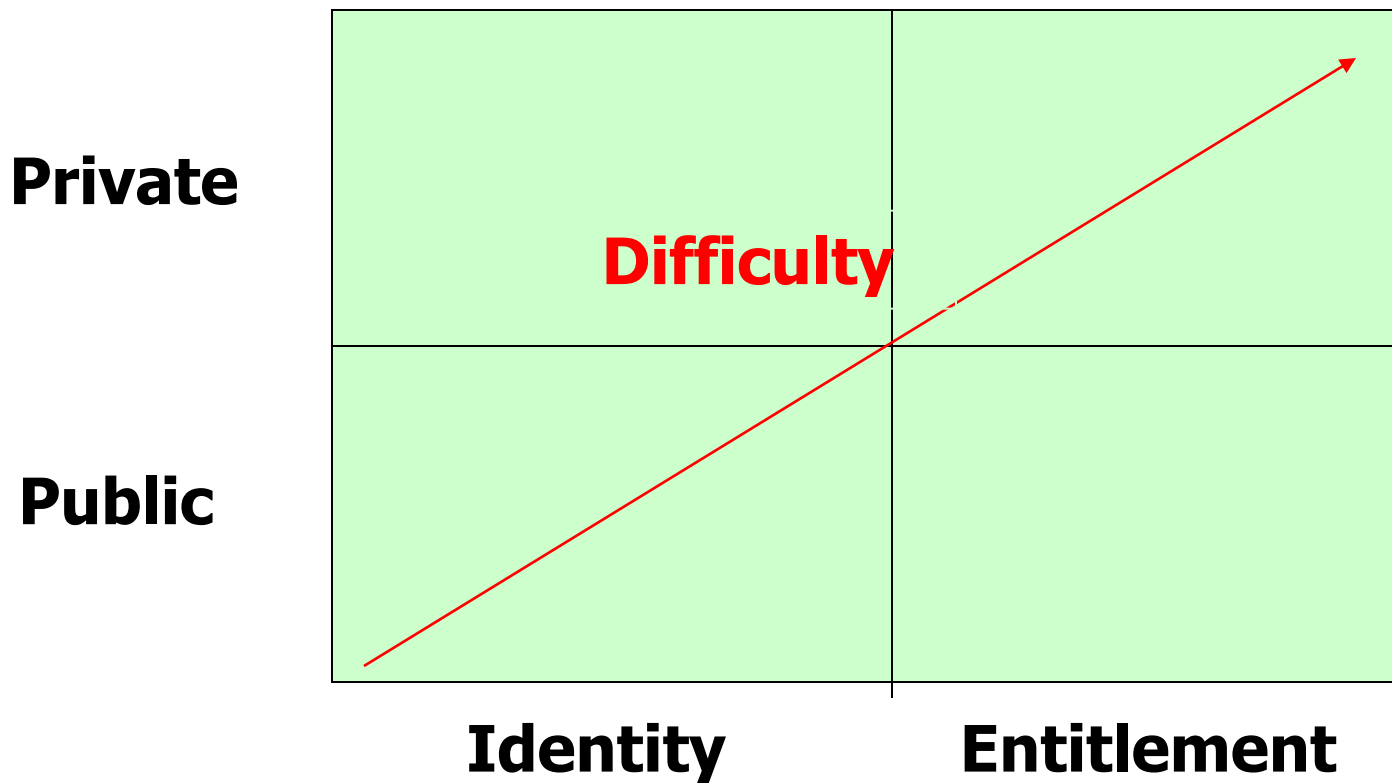
Rights to private data

- Citizens should retain rights to personal data
- We should consent to it being linked
- Government must protect citizens from having their rights removed
- Government will lose trust if it does not protect the rights of its citizens.

Personal data or public data?

- Is **ID** personal data? Not clear
 - No rights to parts of our own body!
 - No rights to our own image!
 - Limits are societal / privacy, not legal (except assault)
- **ID+** is usually personal data – but some of it (e.g. address) is far from private (e.g. electoral register) and all is changeable.

Government sharing what data, why and with whom?



Garbage in - garbage out?

- How can government align its records to physical identity?
 - Personal secrets (e.g. password, PIN, known facts)
 - Biographical footprint (some things about the person, ultimate is interview)
 - Physical biometric (the more unique the better, the more usable remotely the better)

The role of identity management in building trust

- Identity management can build trust in e-services through:
 - Confidence in the identity of the citizen
 - Confidence in the integrity of the information linked to the citizen's identity
 - Confidence in the authentication and validity of those accessing citizen information (both the citizen and other authorised enquirers)

The balance between risk and benefits



If something is provided more easily, cheaper, faster electronically with the disclosure of private data, people will do it, provided the risk is below a threshold that they believe is acceptable

The Personal Data Guardianship Code

The Code identifies the principles and responsibilities on which best practice is based, and gives:

- The roles and responsibilities of the **responsible person**
- The roles and responsibilities of the **data handler**
- The rights and responsibilities of the **data subject**

In the Boardroom

“Show me the audit trail proving that we have deleted all copies of personal data after twelve months”



In the Ministry



“If we link these databases will it help the public or just make our administration easier?”

“Will our administration actually be better or cheaper if the data in these linked databases is inaccurate?”

“Have we included what it will cost to clean the data in the project?”

Employee inputting data



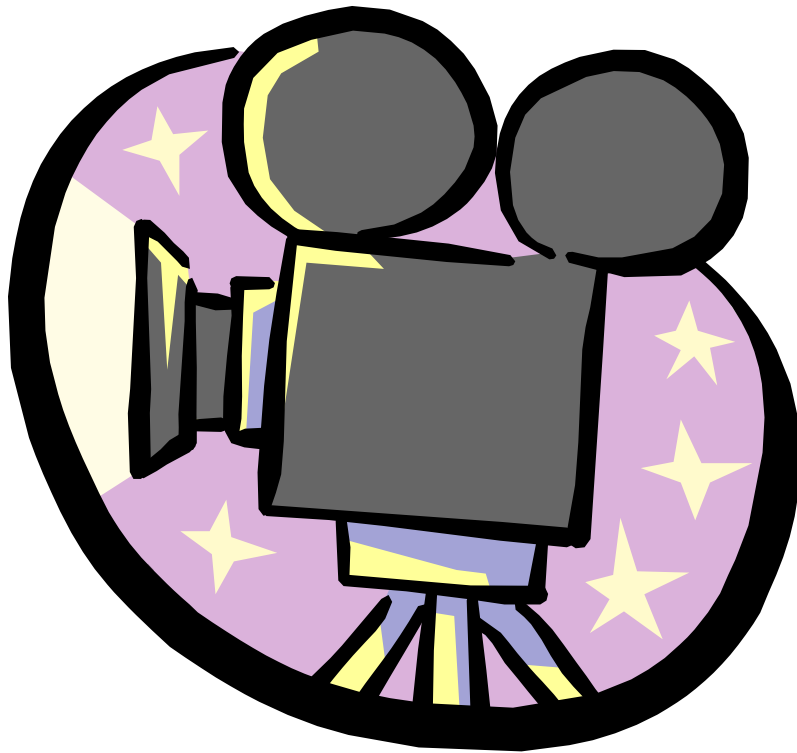
“Did she say her postcode was 8HP or 8PH? If I get it wrong the heart attack may go on the wrong record”

Employee going home



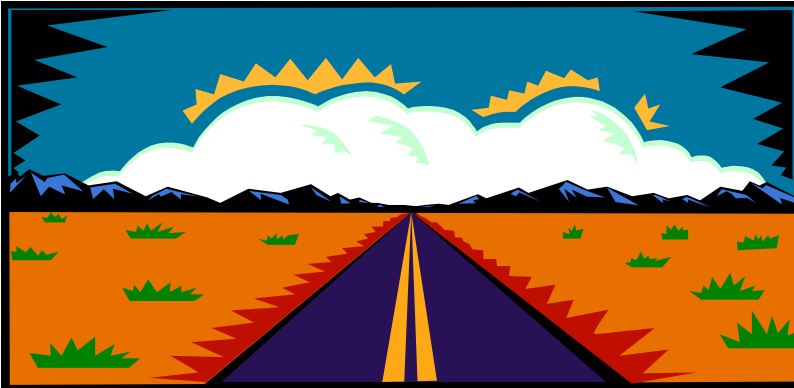
“I have got staff records on my laptop. Would it hurt them if my laptop was stolen?”

On the Internet



“I only want to buy a ticket, so why do they want to know my ethnic origins..gender... marital status?”

Line in the sand



The Government must protect the rights of their citizens to chose their private space