EnCoRe
Ensuring Consent and Revocation

Collaborative research into informational privacy by UK industry and academia
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
How does EnCoRe work?

June 2008 – November 2011

£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
Speakers

Pete Bramhall
   Hewlett-Packard, Project Co-ordinator

Dr Edgar Whitley
   LSE, Reader in Information Systems

Paul Hopkins
   University of Warwick, Senior Researcher

Dr Jane Kaye
   University of Oxford, Director, HeLEX Centre

Dr Dave Lund
   HW Communications, Technology Director
Consent ...

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

- Human right
- Breaches – high profile, costly
- Increasing awareness
- Information storage is *not* free
- Law and Regulation
Bill’s story
Confirm your attendance at the EnCoRe June 29 Press Conference at the London School of Economics by completing and sending this form

First name: 
Surname: 
Email: 
Phone: 

Representing (Name of Publication, Programme or Organisation, or "Self"): 

How long have you been associated with the above entity? 

Dietary requirements: 

Tick to subscribe to the EnCoRe Newsletter.

Latest News

Latest EnCoRe Tidbits
Snippets of news, etc. relevant to consent and revocation.

[more]

23.04.2010 Seventh Quarter Summary
A summary of the project’s seventh quarter activities is now available.

[more]

10.02.2010 EnCoRe Technical Architecture
The Technical Architecture for the first Case Study is now available.

[more]
they leave our site, and to read the privacy statements of these third party sites. This EnCoRe privacy statement applies solely to information collected by this EnCoRe website.

Rights and Obligations
The user has the right at every time to request information about the stored personal data. He or she has the unrestricted right of erasure, updating and correction of the stored personal data. This can be requested from the Project Co-ordinator. The submission of an EnCoRe webform to indicate participation in an EnCoRe event obliges the attendee to make a substantial donation towards a scholarship fund for the benefit of students at one or more of the academic partners in EnCoRe. Each attendee’s specific obligation will be publicized at the event unless the attendee notifies the Project Co-ordinator in advance of the event, in which case he or she will receive a small token in recognition of having read the foregoing.

Notification of Changes
If we decide to change our privacy policy, we will post those changes on the EnCoRe website so its users are always aware of what information we collect, how we use it, and under which circumstances we may disclose it.

Project Co-ordinator
Pete Bramhall
EnCoRe Project Co-ordinator
Hewlett-Packard Laboratories
Long Down Avenue
Stoke Gifford
Bristol
BS34 8QZ
United Kingdom
pete.bramhall@hp.com

(c) 2006-10 The EnCoRe Project. EnCoRe receives funding from the UK Government’s Technology Strategy Board, Economic & Social Research Council and Engineering & Physical Sciences Research Council.
Rights and Obligations
The user has the right at every time to request information about the stored personal data. He or she has the unrestricted right of erasure, updating and correction of the stored personal data. This can be requested from the Project Co-ordinator. The submission of an EnCoRe webform to indicate participation in an EnCoRe event obliges the attendee to make a substantial donation towards a scholarship event fund for the benefit of students at one or more of the academic partners in EnCoRe. Each attendee's specific obligation will be publicized at the event unless the attendee notifies the Project Co-ordinator in advance of the event, in which case he or she will receive a small token in recognition of having read the foregoing.
Prize-giving
Information Collection and Use
All information collected from the user by the EnCoRe website will only be processed by one or more partners in the EnCoRe consortium, as listed on the EnCoRe website, and by other parties who provide a service for the benefit of one or more partners or the EnCoRe consortium as a whole, to whom such partners may forward it. The data will be stored by EnCoRe partners only for as long as is reasonable for the purposes of the EnCoRe project, or as required by law.
Catering, anyone?
Catering, anyone?

Sponge cake, with jam and buttercream

Easy-peel satsumas

Giraffes?
Giraffes?

Exploring different life arrangements.
www.youtube.com/user/EnCoReProjectVideos

Thanks to Ken Shaw & Oliver Sin

BA (Hons) Graphic Design students, University of the West of England
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
Three Case Studies

Enhanced employee data sharing

Biobanks

Assisted living
Technical Architecture

Access to Services

Data + Consent Revocation

Web Browser + C&R Privacy Assistant Plug-in

Employee & Individual

Portals & Access Points

Enterprise A

Enterprise B

Disclosure & Notification Manager

Data Registry Manager

Data Registry Daemon

Data Registry Mapping Process

Data Ref + C/R preferences

C&R Provisioning Daemon

C&R Verification

C&R Registration Process

Workflow Manager

Consent & Revocation Provisioning

Privacy-aware Policy Enforcement

Context Handler

Policy Decision Point

Agent

Applications Services Business Processes

Admins Policies

User Interaction Manager

To Employee

Audit Logs

Notifications

Notification Issuer

Data Disclosure Manager

Notification Orchestrator

PEP

To Employee

C&R Preference Configuration - PII Data Storage

Data + Consent & Revocation Requests

Service Requests

PEP

Data Viewer & Manager

PEP

Data + Consent

PEP

C&R Privacy

Assistant

Plug-in

Portals &
Access Points

(Virtual)

Data Registry

EnCoRe
Demonstration

Case Study 1 Prototype
Consent in practice

Focus Groups
Privacy policies, terms and conditions

“I just showed you on Facebook the terms and conditions on my Blackberry, which nobody ever will read, the only thing in big letters is the “I Accept” button, you know, so, so before you can do any, you know, any, any, any meaningful consent you’ve got to address the issue of how aware people are, consumers are, users are, about what’s collected about them, how it is used, for what purposes and how... what can they do about it, because most people have no clue.” [CSO 847]
Effective control over personal data

“...the citizen currently, in some areas, has no right to give permission anyway, because there is a legal power for some of those bits of data to be shared whether the citizen gives consent or not.” [PSO 89]
Consent and regulatory requirements

“... a very large amount of, I’ll call it administrative overhead in an organisation, that we know exists in the enterprise and that we know that as small businesses we should be doing it but many of us simply don’t, because you’ve not got the time, you’ve not got the knowledge, you require that extra expertise.” [SME 66]
The nature of informed consent

“I mean I know when I did my ISEB [Information Systems Examinations Board] training one of the things I was told was that processing under consent is what the desperate resort to [LAUGHTER]. In other words it’s the last thing you ever want to process personal data under.”  [DPP 909]
Why Compliance?
Compliance

What is it?

Threat
Level of threat

Access controls

Opportunities to do damage

Assurance

Compliance Level

Determine useful variants
Granularity

User needs
Compliance

• Programme
  • Framework
  • Privacy Risk Analysis
  • Privacy Monitoring
  • Architectural Patterns
  • Testing
Legal

No legal right of informational privacy for non-celebs
Consent need not and does not drive most data processing
Legal

Marketing/spam aside, there is no effective, express right of revocation of consent in the Data Protection Act...
Legal

... no effective legal codification of user-control of personal data
Q & A

Refreshments
www.encore-project.info

http://www.twitter.com/encore_project

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