



# EnCoRe Publication

Title: INFORMATIONAL PRIVACY, CONSENT AND THE  
“CONTROL” OF PERSONAL DATA

Authors: Edgar A. Whitley

Date: 1 September 2009

Publication Details: To appear in Information Security Technical Report  
(2009)

Summary: This paper reviews how the notion of control has been conceptualized in relation to informational privacy and, from a perspective of consent and the revocation of consent, suggests that there are more sophisticated notions of control over personal data that can be proposed. The paper outlines some of the challenges underlying these enhanced notions of control in the context of privacy and consent.

Keywords

Privacy, Consent, Revocation, Control

# INFORMATIONAL PRIVACY, CONSENT AND THE “CONTROL” OF PERSONAL DATA<sup>1</sup>

*Edgar A. Whitley*

*Information Systems and Innovation Group*

*Department of Management*

*London School of Economics and Political Science*

*Houghton Street*

*London WC2A 2AE*

*United Kingdom*

*e.a.whitley@lse.ac.uk*

*<http://personal.lse.ac.uk/whitley>*

## *Abstract*

This paper reviews how the notion of control has been conceptualized in relation to informational privacy and, from a perspective of consent and the revocation of consent, suggests that there are more sophisticated notions of control over personal data that can be proposed. The paper outlines some of the challenges underlying these enhanced notions of control in the context of privacy and consent.

## *Keywords*

Privacy, Consent, Revocation, Control

## **1 INTRODUCTION**

In order to gain access to the many services and benefits of society, individuals are increasingly required to provide personal information via the internet. However, the (mis)handling of personal data by companies, government bodies and other institutions is resulting in a growing unease about this aspect of modern society. Concerns about privacy risks of data handling, as exemplified by the loss of two disks containing the child benefit details of 25 million people by the UK government, are becoming increasingly mainstream (Whitley, 2009) and individuals are looking for better ways to control the way their personal data is used by others.

The nature of the responses to this problem, ranging from increasingly sophisticated technological measures such as encryption to legal remedies and changing business practices is driven, to a large extent, by the conceptualisations of privacy found in the

---

<sup>1</sup> This work was supported by the Technology Strategy Board; the Engineering and Physical Sciences Research Council and the Economic and Social Research Council [grant number EP/G002541/1]

literature. These conceptualisations create formative contexts (Ciborra & Lanzara, 1994) that limit the ways in which the problem is understood and hence the available solution space.

In recent years there has been growing recognition that providing users with control over their personal data is an important aspect for maintaining trust in an online environment. However, as this paper argues, the understanding of user-centric control that frequently emerges is an impoverished version based on earlier understandings of technology. This paper draws on notions of consent and, importantly, the revocation of given consent as a basis for a new understanding of control of personal data. This new understanding opens up novel opportunities for enhancing trust in an online society addressing some of the key informational privacy concerns that exist.

This paper draws on work being undertaken by a large, cross-disciplinary project (EnCoRe— Ensuring Consent and Revocation) funded by the UK's Technology Strategy Board, Economic & Social Research Council and Engineering & Physical Sciences Research Council. EnCoRe's aim 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". The project starts from the perspective of consent rather than privacy and recognizes that consent can both be given and revoked (or retracted). Revocation of consent introduces a new form of control of personal data that has not been well studied in the literature or in the practice of informational privacy. Starting from consideration of consent opens up our understanding of the nature of informational privacy and offers new opportunities for addressing the concerns of individuals about data handling.

The structure of the paper is therefore as follows. The next section reviews how notions of privacy and consent have been conceptualised in the literature and demonstrates the implicit notions of control held within them. This is followed by a section that reviews how these views of control have been operationalised in recent empirical research. A section that discusses some of the implications for understanding the control of personal data that includes revocation follows and the paper ends with a discussion of some of the research and implementation issues that arise from this new perspective on privacy, consent and control.

## **2 PRIVACY, CONTROL AND CONSENT**

Wittgenstein (1956) tells us that language is a social activity and hence that specialised terms like privacy are arrived at socially. The term privacy, therefore, has no inherent definition rather different social groups and disciplines have developed different meanings and interpretations of the concept.

Introna (1997) reviews the literature on privacy and suggests that there are three broad categories of privacy definitions: privacy as no access to the person or the personal realm; privacy as control over personal information and privacy as freedom from judgement or scrutiny by others.

Drawing on earlier discussions of the distinction between public and private realms, legal theorists began drawing out some of the implications of this distinction in terms of legal rights. One of the earliest and most significant was the argument by Samuel Warren and Louis Brandeis (1890) who developed a right of privacy, namely "the right to let alone",

based on an earlier judgement by Thomas Cooley who proposed ‘the right to one’s person and a right of personal immunity’ (see DeCew, 1997, p. 14). That is, they saw privacy as closely related to being able to control actions and information about oneself. Privacy is thus associated with notions of personhood and self-identity (Kanellopoulou, 2009).

The Warren and Brandeis definition, therefore, falls within Introna’s first category and raises questions about the kinds of controls that can reasonably be implemented or expected to limit access to the individual. For example, this helps us to distinguish between conversations undertaken in our home with those that take place in a public space. We can control who enters our home and hence who might overhear our conversations, a level of control we can’t have in a public space.

Introna’s second definition highlights what is often described as informational self-determination (De Hert, 2008), based on a 1983 ruling by the German Federal Constitutional Court. The argument here is that if an individual cannot reasonably control how their information is used (for example, if it is subject to searches by the authorities) then they may refrain from undertaking socially useful information-based activities such as blogging on particular topics.

The third category, freedom from judgement by others, again relates to the disclosure and use of personal data by others. For example, in this category personal health data might reasonably be considered private because its involuntary disclosure may cause others to judge an individual’s lifestyle choices.

Many scholars see privacy as having intrinsic value as a human right, something that is inextricably linked to one’s essence as an (autonomous) human being. For example, Introna considers the hypothetical case of a totally transparent society (i.e. where there is no privacy). He questions the nature of social relationships in such a space asking how your relationship with your lover could differ from that with your manager: “What is there to share since everything is already known?” (Introna, 1997 p. 265). This transparent world also highlights a more instrumental perspective on privacy. In a totally transparent world, competitive advantage (knowing something that your competitors do not) is not possible (or at least not sustainable).

A related dichotomy is presented by Anita Allen (1999) who distinguishes between decisional privacy and other forms of privacy such as informational privacy, physical privacy and proprietary privacy. Decisional privacy can be seen as the consequence of Introna’s freedom from judgement category and relates to mechanisms that allow decisions to be made free from outside influence (or perceived influence) whilst the other forms of privacy are more closely related to the kind of personal disclosures that could take place.

In Europe, the Data Protection Directive (Directive 95/46/EC) states that the main aim of national data protection laws should be to ensure the protection of an individual’s privacy rights. Thus, data protection legislation can be seen to implement informational privacy, although the UK Data Protection Act doesn’t mention the word privacy, relying instead on a series of “privacy-friendly” data processing principles.

All of these definitions share an implicit and limited view of the kinds of controls that an individual could or should have, particularly with regard to informational privacy. For example, Westin’s (1967) seminal book defines privacy as:

the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others (p. 7)

Control in this context is seen as something that occurs at the start of a disclosure process and privacy control is seen solely in terms of limiting what personal data is made available to others. In practice, however, this is a rather partial view of how personal data is disclosed and shared with others. It is increasingly common for individuals to register with various online services and disclose data about themselves (name, email address, etc.). This data is then stored in enterprise databases for significant periods of time and may be shared with other parts of the enterprise or selected third-party organisations. Whilst in earlier times control over personal data may have been best undertaken by preventing the data from being disclosed, in an internet enabled society it is increasingly important to understand how disclosed data is being used and reused and what can be done to control this further use and reuse.

Consent to the processing of personal data is probably the most important mechanism that currently exists for determining how and when this data can be used. The notion of informed consent, for example, originated in the context of medical research and the development of the Nuremberg Code which clearly established the right to withdraw from medical research, effectively revoking any consent that was given or implied (Hoeyer, 2009).

For informed consent to be meaningful, it is generally acknowledged that the individual giving the consent should understand what they are giving consent to (raising important questions about informed consent in the context of the young (Dowty, 2009), the dying and mentally handicapped (Hoeyer, 2009)). Informed consent is also meaningless if the individual has no choice about providing their consent (“Hobson’s consent”). This lack of choice can arise in cases where data is collected for statutory purposes (such as data relating to your income tax obligations). In other cases, individuals may find that they have to provide data and consent to its use in order to gain access to electronic sources and services.

It is not always necessary to obtain consent for the use of personal data. For example, the UK’s Information Commissioner Office has recently issued a code of practice about Privacy Notices (Information Commissioner's Office, 2009) which states:

There is a fundamental difference between telling a person how you’re going to use their personal information and getting their consent for this. In many cases it is enough to be transparent. In other cases a person’s positive agreement will be needed. This is most likely to be the case where sensitive information is being collected, or where previously collected information is to be used in a significantly different way (p. 8).

There are also complications associated with obtaining informed consent in online contexts. For example, in April 2008, Data Protection Regulators from across the European Union released their opinion on the processing of personal data by search engine providers. In that document, the “Article 29 Working Party” recommended that search engine providers must obtain consent from their users before engaging in any data collection or profiling. In and of itself, this was a controversial conclusion for industry and civil society organisations.

Further complications arose from the Working Party’s requirement that service providers enable both authenticated and non-authenticated users to provide consent (LSE Policy Engagement Network, 2009). For authenticated users, it is possible to explicitly ask them to give consent to the data profiling activities and to record details of the consent given

alongside the details of the authenticated user. For example, when logging in to the service, the user may be asked to agree to the processing by ticking a box. Details of when the box was ticked could then be stored in the system. However, for non-authenticated users the problem is more complex. What mechanisms can exist to allow the same non-authenticated user to indicate that they have given (or refused) consent for certain data processing activities (especially if they access the service from various computational devices)?

“Natural consumer behaviour” adds even further complexity to the question of informed consent as very few individuals will read and understand the privacy notices that they are presented with and simply click-through and accept them (McRobb & Rogerson, 2004; Milne & Culnan, 2004). At most, individuals might opt-in or opt-out of various marketing options although all too often these are not worded clearly (Information Commissioner’s Office, 2009).

Various privacy risks (Solove, 2002) highlight a further important complexity, namely the extent to which individuals can fully understand and meaningfully evaluate the various risks and harms that their personal data might be subject to. Whilst some obvious risks might be readily apparent to a reasonably well informed individual (e.g. not sending credit card details over a non-https link—i.e. a connection that doesn’t have a closed padlock symbol), others may be less well understood and less easily verified, for example, it would be difficult to determine the patch policy of the enterprise or how proactive its network intrusion detection mechanisms were (Goodall et al., 2009; Arora et al., 2009), and thus difficult to evaluate how likely it is that the data is held securely.

Having given consent for the processing of personal data (regardless of how effectively that consent was given) it would seem reasonable for individuals to be able to revoke that consent at a later stage, that is to indicate that any consent previously given was no longer valid (and, symmetrically, for any previously declined consent to be replaced with newly given consent). However, thinking of control of personal data in terms of giving and revoking consent has had very limited traction in the extant literature whose notion of control has been limited to controlling the disclosure of data. The next section reviews some recent studies of privacy to demonstrate just how dominant this limited view of control has been.

### **3 EMPIRICAL TESTS OF INFORMATIONAL PRIVACY CONTROL**

In the literature online privacy concerns have been particularly associated with issues of trust in e-commerce (Dinev & Hart, 2006), internet use (Son & Kim, 2008) and personalization (Awad & Krishnan, 2006) with many studies noting that concerns about privacy may limit the ways in which individuals interact with organisations online, for example by refusing to disclose data or misrepresenting themselves to the company (Son & Kim, 2008).

Several studies have sought to model the concerns that individuals have about information privacy (Malhotra et al., 2004; Stewart & Segars, 2002), drawing on previous work by Smith et al. (1996). Issues of control are frequently mentioned in these studies, for example, Hann et al. (2002) note in a footnote that “Control was commonly operationalised by allowing information to be disclosed only with the subjects’ permission” ( footnote 3) and Alge et al.

(2006) adding a second facet to their model: once data has been collected “how much control one believes he or she has over the handling of information (use and dissemination)” (p. 222).

Culnan and Armstrong (1999) suggest that (perceived) procedural fairness may make individuals more likely to disclose personal data to an organisation and suggest that giving the consumer “voice and control” over actual outcomes is one way to contribute to perceptions of procedural fairness (Milne & Rohm, 2000). They propose fair information practices (c.f. Bonner & Chiasson, 2005) as a basis for this voice and control, but then limit the amount of control they propose by stating:

People will also have the right to control how their personal information will subsequently be used by objecting to uses of their personal information when information will be collected for one purpose and used for other purposes (Culnan & Armstrong, 1999 p. 107)

They note that, in the context of marketing, “a central element of fair information practices is the ability of individuals to remove their names from mailing lists” (p. 107). This echoes one of the privacy-protective responses proposed by Son and Kim (2008). That paper aims “to offer a systematic understanding of a variety of internet users’ information privacy-protective responses”, yet their analysis of potential responses to privacy concerns focuses on refusal to provide information, the provision of falsified data or using opt-out procedures. Following Culnan and Armstrong (1999) they suggest that to increase perceived fairness, online companies “need to give their customers a certain level of control over the collection and use of their personal information” (Son & Kim, 2008). The example they give of this level of control, however, is limited to giving consumers the choice of whether to be included in the database to receive targeted marketing messages.

In a similar manner, Malhotra et al. (2004) use social contract theory to suggest that a firm’s collection of personally identifiable data is only likely to be perceived to be fair when the consumer is granted control over the data and informed about the firm’s intended use of it, but once again control appears to be limited to manifestations in terms of the existence of voice or exit such as opt-out.

Stewart and Segars (2002) also acknowledge the need to give consumers control over their data but provide limited insight into how this might be achieved. They report that “consumers are less likely to view a given information practice as privacy invasive if they are able to maintain, *even to a small degree*, some measure of control over their personal information” (pp. 39–40, emphasis added). The examples of this “small degree” of control include asking consumers for permission to use their personal information for secondary purposes or providing access to their data to verify its accuracy. “Consumer control is also communicated on behalf of companies when they state on application forms that any personal information collected will not be shared with any other organization” (p. 40). These extra controls that are proposed are, in Europe at least, statutory minimum requirements specified by EU and national laws, such as the UK Data Protection Act 1998 and not dissimilar to U.S. regulations affecting, for example, direct marketing (Petty, 2000).

In another study, Hui et al. (2007) suggest that requests for personal data from consumers may create “disutility”. This could be due to the risk of information misuse as “once a firm possesses consumer data, it is difficult for consumers to remove them or control their future use” (p. 21). They continue by stating that “obviously”, firms need to commit to use

consumer data responsibly and should convey this commitment to consumers. Thus, the control over personal data once disclosed in this scenario is limited to the responsible actions of the organization (and, implicitly, any enforcement methods available to the providers of privacy signalling mechanisms such as privacy seals).

Van Dyke et al. (2007) introduce the construct “privacy empowerment” in an attempt to measure the effects of giving consumers more control over their personal data than the fair information processing principles of notice, choice and access. Although they don’t measure any actual privacy empowerment, using instead the proxy measure perceived privacy empowerment, their survey found that “those firms which meet the demand for control through empowering the consumer are rewarded with lower levels of privacy concern and increased trust” (p. 78).

## 4 REVOCATION

As the previous sections have demonstrated, although control is widely understood to play a significant role in relation to issues of privacy and consent, the conceptualisation of control is typically limited. That is, many of the studies see control as little more than the fair information processing principles of notice, choice and access coupled with, at best, the ability to opt-in or out of marketing lists. Whilst this is understandable given the mainframe based systems that existed in the 1950s and 1960s, it becomes somewhat limited given the range and flexibility of modern computer systems where notions of user centricity are increasingly coming to the fore. Users are increasingly able to create and manage their own regulatory environments (Tsiavos et al., 2003). For example, they may choose to pay to use tools without spyware rather than using free, spyware driven packages (Mlcakova & Whitley, 2004) and in the same way are expecting more control over how their personal data is used.

The EnCoRe project seeks to address the limited conceptualisations of privacy control by explicitly exploring the notion of revocation as a form of user-driven privacy control. As noted above, while consent is often implicit in the collection of personal data, other than opt-in / opt-out mechanisms there is little consideration of the situation where an individual may choose to change the consent variables associated with an enterprise. For example, an individual may wish to change the consent that has previously been given or withheld, may wish to change the period for which consent is given or may wish to alter the kinds of secondary uses that they had consented to their data being used for.

These changes may arise for a variety of reasons. They may be triggered by changes in the market place such as when the company they had previously given their consent to is bought out by a competitor or when the company chooses to relocate its data centre overseas. They may be triggered by increased awareness of data protection risks following high profile data breaches. They may be triggered by the disclosure of unexpected detail about the secondary uses that the data is put to such as when a medical research company reveals that it uses medical data for research funded by pharmaceutical companies. Changes in consent may result following receipt of unsolicited / unexpected marketing materials (junk mail and spam) or simply at the whim of the individual.

The revocation of consent, however, can mean a variety of different things depending on the circumstances and statutory / constitutive purposes that the data is being held for. It is

helpful, therefore, to differentiate between revoking the right to hold personal data and revoking the right to use personal data for particular purposes. Thus, when contractual relationships with a service provider come to an end, individuals may revoke the right for that organisation to hold their personal data. It is, however, meaningless to revoke the right to hold data about them while the contractual relationship is ongoing. In such cases, however, they may choose to revoke the right to use their personal data in particular ways.

Further refinements are required for understanding what is meant by revocation in the context of organisational systems. For example, there are likely to be different levels of revocation that are either available to organisations (depending on their existing technology infrastructures) or requested by individuals. For some individuals, the details of revocation may be irrelevant as long as the revocation is performed correctly. For others, revoking the right to hold might be implemented by marking a particular record as no longer 'being live'. In other circumstances, revoking the right to use might require the deletion of records and, in extreme cases, this might require the deletion of the data from backups and physically grinding the hard disks to dust to ensure that no trace of the record remains. Thus a challenge ensues in determining how the data may be removed and yet at the same time it can be verified that it was processed, and proved to be processed, in accordance with the user's wishes.

There are also challenges with ensuring that consent and revocation preferences are associated with the personal data they refer to both within and beyond the organisation's boundaries. This is particularly the case for revocation of the right to use certain items of personal data for particular purposes. For example, revoking the right to use medical data for research purposes by a certain organisation requires the revocation preference to be associated with the medical data, including details of which organisations may and may not use it and ensuring that if the data is passed on to a third party, those preferences remain with them. The use of cryptographically enabled "sticky policies" and interoperability standards are being explored as possible solutions to these issues as consent and revocation preferences can change over time and yet within any large enterprise, the use and location of data is likely to be dispersed across multiple, distributed systems.

Control, therefore, also arises for revocation but control in this context is an engineering concept rather than a desirable social attribute of an exchange process. That is, issues of control quality come to the fore as it may be possible to offer and implement different forms of consent and revocation control, with differing degrees of assurance and auditability. Control becomes multi-faceted and organisations can choose from a range of different levels of revocation tied to the degrees of system refresh they are undertaking. In the same way that software development has the Capability Maturity Model (CMM) for process maturity in software development, so individuals may choose to interact with those organisations whose revocation maturity level is highest in the market.

## **5 A RESEARCH AGENDA FOR THE NEW UNDERSTANDING OF CONTROL IN THE PRIVACY ARENA**

The space opened up by this new understanding of control in the privacy arena raises a number of research and development challenges, many of which are being addressed by the EnCoRe project. Of particular significance to individuals and organisations is the shift to

user-centric controls implicit in this view of consent and revocation. In this view control over personal data is no longer something that is managed by organisations beneficently on behalf of individuals, instead individuals (about whom the data relates) have the opportunity to take an active role in the control and management of their personal data.

Such a shift is, of course, not without its problems. It implies a sophisticated user and an intuitive interface to specify consent variables (or, at the very least, a range of meaningful default values). As Schwartz (2000) warns with his metaphor of the blinking 12:00 on the microwave, even setting basic values may be considered to be too complex a task for many users and their awareness and appreciation of the various risks associated with the processing of their personal data may also be very limited.

In particular, given that most users simply click through any privacy / consent notices can steps be taken to ensure that their consent and revocation is considered to be more meaningful than these default actions and can anything be done to ensure that the status of any revocation request has appropriate legal / contractual force, for example by requiring enterprises to confirm, on a regular basis, that consent is still valid? Similarly, how “paternalistic” should default consent and revocation values be for any service offering this functionality?

An important business concern for revocation is how to ensure revocation compliance throughout the supply chain. If an individual revokes consent with the original service provider this needs to pass through the supply chain to all other service providers who are handling the data and the original service provider (and individual) need assurance that the revocation has taken place through the chain. Providing auditable, privacy friendly proof of compliance is a challenge both technologically and legally.

Implementing effective consent and revocation mechanisms is a mode 2 type problem (Gibbons et al., 1994) as it raises technological, legal and business challenges that don't neatly fall within discipline based boundaries. One of the main challenges that EnCoRe is facing, therefore, is to operate effectively in this space. Opening up our understanding of control over personal data is one step towards this goal.

## **6 ACKNOWLEDGEMENTS**

The ideas expressed in this paper have emerged from the various EnCoRe project meetings. In particular, the question of how control was conceptualised in the privacy literature was first raised in discussion between Simon Wiseman and Paul Hopkins. The paper has benefitted from discussions with all members of the project team and particular thanks are due to Sadie Creese, Liam Curren, Paul Hopkins, Gus Hosein and Jane Kaye for their insights and suggestions on drafts of the paper.

## **7 ABOUT THE AUTHOR**

Edgar Whitley is a reader in information systems in the Department of Management at the London School of Economics and Political Science. He is co-editor of the journal *Information Technology and People* and an associate editor for *MIS Quarterly*. In addition to his work on EnCoRe, he is also a member of the BCS Information Privacy Expert Panel

and research co-ordinator for the LSE Identity Project. His book, *Global challenges for identity policies*, co-written with Gus Hosein, was published by Palgrave in 2009.

For more information about EnCoRe, see [www.encore-project.info](http://www.encore-project.info)

## 8 REFERENCES

Alge BJ, Ballinger GA, Tangirala S and Oakley JL (2006) Information Privacy in Organizations: Empowering Creative and Extrarole Performance. *Journal of applied psychology* 91(1), 221-232.

Allen AL (1999) Coercing Privacy. *William and Mary Law Review* 40(3), 723-757.

Arora A, Krishnan R, Telang R and Yang Y (2009) An Empirical Analysis of Software Vendors' Patch Release Behavior: Impact of Vulnerability Disclosure. *Information Systems Research* Forthcoming,

Awad NF and Krishnan MS (2006) The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly* 30(1), 13-28.

Bonner W and Chiasson M (2005) If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy. *Information and Organization* 15(xx), 267-293.

Ciborra CU and Lanzara GF (1994) Formative contexts and information technology: Understanding the dynamics of innovation in organizations. *Accounting, management and information technologies* 4(2), 61-86.

Culnan MJ and Armstrong PK (1999) Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation *Organization Science* 10(1), 104-115.

De Hert P (2008) Identity management of e-ID, privacy and security in Europe. A human rights view. *Information Security Technical Report* 13(2), 71-75.

DeCew J (1997) *In Pursuit of Privacy: Law, Ethics and the Rise of Technology*. Cornell University Press, Cornell.

Dinev T and Hart P (2006) An extended privacy calculus model for e-commerce transactions. *Information Systems Research* 17(1), 61-80.

Dowty T (2009) Protecting the Virtual Child – the law and children’s consent to sharing personal data Action on Rights for Children Archived at <http://www.archrights.org.uk/issues/Virtual%20Child.htm>

Gibbons M, Limoges G, Nowotny H, Schwartzman S, Scott P and Trow M (1994) *The new production of knowledge: The dynamics of science and research in contemporary societies*. Sage, London.

Goodall JR, Lutters WG and Komlodi A (2009) Developing expertise for network intrusion detection *Information Technology and People* 22(2), 92-108.

Hann I-H, Hui K-L, Lee TS and Png IPL (2002) Online information privacy: Measuring the cost-benefit trade-off. In *Twenty-Third International Conference on Information Systems*.

Hoeyer K (2009) Informed consent: The making of a ubiquitous rule in medical practice. *Organization* 16(2), 267-288.

Hui K-L, Teo HH and Lee S-YT (2007) The value of privacy assurance: An exploratory field experiment. *MIS Quarterly* 31(1), 19-33.

Information Commissioner's Office (2009) Privacy notices code of practice Archived at [http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guide/s/privacy\\_notices\\_cop\\_final.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guide/s/privacy_notices_cop_final.pdf)

Introna LD (1997) Privacy and the computer: Why we need privacy in the information society. *Metaphilosophy* 28(3), 259-275.

Kanellopoulou N (2009) Legal Philosophical Dimensions of Privacy. *EnCoRe briefing paper*

LSE Policy Engagement Network (2009) From legitimacy to informed consent: mapping best practices and identifying risks A report from the Working Group on Consumer Consent Archived at [http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/consent\\_report.pdf](http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/consent_report.pdf)

Malhotra NK, Kim SS and Agarwal J (2004) Internet users' information privacy concerns (IUIPC): The construct, the scale and a causal model. *Information Systems Research* 15(4), 336-355.

McRobb S and Rogerson S (2004) Are they really listening?: An investigation into published online privacy policies at the beginning of the third millennium. *Information Technology and People* 17(4), 442-461.

Milne GR and Culnan MJ (2004) Strategies for Reducing Online Privacy Risks: Why consumers read (or don't read) online privacy notices. *Journal of interactive marketing* 18(3), 15-29.

Milne GR and Rohm AJ (2000) Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives. *Journal of public policy & marketing* 19(2), 238-249.

Mlcakova A and Whitley EA (2004) Configuring peer-to-peer software: An empirical study of how users react to the regulatory features of software. *European Journal of Information Systems* 13(2), 95-102.

Petty RD (2000) Marketing without consent: Consumer choice and costs, privacy and public policy. *Journal of public policy & marketing* 19(1), 42-53.

Schwartz PM (2000) Beyond Lessig's CODE for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices. *Wisconsin Law Review* (4), 743-788.

Smith HJ, Milberg SJ and Burke SJ (1996) Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly* 20(2), 167-196.

Solove DJ (2002) Conceptualizing Privacy. *California Law Review* 90, 1087-1155.

Son J-Y and Kim SS (2008) Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly* 32(3), 503-529.

Stewart KA and Segars AH (2002) An empirical examination of the concern for information privacy instrument. *Information Systems Research* 13(1), 36-49.

Tsiavos P, Hosein IR and Whitley EA (2003) The footprint of regulation: How information systems are affecting the sources of control in a global economy. In *Organizational information systems in the context of globalization* (Korpela M, Montealegre R and Poullymenakou A, Eds), pp 355-370, Kluwer, Athens, Greece.

Van Dyke TP, Midha V and Nemati H (2007) The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce. *Electronic markets* 17(1), 68-81.

Warren S and Brandeis L (1890) The right to privacy. *Harvard Law Review* 4, 193-220.

Westin AF (1967) *Privacy and Freedom* Atheneum Press, New York.

Whitley EA (2009) Perceptions of government technology, surveillance and privacy: the UK identity cards scheme. In *New Directions in Privacy and Surveillance* (Neyland D and Goold B, Eds), pp 133-156, Willan, Cullompton.

Wittgenstein L (1956) *Philosophical investigations*. Basil Blackwell, Oxford.