

Privacy as a key system requirement for building trust

Dr Ian Brown

HMRC data debacle

- 25m names, addresses, dates of birth, Child Benefit numbers, National Insurance numbers and bank or building society account details lost
- A stream of other losses to be revealed



Steve Bell, *The Guardian*, 22/11/07

Insider fraud

<i>Information required</i>	<i>Price paid to 'blagger'</i>	<i>Price to customer</i>
Occupant search/Electoral roll check (obtaining address)	not known	£17.50
Telephone reverse trace	£40	£75
Telephone conversion (mobile)	not known	£75
Friends and Family	£60 – £80	not known
Vehicle check at DVLA	£70	£150 – £200
Criminal records check	not known	£500
Area search (locating a named person across a wide area)	not known	£60
Company/Director search	not known	£40
Ex-directory search	£40	£65 – £75
Mobile telephone account enquiries	not known	£750
Licence check	not known	£250

Source: "What price privacy?", Information Commissioner, May 2006

Engineering privacy

- Privacy, like security, must be built in to a system from the start - not bolted on at a late stage
- Key legal and technology requirements are **minimisation** (of personal data collected, purpose, time kept, access given) and **protection** (data stored securely and access strictly limited)

Privacy Directive principles

- 1. Personal data shall be processed **fairly** and lawfully
- 2. Personal data shall be **obtained** only for one or more **specified** and lawful **purposes**, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- 3. Personal data shall be **adequate, relevant and not excessive** in relation to the **purpose** or purposes for which they are processed.
- 4. Personal data shall be **accurate** and, where necessary, kept up to date.
- 5. Personal data processed for any purpose or purposes shall not be kept for **longer than is necessary** for that purpose or those purposes.
- 6. Personal data shall be processed in accordance with the **rights of data subjects** under this Act.
- 7. Appropriate **technical** and **organisational measures** shall be taken against **unauthorised or unlawful processing** of personal data and against **accidental loss or destruction** of, or damage to, personal data.
- 8. Personal data shall not be **transferred** to a country or territory outside the **European Economic Area** unless that country or territory ensures an **adequate** level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Minimisation

- Why is personal data being collected in the first place?
- Identification vs authorisation
- Privacy Enhancing Technologies
- Distributed v centralised

Protection

- Data held and transmitted securely to prevent unauthorised access and modification
- Extensive protection against data loss or corruption
- Resistant to Denial of Service attacks
- All transactions must be loggable *by user*

Some (bad) UK examples

- NPfIT (over 1 million potential users)
- ContactPoint (330,000 users)
- National Identity Register (public & private sector use)

