EnCoRe
Ensuring Consent and Revocation

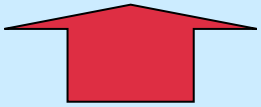
Collaborative research into informational privacy by UK industry and academia

Pete Bramhall, Hewlett-Packard

14 September 2010

Privacy – some definitions

Data Privacy >> Data Protection >> InfoSecurity



Human right

Principles

Mechanisms

EnCoRe

Data Privacy == Informational Self-determination

- Putting individuals in control of their personal data
- Can be achieved in a number of very different ways
- These are based on different trust models
- EnCoRe's approach is based on the notion of trust that the limits of an individual's consent will be respected by all those that process his/her personal data

Privacy: who cares about it?

- Individuals are increasingly becoming aware and concerned about
  - Their own personal trails of digital litter
  - Who might (mis)use this
  - The lack of help in obtaining restitution and redress
  - The need to take some action themselves
  - It's hard to do so
    - Ignorance, complexity
  - See:
    - http://news.bbc.co.uk/1/hi/technology/8009890.stm
    - http://www.trustguide.org.uk

EnCoRe

Privacy: who cares about it?

- Enterprises (partially)
  - Collective concerns: the risk of not gaining the economic efficiency benefits of a digital society
  - Some (a few?): differentiation by “doing the right thing” and making this known
  - Most: aim for the lowest-cost approach to legal compliance
  - No clear universal business case, but:
    - increasing awareness that personal information is a potential liability as well as a potential asset
    - information storage is not free, even if hardware is

Privacy: who cares about it?

- Governments (partially)
  - Similar concerns to enterprises' collective concerns
  - UK government funding three informational privacy research projects: EnCoRe, VOME, PVNETS
  - But see also Privacy International's 2007 Privacy Rankings:

http://www.privacyinternational.org/article.shtml?cmd%5b347%5d=x-347-559597

EnCoRe

Law and Regulation

- EC Directive 95/46
- UK Data Protection Act
- Information Commissioner's Office
  - Oversees compliance
  - Provides guidance
  - Fair information principles
  - The role of consent in these

Consent ...

... by an individual, to the collection, storage, use and onward sharing of personal data about himself/herself

The role of consent

- “When an individual has a choice as to whether they provide their information or not, that decision must be underpinned with the necessary information so that the individual can provide genuine, informed consent.”

- “It is also important that, where an organisation seeks to rely on genuine consent that they make it clear how consent can be withdrawn and what happens where this occurs.”

Source:
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico%20position%20paper%20on%20data%20loss%20reports.pdf

The overall vision of this project is to make giving consent as reliable and easy as turning on a tap…

…and revoking that consent as reliable and easy as turning it off again


EnCoRe


EnCoRe

The EnCoRe project's aims are to:

- enable business to adopt scalable, cost effective and robust consent and revocation methods for controlling the use, storing, locating and sharing of personal data.
- benefit individuals by providing meaningful, intuitive mechanisms which will allow them to control the use of their personal information held by others.
- help restore individual confidence in participating in the digital economy and so, in turn, benefit the wider society.

How does EnCoRe work?

June 2008 – February 2012

£3.6million funding

£2.5million of which is public:

- Technology Strategy Board
- Economic & Social Research Council
- Engineering & Physical Sciences Research Council

Who is in EnCoRe?

Hewlett-Packard Laboratories (*Co-ordinator*)

University of Warwick

London School of Economics

HeLEX Centre, University of Oxford

HW Communications

QinetiQ

Overview

interdisciplinary
social, technical, legal, economic, process

data processing
consent = weak, vague, and rarely meaningful

enablement
scalable, compliant, cost-effective, intuitive systems (technology & advice)

end-user pull
increase awareness and confidence (lay & professional)

recommendations
policy, regulation, best practice, standards

Project deliverables

- Technical architectures and prototypes
- Regulatory recommendations
- Proposals for compliance and certification
- Taxonomy and requirements formalisation

Expected outcomes

- General and sector-specific enhancements to the regulatory regime
  - Law, regulation, standards, best practices
- Enablement of easy, cost-effective compliance
  - Process & system designs
  - Technology components (products, sub-systems)
  - Implementation expertise & assistance
    - Guidelines, examples, consultancy services
- Creation of end-user pull for all the above
  - Widespread awareness (lay & professional)

Challenges

Some challenges around consent by individuals, to the storage, use and sharing of their personal data:

- Regulatory challenges
- Business challenges
- End-user challenges
- Technological challenges

Regulatory challenges

- No legal right of informational privacy for non-celebrities
- Consent need not and does not drive most data processing
- The right to revoke consent is limited to being an implied right to withdraw consent
- No effective legal codification of individual control over personal data

Business challenges

- “I know when I did my training one of the things I was told was that processing under consent is what the desperate resort to”

- Is business ready to buy-in to EnCoRe functionality?

End-user challenges

- “Natural consumer behaviour”
- “I never read the terms of agreement, not at all, it doesn’t really interest me”
- “You needed an average reading age of like 27 to read the average privacy policy”

Technological challenges (1)

- Privacy preferences/consents
  - Personalised access control
  - Personalised obligations
    - Notifications, deletions, etc.
- Stickiness of preferences/consents to all personal data copies in a chain
  - How much stickiness is needed?
  - How to achieve it?
- How to keep track of all copies?

Technological challenges (2)

- How to combine system policies & individuals' preferences/consents into a single enforcement mechanism?
- How to encode the consents in a machine-executable language?
- How to enforce and verify respect for consents all along a chain?
- How to enforce and verify revocation requests all along a chain?

Three Case Studies

Enhanced employee data sharing

Biobanks

Assisted living

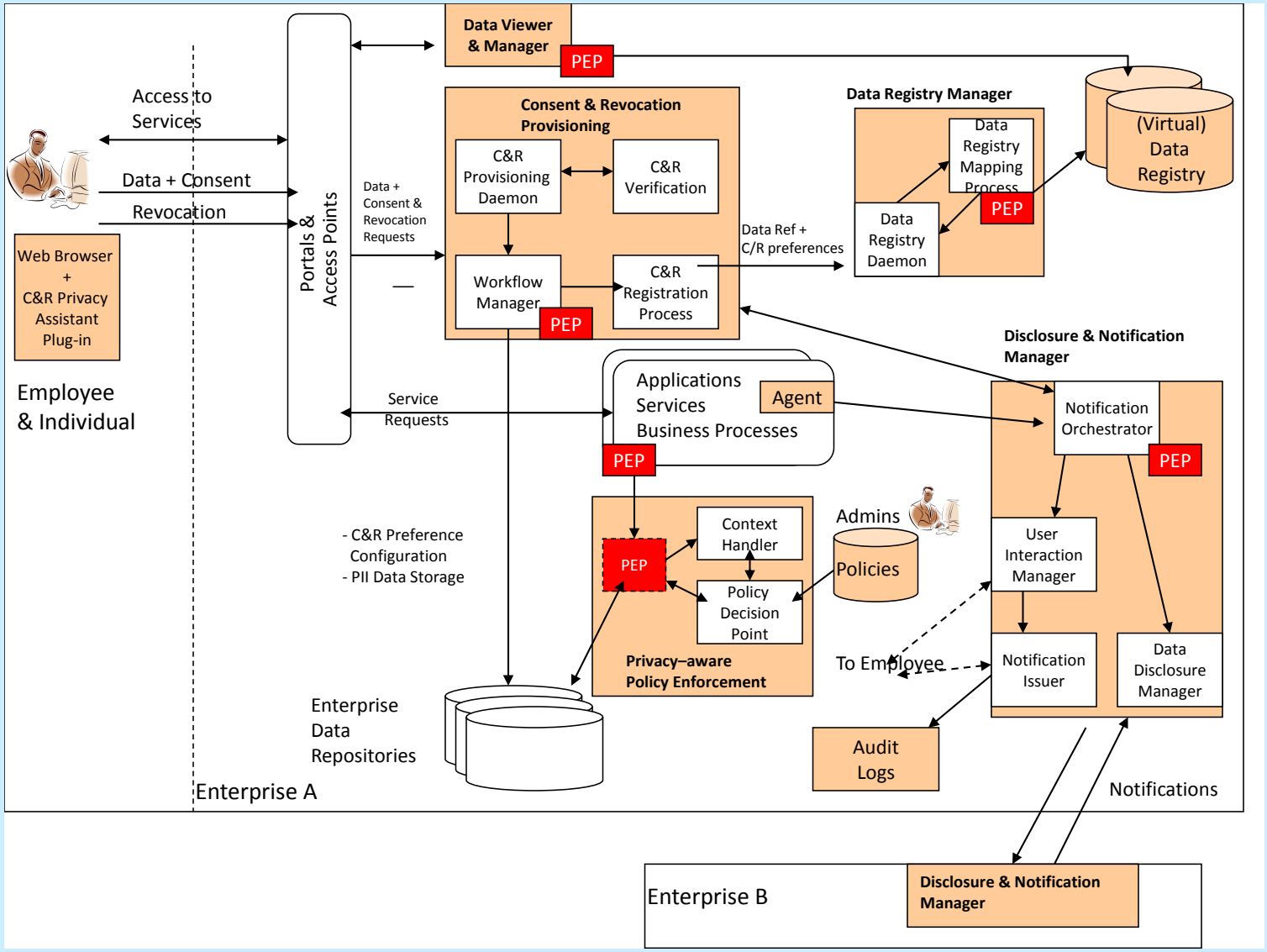
Current status (1)

- Case Study 1 complete
  - Requirements gathered
    - User focus groups/workshops
    - Legal analysis
    - Business process/compliance analysis
  - Technical Architecture defined, published
  - Prototype and demonstrator built

Current status (2)

- In process
  - Taxonomy and Formalisation work
  - Compliance process
- Case Study 2
  - Working with Oxford Radcliffe Biobank

Technical Architecture D2.1



EnCoRe

www.encore-project.info

http://www.twitter.com/encore_project

http://www.encore-project.info/newsletters/newsletter01/EnCoReJuly2010.htm

http://www.youtube.com/user/EnCoReProjectVideos