Reaching for Informed Revocation: Shutting Off the Tap on Personal Data

Ioannis Agrafiotis, Sadie Creese, Michael Goldsmith, Nick Papanikolaou

Reaching for Informed Revocation: Shutting Off the Tap on Personal Data

Ioannis Agrafiotis, Sadie Creese, Michael Goldsmith
and Nick Papanikolaou

International Digital Laboratory, University of Warwick, Coventry UK
{I.Agrafiotis, S.Creese, M.Goldsmith, N.Papanikolaou}@warwick.ac.uk

Abstract. We introduce a revocation model for handling personal data in cyberspace. The model is motivated by a series of focus groups undertaken by the EnCoRe project aimed at understanding the control requirements of a variety of data subjects. We observe that there is a lack of understanding of the various technical options available for implementing revocation preferences, and introduce the concept of *informed revocation* by analogy to Faden and Beauchamp's *informed consent*. We argue that we can overcome the limitations associated with informed consent via the implementation of EnCoRe technology solutions. Finally, we apply our model and demonstrate its validity to a number of data-handling scenarios which have arisen in the context of the EnCoRe research project. We have found that data subjects tend to alter their default privacy preferences when they are informed of all the different types of revocation available to them.

Keywords: Data Privacy, Consent, Revocation, Requirements

1 Introduction

In an environment dominated by information systems, e-services and e-commerce whose applications are continually evolving, enterprises have an ever-growing reason and capability to collect, store and process huge quantities of personal data. Increasingly we depend on cyberspace and necessarily disclose personal data in order to gain access to services. But we do so without having any practical control over how our data is handled; once we have handed over our data it physically resides on technology beyond our physical and logical reach, unless a service provider specifically provides functionality offering control. Consider the information uploaded by data subjects of social-networking sites. It is often analysed and sold to enterprises, and data subjects are categorised in profiles according to their commercial preferences. This offers significant value as marketing and products can become personalised and targeted. Mechanisms to enable data subjects to control these actions and, for example, to remove or modify personal data held by others, are missing. This lack of control directly hinders data subjects' ability to protect their own privacy in cyberspace.

The right to privacy has been historically protected. It has been the basis for the stability of all democratic societies, and its importance is highlighted throughout the published literature [1, 4,13] e.g.. It is difficult to conceptualise privacy because it is

multidimensional, subjective and context dependent; people feel differently about what privacy means to them. So unsurprisingly its definitions vary widely and a definition of privacy that is acceptable in one context fails in another. The volatile notion of privacy and the pervasion of technological innovations throughout our daily lives highlight the importance of personal data privacy and the complexity of controlling it.

In the field of privacy there is a constant debate over the relative importance of the individual right to privacy versus the common good for society [1, 4, 5, 13]. Legislation and regulatory procedures endeavour to establish functions that may find a balance between individuals' right to privacy and the common good. But every time a balance is found, the use of new technologies alters old norms either in favour of the individual or in the interest of the common good, and new norms and functions need to be re-established to restore the balance, thus forming a vicious circle.

Figure 1. The constant development of data collection, aggregation and processing technologies results in a vicious circle as society attempts to seek a balance of protection between the individual's privacy and security of society.

As technology advances, new ways of gathering private information emerge. This affects the ways in which privacy may be either protected or violated, depending on the purpose for which these advances are applied. Technological developments always proceed faster than the establishment of legislation and regulatory policies, thus fuelling the vicious circle. Thus, society is continuously attempting to achieve a balance between privacy and security without ever fulfilling this goal. Consider the war against illegal drugs in the US: It was thought that using heat sensors to find marijuana growing operations would be acceptable, but in 2001 [Kyllo v United States (533 U.S. 27)] it was ruled that using thermal imaging devices that can reveal previously unknown information without a warrant does indeed constitute a violation of privacy. Our research, and the EnCoRe project more generally [2], seeks to develop methods by which balance can be achieved via consent and revocation controls over the use of personal data.

The need for control mechanisms to deliver privacy of personal data is not a new observation. Many theories [1,4,13] reframe privacy either as individual liberalism or as a fundamental human right and an essential component in the functioning of democratic societies. Westin foresaw the need of the individuals to determine when, how, and to what extent information about them is communicated to others. Similarly, Faden and Beauchamp [5] perceived privacy as the possibility to choose or consent whether to disclose personal information. Solove [11] discusses the various ways in which data collection and aggregation can result in privacy problems and violations, and uses Wittgenstein's concept of family resemblances to identify and classify privacy violations. Seeking an understanding of what can be practically protected and regulated against, he argues that privacy can be conceptualised as having various similar characteristics, but the combination of these similarities makes its nature slightly different every time. Thus, the focus is on classes of privacy violations and not on prevention (beyond the contribution of an effective legal deterrent of course).

In line with the theories of Westin, Faden and Beauchamp, we believe that data privacy can be provided most effectively by providing data subjects with *control* over their personal data. We seek here a conceptual model of revocation suitable for implementing technical solutions, and which provides greater situational awareness as to the state of personal data, thus addressing the data aggregation problems highlighted in Solove's work [11].

Historically, enterprises have often been unwilling to implement such mechanisms in their databases due to the cost and the constraints that these would impose on enterprise data-handling practices. Privacy controls have only recently been introduced in large-scale information systems, and the use of privacy-impact statements is still a maturing discipline (and arguably is part of current best practice in managing risks associated with handling personal data). Social-networking sites such as Facebook and Twitter include embedded mechanisms to capture data subjects' preferences regarding their consent, which does offer some semblance of control. However, whilst data subjects may consent explicitly to sharing, storing and processing data on such sites, they cannot so easily revoke (permissions to hold or process) data that they may already have disclosed. This means that in most cases it is not possible for data subjects to change their privacy preferences in a transparent way; without an explicit revocation capability data subjects cannot have clear and unambiguous control mechanisms to protect data privacy. Unfortunately, there is a general lack of revocation controls in social-networking, e-commerce or indeed almost any cyberspace applications. Indeed, this lack is manifest not only in computer systems but in the relevant legal and regulatory policies also.

2 Revocation Requirements

In order to capture data subjects' requirements for revocation, we conducted a literature review. Due to the limited number of references to revocation mechanisms in the published literature, we extended our investigation to online articles covering realistic case studies. Furthermore, we analysed the transcripts of four focus groups, held by the EnCoRe project, to gain deeper understanding of data subjects' require-

ments. Within the setting of the EnCoRe[1] project, Edgar Whitley's group at the London School of Economics (LSE) conducted a series of interviews with multiple groups of data subjects to discover what their expectations might be of a system that provided revocation controls.

The focus groups were held at the University of Warwick and at the LSE. In the first group participants were students from Warwick University and unsophisticated data subjects. In the second participants were PhD students from LSE with a background in Information Systems. The third focus group, held also at the LSE, interviewed civil society representatives, and the participants of the fourth focus group were data protection professionals and representatives from the EnCoRe project. Data subjects were presented with various realistic scenarios in which they would need to grant and might wish to revoke consent for access to their personal data.

The focus groups were recorded and transcribed and the participants were informed that "the data from their session will be available to all researchers working on the project but the transcripts will be kept anonymous. The data may also be used in reports and publications and direct anonymised quotations from the transcript may be used in published output" [2]. For the needs of this paper, we used the ATLAS.ti software to analyse the transcripts. In our analysis here, we include relevant excerpts from transcripts in *italics.*

Our initial finding was a gap between the legal and the technical perspectives on revocation. In the legal view there is an ongoing philosophical debate to understand the concept of privacy independently of technology, while computer scientists perceive privacy mechanisms only as security requirements. Even though the examined sample was relatively small, references to revocation requirements were scant and almost without exception revocation was understood as deletion of personal data.

2.1 Context Dependency of Privacy Concerns

The literature [1,4,8,10] suggests that privacy has a context dependent nature. The analysis of the focus groups transcripts verified our literature findings as it emerged that the environment in which data subjects revoke personal data, drastically influences their preferences. In this section, we present and analyse the possible environments that are created, when adopting a data subject's perspective. When stakeholders with different interests in the privacy problem interact, they establish relationships. In these relationships, there are conflicting needs to be balanced, different kinds of requirements arise and, as a result diverse environments are formed. We concern ourselves with three different categories of stakeholder:

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

Here, we adopt a data subject's perspective, and we will examine the environments that are created when a data subject interacts with each one of the above three different stakeholders. Understanding the interactions that dominate in each relationship is

[1] See www.encore-project.info for more information on EnCoRe.

the first step to capture the contextual nature of privacy. We focus on interactions in order to obtain a representative view of a relationship in motion, as opposed to just a snapshot of a specific situation. Each type of interaction leads to different revocation requirements and we have distinguished four cases of interest depicted in Figure 2 below. The arrow denotes an interaction between the data subject and a stakeholder.

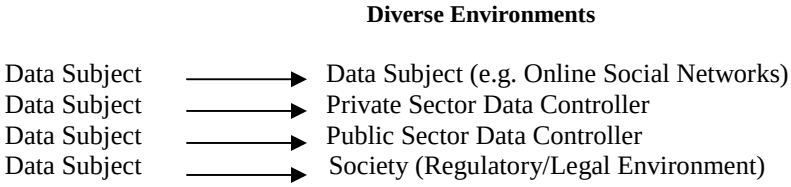

Figure 2. The environments that are formed, when a data subject interacts with the possible stakeholders of the privacy problem

The interactions of the data subject with public and private sector data controllers must be treated separately, as the participants of the focus groups emphasised; privacy preferences of data subjects differ substantially in these two cases, as the asymmetries that emerge especially in the public related environment, create more complex situations for the data subjects to handle. Participants in the focus groups were not asked specifically to distinguish the diverse environments in which they perform the act of revocation. What follows below is an analysis of the identified environments.

2.2 Identifying Data Subjects' Requirements

In this section we present our analysis of the way in which privacy requirements vary across these environments**.**

2.2.1 Social Networking Interactions

The social networking environment involves interactions between data subjects mediated by a third party. The literature suggests [3, 7] that social networking enables data subjects to control not only their own data, but often that of their friends by providing the means to disseminate information from various data subjects to some extent. Thus, data subjects are now empowered with capabilities that enable the collection process and dissemination of personal information.

In the focus groups, there were a number of references to data subjects' interactions with other citizens, in the context of social networks. People indicated that they use sites such as Facebook and Twitter only for socialising. They do not bother to read privacy terms and conditions as they believe that the information they disclose is trivial. Even though it may be a fallacy, data subjects believe that they are always able to delete data uploaded onto these sites. They feel secure and more confident to disclose data with deletion mechanisms in place, even though they have no guarantee that the act of deletion on the part of the data subject actually puts their data out of use. To quote one participant:

"Twitter's advanced search page allows data subjects 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."

On social networking networks there are some privacy controls already available. Facebook provides fine-grained privacy settings[2] [8] that allow data subjects to control with whom to share what, for example. Revocation in this setting is almost exclusively understood as deletion of data, and this is not always possible (as the above quote illustrates). Data subjects generally would like to have more revocation options, including anonymisation and actual deletion (expunging the data from the system altogether).

2.2.2 Interactions with Private Sector

When data subjects interact with private data controllers, they seek to build and enhance a relationship based on trust. Data subjects experience a *lock-in effect*, as they are reluctant to have to disclose data to another controller. They often highlight the importance of *"previous experience"*. In contrast to the social networks, where the interactions between data subjects have similar value for both parties (although there are exceptions [7]), all participants have the same expectations and the environment regarding privacy is not complex, in such an environment the situation becomes far more complex and new asymmetries emerge. These asymmetries take the form of asymmetric expectations, in which "one party expects the other party to behave in ways in which the other party does not expect or intend to behave" [7].

As mentioned above because of "expectations asymmetries," their trust is sometimes violated and data subjects wish to perform revocation mechanisms to balance the situation. Individuals are only vigilant if they happen to have experienced a breach of their privacy, and are unwilling to revoke data when the revocation mechanisms available are not clear in terms of objective and function:

"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".

When data subjects act in this environment they mainly conceptualise revocation as deletion and opt for a regulatory organisation to certify that not only is their data properly deleted in accordance with their preferences, but also that it is not used in an arbitrary way. The importance of revocation mechanisms, understood just as deletion of data, is underlined from both data subjects and enterprises:

"I want the option [to delete my data], *no matter what* [damage] *it does to the public* [good]*."*

We observed in the focus groups that participants in this environment would opt for revocation mechanisms, such as revocation of permission to process data and revocation of permission to disseminate data. These mechanisms were not explicitly identified by them at the beginning of the focus groups. Only through discussions and a presentation of detailed revocation options at the focus groups did participants realise in how many ways they could exercise control.

---

[2] See http://www.facebook.com/privacy/explanation.php?ref=pf for more information on Facebook's new privacy policy

2.2.3 Interactions with Public Sector

According to the literature when data subjects interact with public data controllers new forms of asymmetries occur and thus data subject's preferences differ from the previous environments [7]. We derived from our analysis the following diverse forms of asymmetries:

- *Asymmetry in value*, in which public controllers derive high value from interactions, but data subjects derive low value
- *Asymmetry in expectations*, in the same sense where data subjects experience this form when interacting with a private data controller, as described above.
- *Asymmetry in power*, in which data subject has disproportionate ability to cause "damage" to the public controllers as some times data subjects are forced to consent and have no information on how their data is collected, processed and disseminated among the diverse public data controllers.

From the focus groups, participants indicated that they alter their perception of revocation when they interact with a public data controller. We identified the asymmetries that they experience in this environment. The data collected and processed by the public sector is sensitive private information and citizens' interest in preventing an invasion in their private lives may be by-passed for the sake of national security, to enable medical research, or in the interest of the common good or government policy. In a focus group, a data subject expressed concern about the

"...*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 organised crime and so on and that again is making it more complicated..."*

Recent incidents of lost or stolen government data [17] have reduced confidence in public authorities. Data subjects are increasingly concerned about preventing arbitrary use of personal data by government services. Although data subjects acknowledge that, in particular cases, the revocation of data will not be permitted (e.g. DNA database), they desire revocation mechanisms so as to deal with the aforementioned problems and to restore a relationship of trust.

Individuals are willing to share personal data for medical research if certain conditions are met. Those participated in the focus groups have indicated that anonymity and traceability are required features of a health database if they are to disclose their medical records. However, these two concepts are in tension, often resulting in solutions based on separation but with the potential for tracing back:

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

Due to the asymmetries, participants believed that they could not perform any revocation. However, when they realised the options that they could have, data subjects opted for revocation of permission to process data, to disseminate data and of delegated revocation. In medical cases, delegated revocation was a popular option.

2.2.4 Interactions with Society

Society could motivate enterprises to enhance their privacy mechanisms by providing revocation controls. Privacy guidelines for large enterprises exist, and law

requires that these are used. Smaller enterprises need to abide by the same rules and report to the Information Commissioner Office. On the contrary, in the public sector it appears to be occasions where revocation controls are prohibited for the sake of common good [16]. In the name of society data subjects' right to privacy is invaded and in cases such as criminal records and police's dna data bases data may have a lifetime persistence [18].

To synopsis our findings in this environment, the only revocation mechanism that a data subject could apply, in terms of legislation, is the right to object to:

"*unfair/unlawful processing by withdrawing the existing consent – i.e. revoke – and optionally replace it with a new consent; terminating any relevant contract with the data controller/ processor; objecting on the basis that the processing is prejudicial to the data subject's 'rights and freedoms' or 'legitimate interests"*.

Finding a balance between individuals' privacy and national security is an ongoing debate. [10] As the requirements that emerge from this environment are more of legal nature and were found also in the other three environments, we consider this debate beyond the scope of this paper.

3 Revocation Model

The principal results of our analysis is a novel taxonomy of revocation. We identify four *fundamental* types of revocation (1.-4. below), and four *derived* types of revocation (5.-8. below).

1. **No Revocation At All:** Personal data remains static, and once it has been disclosed, it is either physically impossible to revoke (how could ever revoke reputation) or prohibited for various reasons (e.g. law-enforcement, data from police's DNA database).

2. **Deletion:** Data are completely erased and cannot be retrieved or reconstituted in any way. Certain privacy rights are enshrined in national and European legislation; it is worth mentioning here how our model incorporates some of the stipulations of the EU Data Protection Directive 95/46/EC. In article 12, for example, the directive mentions "the **rectification,** erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data." Rectification is a variant of revocation in the sense that a data subject may request the deletion of incorrect data held about him or herself and have it replaced with other data.

3. **Revocation of Permissions to Process Data:** Data subjects withdraw consent that would enable an enterprise to process or analyse their personal data for a specified purpose. EU Data Protection mentions "blocking," which corresponds exactly to revocation of permissions to process data in our model.

4. **Revocation of Permissions for Third Party Dissemination:** Data subjects withdraw consent that would enable an enterprise to disclose information to a third party.

5. **Cascading Revocation** is a variation on any of the above kinds of revocation, whereby the revocation is (recursively) passed on to any party to whom the data has been disclosed. Through this mechanism, data subjects are able to revoke data by only contacting the enterprise that they disclosed their data to originally.

We may remark that offering such a service is only practicable if data is only disclosed to organisations which themselves offer such a control.

6. **Consentless Revocation:** Personal data for whose storage and dissemination no consent has been explicitly given by the data subject, but which may need to be revoked. Again, any of the fundamental types of revocation may be invoked. We introduce this form of revocation to capture the privacy problems identified by Solove [11] . The need to revoke consentless data emerges mainly when a breach in privacy has occurred and the data subject experiences one of Solove's problems.

> Example: A picture of Jane drunk at a party was uploaded onto Facebook without her consent. As a consequence her reputation is ruined. She takes legal action in order to have the photograph removed from the site.

7. **Delegated Revocation:** This is a kind of revocation which is exercised by a person other than the individual concerned, such as an inheritor or parent/guardian.

8. **Revocation of Identity (Anonymisation):** Data subjects may be happy for personal data to be held for certain purposes so long as it is not linkable back to them personally. Anonymisation may be regarded as a variant of revocation, in that data subjects request a change to data held so that it is no longer personally identifiable (but see *Limitations* below).

3.1 Limitations

The model proposed in this paper may be limited in the following ways:

- The issue of *granularity* needs to be considered specifically for the deletion type of revocation.
- Data subjects may want to *partially revoke* their data, or to *scramble* their data instead of having it erased completely.
- The question of *deletion certificates*, namely, non-repudiable proofs that deletion has really been performed, but this is beyond the scope of this paper.
- The possibility of anonymisation poses interesting problems as it makes the origin of data untraceable; there are cases where this is not in the interest of security or the common good in general. A system implementing anonymisation should have safeguards in place to ensure that data subjects will act legitimately. On the other hand, if data is (even partly) identifiable, an enterprise can aggregate it and eventually infer to whom it refers. Such issues need to be taken into consideration when implementing revocation mechanisms.

4 Reaching for Informed Revocation

We found there to be a lack of in-depth understanding of the different ways in which revocation can be performed and/or implemented in practice. Participants at our focus groups perceived revocation simply as deletion of data, and they highlighted

the need to be informed about the nature of deletion and the privacy protection it can actually offer. Furthermore, when they were denied the option of deletion, they were reluctant to search for alternatives. We distinguished a significant change in people's preferences when they were informed of all the available types of revocation that they could perform in the context of a particular scenario. People become more selective and seek the revocation mechanism closest to their needs.

Tables 1 and 2 illustrate data subjects' choices of revocation mechanisms for a set of example scenarios. In Table 1 we have captured which revocation mechanisms data subjects expect by default. Table 2 shows the revocation mechanisms that data subjects chose after they were informed of their existence. It is quite evident that, once data subjects are informed of the different variants of revocation, they make more careful choices. Before being informed, they choose either to have data deleted or left intact. When given a choice between the different types of revocation (as identified in Section 3), they take advantage of the different controls available.

	Social Networking	Medical Environment	Public Data Controller	Private Data Controller	Legal Environment
Deletion	✓	✓		✓	✓
No Revocation		✓	✓	✓	✓

Table 1. Initial/Default Choices.

	Social Networking	Medical Environment	Public Data Controller	Private Data Controller	Legal Environment
Deletion	✓	✓		✓	
Anonymisation		✓			
Cascading Revocation				✓	
Revocation of Permissions to Process		✓	✓	✓	
No Revocation	✓	✓	✓	✓	✓
Revocation of Permissions to Disseminate		✓		✓	
Consentless Revocation		✓	✓	✓	✓

Delegated Revocation				✓	✓

Table 2. More Informed Choices .

In order to explain this phenomenon, we introduce the concept of *informed revocation*, by analogy to Faden's and Beauchamp's *informed consent* [5]. In their research, they argue that consent of data subjects needs to be voluntary – not the result of force or coercion – and they need to be informed about how their data is to be used, and how they can exercise rights over it if needed. When these conditions are met, consent granted for a particular use is considered *informed*.

We define informed revocation as a process that allows data subjects to remove and/or change permissions associated with:

- Personal data held by an enterprise.
- 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 (cf. anonymisation), 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 or she can perform, without being forced or coerced to give up any of these rights.

The idea of consent is at the heart of codes of research ethics and the writings on that subject [5,14]. Consent may be regarded as the opportunity to decline to take part or to withdraw from the process taking place without such decisions triggering adverse consequences for them. According to the Theory of Informed Consent, people can only consent to something if they have received sufficient information, have understood it and have explicitly expressed agreement [5]. Its early adoption is associated with medical practice and the right of patients to be informed about the risks of medical procedures that might affect their wellbeing. Today its scope has broadened to include, amongst other elements, the right of online service data subjects to be informed of the way their personal information is used.

A criticism of the concept of informed consent has been raised on the grounds that, since consent is elicited only once – before personal data is processed – it cannot be considered 'informed' throughout the lifetime of the data; in other words, consent is granted on the basis of information available at a fixed moment in time, and whether that decision may be deemed 'informed' depends only on how much information was available at that moment. At a subsequent time data might be used for alternative purposes than the data subject initially consented to, so that he or she may not be fully informed.

Another concern surrounding achieving informed consent [6] is how free the individual is to participate. Particularly in medical environments, people often decide to consent before they read the consent form. Patients see the process of giving consent as a mere ritual and they sign the form more as a symbolic act rather than a meaningful process that has illuminated them about the situation to be experienced.

Fisher [6] also argues that researchers experience the same phenomenon. They perceive that participants share the same understanding and have the same perception

about the process of consent with them and incorrectly conclude that the form they sign is informative enough for the consent of the patient to be informed.

Our revocation model in itself cannot address the criticisms levied at Information Consent as a concept. However, we believe the EnCoRe methodology can, and so we hope to achieve informed revocation through the nature of the EnCoRe system since data subjects will necessarily engage in a process of setting consent and revocation preferences; the nature of the process tackles the problem of the non experience of the situation. Imagine playing a game of chess where consent is like making the first move where the combination of moves are infinite and revocation is like deciding which move to make when the game is ending where the combination of moves could be calculated and the result could be anticipated. Individuals are aware of the situation and do not experience the procedural misconception effect because they have already evaluate the situation and they want to exercise their right to revoke because of their experience. Furthermore, we have formed informed revocation in such a way that the process of revocation is unambiguous. The definitions are not open to interpretation as some consent forms are. Individuals only need to be informed of the different revocation mechanisms that they may perform and what each mechanism could achieve. However the implications that their act of revocation may have to the data controllers cannot always be predicted. This paper has adopted an individual's perspective and further research needs to be conducted to clarify this aspect.

5 Conclusions and Future Work

Information systems abound in our everyday life, and we are constantly disclosing personal data to enterprises and government in an effort to gain access to products, services, and society's many benefits. There is consequently a need to provide data subjects with mechanisms enabling them to control the storage, use and dissemination of such data.

In this paper we have detailed the different kinds of control that data subjects desire to exercise over personal data concerning them that is held by an enterprise. We have elicited data subject requirements from the literature and from focus groups with actual data subjects carried out within the EnCoRe project, and proposed a model that covers all the different guises of revocation. We are not aware of any other work that specifically addresses revocation and its variants. From our sample, we also noted a tendency by data subjects to alter their choice of revocation mechanism when informed of the many different kinds that exist, and coined the term "informed revocation" to describe this change of behaviour.

There are several avenues for future work. Subsequent research could tackle the issue of granularity and provide a more concrete solution to the conflicting requirements of anonymisation and traceability. Moreover, the model presented could be refined by applying it to more case studies. While this paper has considered only the perspective of the data subject, another direction of investigation is to consider revocation requirements from different perspectives such as the data controller's or the society's perspective. It is highly likely that the requirements elicited from these future researches may not be well aligned or may be even in direct conflict with the findings of this paper.

References

[1] Can A. S. : What Was Privacy? Harvard Business Review, (2008)

[2] Casassa Mont M., Pearson S., Kounga G., Shen Y., and Bramhall P.: On the Management of Consent and Revocation in Enterprises: Setting the Context. Technical Report HPL-2009-49, HP Labs, Bristol, (2009).

[3] Dwyer C., Hiltz S, Passerini K. : Trust and Privacy concern within social networking sites: A comparison of Facebook and MySpace. Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone (2007)

[4] Etzioni A.: Are new technologies the enemy of privacy? Knowledge, Technology & Policy, 20, 115-119, (2007).

[5] Faden R.R and Beauchamp T.L.. :A History and Theory of Informed Consent. New York, NY, Oxford University Press. (1986).

[6] Fisher J.A.: Procedural misconceptions and informed consent: insights from empirical research on the clinical trials industry. Kennedy Institute of Ethics Journal, 16, 251–68, (2006).

[7] Glazer I., Blakley B.: Privacy. Identity and Privacy Strategies In-Depth Research Overview, Burton Group Reports Version 1.0, (2009)

[8] Grimmelmann JT. : Facebook and the social dynamics of privacy. Iowa Law Review 95(4). (2009)

[9] Lipford R. H., Besmer A., Watson J. : Understanding privacy settings in Facebook with an audience view. Proceedings of the 1st Conference on Usability, Psychology and Security, p.1-8, San Francisco (2008)

[10] Riley B. T. : Security vs. Privacy: A Comparative Analysis of Canada, the United Kingdom, and the United States. Journal of Business and Public Policy Volume 1, Number 2, (2007).

[11] Solove D.: Understanding Privacy. Cambridge: Harvard University Press, (2008).

[12] Warren S., Brandeis L. The Right to Privacy. Harvard Law Rev., vol. 4, no. 5, Dec. 1890, pp. 193–200, (1890).

[13] Westin A.F. : *Privacy and freedom.* New York: Atheneum, (1967).

[14] Wilkinson T. : Research, informed consent and the limits of disclosure. Bioethics 15[4], 342-61. (2001).

[15] Various authors: On the anonymity "versus" accountability debate. Available from http://hosteddocs.ittoolbox.com/ks070709.pdf (2009).

[16] http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/5898488/Sex-offender-register-for-life-breaches-rights-of-rapists-and-paedophiles.html. Last accessed on 06/02/2010.

[17] http://www.theregister.co.uk/2008/08/20/uk_gov_lost_records/ Last accessed on 06/02/2010

[18] http://www.theregister.co.uk/2009/12/21/dna_pnc. Last accessed on 06/02/2010.