

EnCoRe

Ensuring Consent & Revocation

A collaborative IT research project being undertaken by UK industry & academia

Defining Consent and Revocation Policies

Dr Nick Papanikolaou

International Digital Laboratory

University of Warwick

<http://go.warwick.ac.uk/nikos>

Joint work with **Sadie Creese**, **Michael Goldsmith** (Warwick),
Marco Casassa Mont, and **Siani Pearson** (HP Labs)

- About EnCoRe
- Why / where C&R Policies are needed
- Formalising Consent
 - Permissions
 - Constraints
- Revocation: the eight variants
- Defining C&R Policies formally
- Conclusions & Future Work

- EnCoRe (**Ensuring Consent and Revocation**) is a UK-wide research project
- Focus: development of a **comprehensive software platform** for managing privacy of personal data in variety of applications
 - **employee data** in an enterprise
 - health data in a **biobank**
 - health data for **assisted living** etc.
- See <http://www.encore-project.info>

- What distinguishes EnCoRe from other privacy projects is the emphasis on consent and revocation as reverse processes
 - **revocation** “should be as easy as turning off a tap”
- EnCoRe promotes **user choice** by providing extensive privacy controls/settings
- **Benefit to users:** privacy as control (Westin)
- **Benefit to enterprises:** more willingness of data subjects to disclose PII

- **Privacy policies...**

- state an enterprise's general practices
- identify purpose and destination(s) of data

- **C&R Policies...**

- specify how and when consent is obtained and processed
- what choices are made available to users, including the revocation mechanisms and how they are applied

- From the enterprise point of view (the data collector)
 - a C&R policy is necessary in order to determine **what measures need to be incorporated** in business processes for collecting data subjects' consent
 - a C&R policy is a **public display of how privacy-friendly** the enterprise's practices are
 - esp. in terms of revocation mechanisms made available to end-users (data subjects)

- From the end-user's (data subject's) point of view:
 - a C&R policy would define unambiguously **which permissions are given to a data collector** when he/she gives consent
 - a C&R policy would tell **how data and permissions on data can be changed** through different types of revocation

- A C&R policy specifies:
 - for the data collector, for which practices consent has been given (**unambiguous statement of consent**)
 - for the data subject, which controls are available to him once consent has been given (**specific statement of revocation options**)

- In EnCoRe we distinguish between:
 - **available options**
 - universe of possible things a user might want to set
 - **options**
 - things a user can actually set
 - **choices**
 - the settings a user has made
 - **preferences**
 - the settings a user would like to make if possible

- When a data subject grants consent related to some datum δ
 - ... he or she is giving **permissions** to the data controller
 - Permissions are subsets of $2^{\{c,p,d\}} = \text{Powerset}(\{c,p,d\})$
 - c = collection, p = processing, d = dissemination
 - c^* , p^* , d^* are then introduced as **transitive permissions** (so that permissions can be shared)
- NB. The law in the UK conflates Collection and Processing

- **Permissions** provide a first means of characterising consent formally
- To be able to express consent in a more fine-grained way, we need constraints
- Consider examples:
 - “restrict data collection so that it occurs only in one country, so that it is subject to that country’s privacy legislation”
 - “consent lasts for only a fixed period of time”
 - “restrict processing of data so that it is used for only certain stated purposes”
 - “share the data with only particular parties, and banish uses of the data by others”

- To characterise consent in a more fine-grained way, we introduce **consent variables**:
 - t** = time for which consent holds
 - v** = volume of data to which consent applies
 - S** = allowed purposes for which data may be used
 - Π** = allowed parties with whom data may be shared

- Consent is formally characterised as a **combination** of:
 - **permissions** given to the data controller by the data subject
 - **constraints** on consent variables

- What do we mean by revocation?
 - is it just deletion of data?
 - is it removal of rights?
- When revocation occurs,
 - does it apply just to the party to whom we have given consent?
- Is revocation expressible in terms of consent?

- At PrimeLife'09, we introduced a **revocation model** with **eight (8) different variants of the notion of revocation**
 - 1) **no revocation: consent is irreversible**
 - 2) **deletion*** of data (*how much?)
 - 3) **revocation of permission(s) to process**
 - 4) **revocation of permission(s) to share**
- the above are the **core** revocation types.

- Derived/composite revocation types:
 - 5) Consentless revocation**
 - 6) Cascading revocation**
 - 7) Delegated revocation**
 - 8) Revocation of identity / anonymisation**

- For each datum pertaining to a user, a C&R policy specifies:
 - **collection** permissions
 - **processing** permissions
 - **sharing** permissions (with third parties)
 - **constraints** on consent variables (if any)
 - **revocation mechanisms** available

- Users $u \in U$
- Personal data for user u : $d \in D$
- For each $d \in D$, a C&R policy consists of:
 - $col \in \{c, c^*\}$
 - $pro \in \{p, p^*\}$
 - $sh \in \{d, d^*\}$
 - $\varphi \in \Phi$ where
 $\Phi ::= \Phi \wedge \Phi \mid t < time \mid v < vol \mid S [= Purposes \mid \Pi [= Parties$
[= denotes 'subset of'
 - $R \in \{(r1, r2) \mid r1 \in \{1, \dots, 4\}, r2 \in \{none, 5, \dots, 8\}\}$ where $(r1, r2)$ is a revocation type
($r1=core, r2=derived$)

- Policy rule for datum d1:
 - **(c,p*,d,t<30 days,(2,6))**
 - processing permission can be transferred
 - deletion is implemented in cascading form
- Policy rule for datum d2:
 - **(c, p, d*, t<30 days \wedge Π [= {gov}, {(2,none), (3,none)}])**
 - d2 can be shared onward transitively
 - consent is granted for 30 days for governmental organisations only
 - revocation options are deletion and revocation of permission to process

- We described C&R policies and what they offer to
 - enterprises / data collectors
 - end-users / data subjects
- Distinguished available options, options, choices, preferences
- Formalised consent as permission + constraint
- Formalised C&R policies as statement of
 - consent needed by data collector
 - revocation types available to data subject

- We plan to
 - refine our definition of consent further
 - make systematic syntax and semantics of permissions and policies
 - cf. our work on Hoare logic and access control model for C&R
 - develop translations to access control languages esp. XACML with suitable C&R extensions