Reaching for Informed Revocation
Shutting off the tap on personal data

Agrafiotis Ioannis
i.agrafiotis@warwick.ac.uk
Joint work with Sadie Creese, Michael Goldsmith
and Nick Papanikolaou

e-Security Group
International Digital Laboratory
University of Warwick

About EnCore

UK industry
- Hewlett Packard Laboratories
- HW Communications Ltd
- QinetiQ

Academia
- LSE information Systems and Innovation Group
- University of Oxford Ethox centre
- Warwick university e-Security Group

EnCoRe vision:
*The overall vision of EnCoRe is to make giving consent as easy as turning on a tap and the **revocation of consent** as easy as turning it off again.*

www.encore-project.info

Outline

- Setting the context
- Define Revocation
- Stakeholders
- Environments
- Revocation model
- Informed revocation

- Based on workshops organized by Dr Edgar Whitley from the LSE

Setting the context

Defining privacy:

- There is no single definition that clarifies what privacy really is
- It varies widely according to context and environment

Privacy as an individual right:

- Privacy is inherently personal. The right to privacy recognizes the sovereignty of the individual (Thomas Edison)

Privacy as supportive tool for social interaction:

- Privacy offers opportunities for political expression and criticism, choice and freedom in family, religion, and in other forms of association (Westin, 1967).

Technology:

- Technological developments taking place since 1970s, our daily interactions are now routinely captured, recorded, and manipulated by small and large institutions alike. Westin's (1967) seminal work articulated a set of fair information practices to give individuals some level of procedural control over their personal information.

Setting the context

Although there is ongoing work on formalizing privacy (Solove's taxonomy)there is no reference in the crucial role of technology which:

- Influences social structure
- Alters the balance and the trade offs taking place, between the individual's
- Right to privacy and society

Solove's view:

- Concept of "family resemblances"
- Each family has various similar characteristics the combination of which makes its
- Nature slightly different every time

Rule (2007) :

- Privacy as the possibility to choose whether to disclose personal information
- Asymmetric relationship between data users and data subjects
- Information gives strategic advantage to the users and places them in a position of power

Definitions of Revocation

- The concise Oxford dictionary describes revocation as:
  The end of the validity or operation of (a decree, decision, or promise).

- The taxonomy describes revocation as:
  The process of withdrawing consent over the use of previously disclosed data. Revocation can be done in a fine grained way, e.g. revoking consent over the usage of specific data for selected purposes but still allowing it to be used for other specified purposes.

- HP expands the above definition adding that:
  Revocation designates the process that permits an individual to invalidate or modify previously given consent, on personal data. This revocation should apply to any copy or instance of this data, within the organisation that initially collected it and in any other third party to which this data was subsequently disclosed … revocation can be fine-grained and be qualified by attributes. It might not just be a matter of "turning off" the entire consent given on a set of personal data but there could be degrees of revocation, affecting specific data items.

Purposes and objectives

From a user's perspective:

- Identify the different contexts where users need to revoke consent.
- Classify different types of revocation.
- Associate the identified types of revocation with the contexts that revocation takes place.

Classification

The EnCoRe project identified three different stakeholders :

- Citizens, who have a role in protecting their own personal information and specifying how it should be handled by others
- Society, who sets the standards, monitors their implementation and ensures compliance
- Data users, who play a role in implementing and operating solutions

Each of these stakeholders has a different interest in the privacy problem and there are conflicting needs to be balanced.

Classification

In different contexts the relationships, from a user's perspective, are the following:

1. Data subject ⟷ Citizen (Social networks)
2. Data subject ⟷ Data controller (Private)
3. Data subject ⟷ Data controller (Public)
4. Data subject ⟷ Society (Regulatory, legal environment)

Social networking (Facebook, Twitter)

- Cannot expect privacy
- Don’t normally read the privacy terms and conditions on a website
- Use it only for socializing
- Ignorance regarding deletion of an account; you can deactivate your account, but you can’t delete it

  “Twitter's advanced search page allows users to find deleted Tweets, an issue highlighted earlier this week after UK chat show host Jonathan Ross accidentally posted his personal email address in a message. Even though he quickly deleted the message the information was still easily obtainable, because Twitter fails to purge deleted tweets from its system.”

Interaction with private data controller

- Usually a question of trust (what I want, whose website I'm visiting....) " I don't trust, I wouldn't visit it". **Lock in effect to established providers**
- Previous experience : "I really make it a point to look at their privacy and conditions just in case they have another problem as well"

Looking for:

- Anonymization
- (Non) Traceability
- Transparency
- Non arbitrary use of data
- Deletion of data
- Certified deletion of data

Interaction with private data controller

Problems for the consumer:

- Waste of time for the consumer.

  "I don't really think I would actually go and pursue every company I've been shopping with and do that, because it would just be a waste, a lot of a waste of my time"

- Companies not obliged by the law to fulfil data subject's wish for revocation

- There is no standard way of implementing revocation

"but it took a long time to actually find someone who could do that for me, that she put me through many different exchanges cos nobody really knew what to do about, you know, taking, deleting some, some stuff off the…"

Interaction with private data controller

Problems for the private controller:

- Business information needs in using data:

  "you've got to really look at how you're using the data and the context of it and work out whether you can establish that there is a business need which outweighs the rights of the individual or whether the rights of the individual outweigh the business need and that, I think that's the problem, you can't… somebody just can't write to you and say, "I revoke my consent for everything".

- 3rd party data involved

- Metadata

- Revocation has stronger implications (cost) for organizations with respect to actions they need to carry out on data to fulfill the changes required by end-users

Interaction with private data controller

Advantages:

- Create relationships of trust
  "I want the option, no matter what it does to the public"
  "there is our public image, we don't want to be seen, not so much the fines, it's we don't want to be the company who <?? – 0.16.50> as you know, we appeared on lunchtime BBC news about 2 months which, you know, was, was not good…"
- Saving cost of storage
- Minimising data to process
- Aligning with data protection act and ICO
  "they can read it and you've destroyed the information <?? – 0.21.45> the Information Commissioner is going to clobber you and you've got at least some defence against litigation "

Interaction with public data controller

- Security reasons

  "merging of state and private sector, which is complicating a lot of the services under which data is actually processed, the value of data is valuable to the state for, you know, for anti-terrorist <?? – 0.29.09> organised crime and so on and that again is making it more complicated because, you know, there's nobody <?? – 0.29.19> and there'll be more of that, that's the trend I can see."
- Financial reasons
- Medical reasons (sensitive data)

Looking for:

- Anonymization (**sensitive data, research for common good vs privacy)**
- (Non) Traceability
- Transparency
- Arbitrary use of data (terrorism?)
- Deletion of data (DNA data bases)
- Certified deletion of data

Interaction with public data controller

Problems for the data subject:

- Cannot always revoke (DNA database)
- Cannot control the use of the data

  "the difference is government can do whatever the hell they like, whereas as individuals and businesses we have to sort of – or theoretically abide by rules to, like you say, benefit from what happened but also safeguard these premises "

- "what data subjects do and what society wants to be able to do often, particularly in medical research, but also in some cases for government systems, can be in direct conflict."
- The whole relationship between the individual government structure on statutory basis, then in a sense, consent is neither here nor there.

Interaction with public data controller

Advantages:

- In medical environment positive steps are made:

  - "Patients - who already had the right to opt out of the scheme - now have the right to have their medical records deleted instead of simply masked once they are put onto the system."

  - Tidiness & Minimisation of data

    "Thomas said the tide is now turning against data collection. "I think we will see less instinctive centralisation and less government collection of personal data in future years," he said."

Data subject interaction with society

- We assume that a consent given freely equates to a consent that can be revoked just as freely?

- Alignment with Data Protection Act
- Rectification
- Blogging

- "Well, I think the issue is what happens is the bigger companies, it's starts… the legislation starts at the top, the bigger companies take it on, they apply it to their systems and we've got to fit within their systems, so we automatically assume we are compliant because we're doing…"

Different types of revocation

From the previous contexts, we can identify the following types of revocation:

1. No revocation (propagate data to render them non-sensitive)
2. Deletion
3. Revocation of permissions to process data
4. Revocation of permissions for third party dissemination
5. Cascading revocation
6. Consentless Revocation
7. Delegated revocation
8. Revocation of identity (anonymization/pseudonimity)

The same types apply to metadata

Schema of revocation types

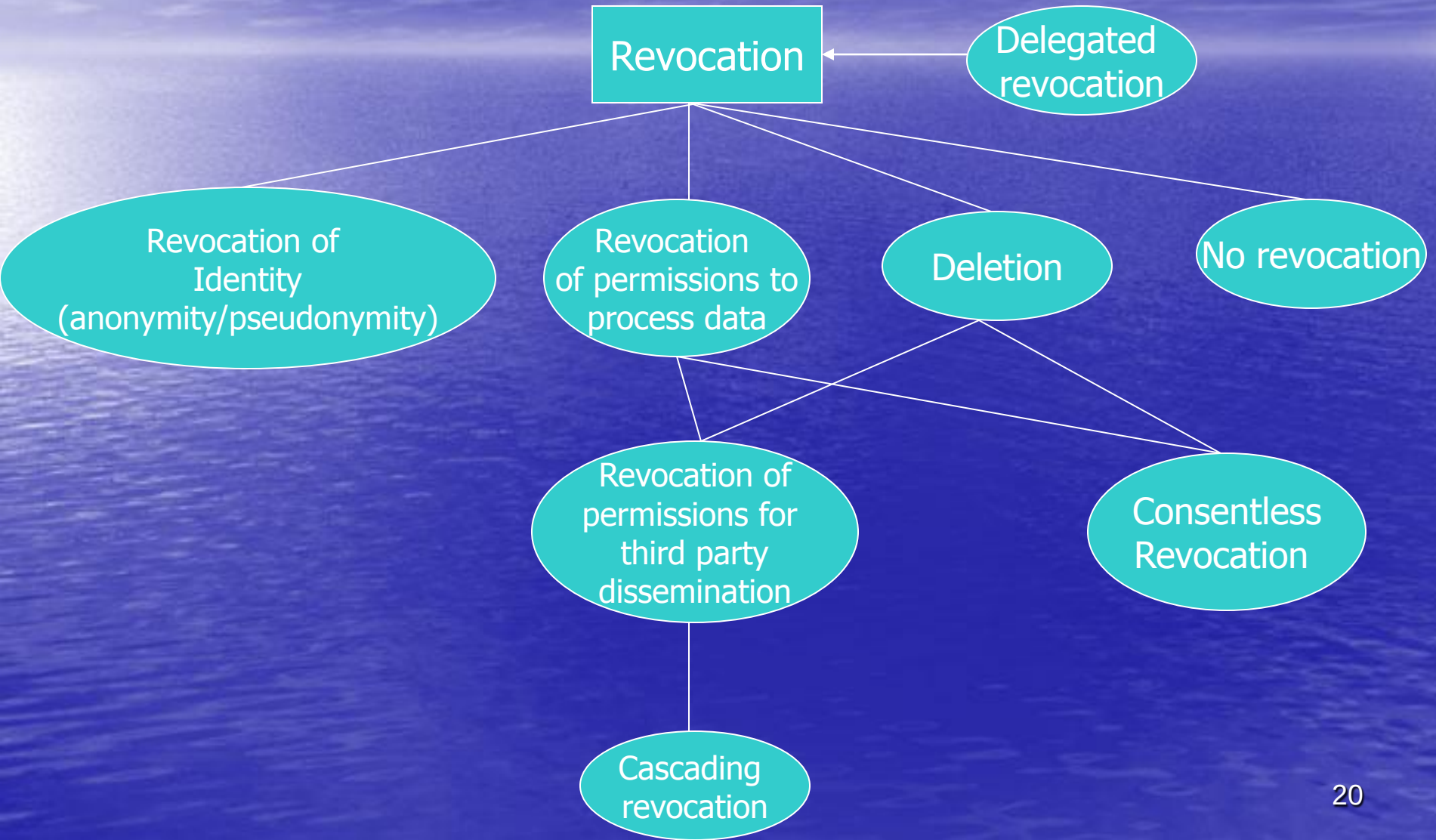

Table of revocation

types / uses	Deletion	Anonymity / traceability	Cascading	Revoke specific Processing of data	No revocation	Revoke the right to disseminate data	Revocation without consent	Delegation of revocation
Social networking	✓							
Medical environment	✓				✓			
Public data controller					✓			
Private data controller	✓				✓			
Legal Environment	✓				✓			

Table of informed revocation

types / uses	Deletion	Anonymity / traceability	Cascading	Revoke specific Processing of data	No revocation	Revoke the right to disseminate data	Revocation without consent	Delegation of revocation
Social networking	✓				✓			
Medical environment	✓	✓		✓	✓	✓	✓	
Public data controller				✓	✓		✓	
Private data controller	✓		✓	✓	✓	✓	✓	✓
Legal Environment					✓		✓	✓

Informed revocation

- There is a change in people's preferences when they are informed of all the possible types of revocation that could perform.

- Informed revocation is the process that allows users to remove or change permissions associated with:
  - Personal data
  - the purpose for which personal data may be processed by an enterprise
  - the sharing or dissemination of data by an enterprise with third parties
  - the identity of a data subject {anonymity} (or render the identity fake {pseudonymity})

even for the case where consent has not been given initially.

- The key characteristic of the concept of informed revocation is that the data subject should be informed of all the available types of revocation that he could perform.

Limitations

- Granularity
- Deletion
- Partial deletion
- Scramble
- Deletion Certificates

- Anonymization/Pseudonimity
- Conflict with the interest of security
- Traceability

Conclusion

- Need to provide users with mechanisms to control the storage, use and dissemination of personal data
- We have detailed different kinds of control that users desire to exercise over their personal data
- Proposed a model that covers all different kinds of revocation controls
- Coined the term of "informed revocation" to describe the change in users' behaviour

Thank you!!

Questions?