Digital Enlightenment Yearbook 2013
M. Hildebrandt et al. (Eds.)
IOS Press, 2013

doi:10.3233/978-1-61499-295-0-165

Towards Effective, Consent Based Control of Personal Data

Edgar A. WHITLEY
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. The principle of consent is widely seen as a key mechanism for enabling user-centric data management. Informed consent has its origins in the context of medical research but the principle has been extended to cover the lawful processing of personal data. In particular, the proposed EU regulation on data protection seeks to strengthen the consent requirements moving them from unambiguous to explicit. Nevertheless, there are a number of limitations to the way that even explicit consent operates in real-life situations which suggest that an alternative, more dynamic form of consent is needed. This chapter reviews the key concerns with static forms of consent for the control of personal data and proposes a technologically mediated form of dynamic consent instead.

Keywords. Privacy, consent, dynamic consent, biobanking

Introduction: The Problem of Privacy and Consent[1]

Notions of consent are becoming increasingly important in questions of data protection and privacy. Leading privacy advocate Simon Davies compiled a report on the issues and trends that will dominate the privacy landscape in 2013 [1]. This report drew on a survey of over 180 privacy specialists from 19 countries. They were asked to identify the most influential privacy themes for 2013 and consent was listed third (after data aggregation and regulatory changes). Consent is also a key feature of the proposed EU regulatory changes regarding data protection (where it is understood as "clear, affirmative consent") [2].

Consent is a key feature of many privacy principles and features in many existing data protection guidelines and regulations, including the UK's Data Protection Act [3]. It is found (expressly or implied) in industry best practice and most notions of fair information processing as well as their implementation in various data protection regulations and guidelines. As such, informed consent is likely to be a significant issue for most public and private sector enterprises that handle personal data, whether for day-to-day operations or for innovative applications.

Much of our understanding of informed consent has its origins in what is seen as ethical medical practice. The importance of requiring informed consent from patients can be traced back at least to the abuses of medical practice in the Second World

[1] This chapter draws on work undertaken as part of the EnCoRe project funded by the Technology Strategy Board (Grant TP/12/NS/P0501A) and the Engineering and Physical Sciences Research Council and the Economic and Social Research Council (Grant EP/G002541/1).

War [4]. As a result, obtaining informed consent from patients, and the limitations of what is covered by this informed consent, directly influence the use of medical data and samples. For example, Dame Fiona Caldicott's review of information sharing for the UK Department of Health [5] noted the importance of allowing people to "give, refuse or withdraw explicit consent" and the need to ensure that these decisions are "traceable and communicated to others involved in the individual's direct care" [5, p.13]. The report continued by reiterating the Helsinki principle that "Patients can change their consent at any time" [5, p. 13].

Consent, however, is a multi-faceted concept that is all too often 'black-boxed' and treated as unproblematic. For example, under UK law, consent is not actually required for all forms of data processing and there are very significant practical issues around how "informed" consent might be operationalized [6].

From an enterprise perspective, for online consent to work companies need to ensure that the person who is expressing the consent is in fact the relevant user and not someone else. One illustration of this is Facebook's requirement that all new accounts are opened with the person stating their age. This is intended to allow Facebook to filter age-restricted services, adverts and applications. It also relates to their terms of service which states that "You will not use Facebook if you are under 13" [7, 4 Registration and account security, condition 5] and is a direct consequence of the US Children's Online Privacy Protection Act (COPPA). However, as Boyd et al. [8] note, Facebook is currently such a desirable space for young children to use that parents are increasingly being pressurized into giving 'parental consent' and setting up accounts on Facebook for them (typically by having the parent knowingly lie about the child's age thus totally undermining the safeguards introduced by the service provider).

1. Data Protection and Consent

In January 2012, the EU put forward proposals for the fundamental reform of data protection within Europe [2]. The proposals are wide ranging and update and modernize the principles enshrined in the 1995 Data Protection Directive [9] to guarantee privacy rights. They focus on reinforcing individuals' rights, strengthening the EU internal market, ensuring a high level of data protection in all areas (including police and criminal justice cooperation): proper enforcement of the rules, facilitating international transfers of personal data and setting global data protection standards [10].

A key feature of the proposed changes is that they are intended "to give people more control over their personal data… Wherever consent is required for data to be processed, it will have to be given explicitly, rather than assumed as is sometimes the case now" [10]. As such, it refines the earlier "Madrid Resolution" on international privacy standards [11].

The influential "Article 29" Working Party of the EU released an "opinion" on consent in 2011 [12]. That opinion "provides a thorough analysis of the concept of consent as currently used in the Data Protection Directive and in the e-Privacy Directive". It notes that the Council Common Position in 1995 introduced a standard definition of consent. Consent is defined as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed". However, even this definition has resulted in areas of confusion and ambiguity.

The opinion gives "numerous examples of valid and invalid consent, focusing on its key elements such as the meaning of 'indication', 'freely given', 'specific', 'unambiguous', 'explicit', 'informed' etc.". These examples, which are drawn from the experiences of members of the Working Party, attempt to clarify some aspects related to the notion of consent, including questions about the timing as to when consent must be obtained and how the right to object differs from consent, etc.

That the Working Party felt it necessary to clarify this (fundamental) area of data protection law and practice is indicative that the concept of consent raises many legal and practical consequences which were not necessarily anticipated when the Directive was originally drafted.

Raab and Goold [13] further suggest that "it is debatable whether 'consent' should be a further (data protection) principle in its own right, or whether – because it is so difficult to define and apply in practice – it should only play a supportive role to the package of other principles" [13, p. 63] and note that as consent is frequently set aside (see below) and is difficult to obtain it is open to question whether it should form the basis for an informational self-determination foundation for privacy.

Before focusing on the problematic issues associated with consent, it is important to recognize that consent is not the only basis upon which data may be lawfully processed. For example, under the UK Data Protection Act [3] the fair processing conditions are:

- Processed with the consent of the data subject;
- Required by contract, or pre-contractual negotiations, with data subject;
- Legal obligation for data controller to process the personal data;
- Necessary to protect the "vital interests" of the data subject;
- Necessary for the administration of justice, parliament, under an Act, crown/government, public interest;
- Necessary for the "legitimate interests" of the data controller/third party unless the "processing is unwarranted… by reason of prejudice to the rights and freedoms or legitimate interests of the data subject", unless ordered otherwise by Secretary of State.

That is, consent is only one (of six) possible conditions for lawful processing of personal data in the United Kingdom.

1.1. Article 29 Working Party Concerns

The Article 29 Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC [14]. The Working Party issues opinions on a range of issues associated with data protection and privacy including technological developments such as search engines [15]. It also reviews the changing technological basis of key data protection terms such as the concepts of data controller and data processor [16].

In 2011 it issued an opinion on the definition of consent [12], and the question of consent also arose in relation to online behavioral advertising [17]. The Working Party argued that a key feature of consent is transparency towards the data subject. "Transparency is a condition of being in control and for rendering the consent valid. Transparency as such is not enough to legitimize the processing of personal data, but it is an essential condition in ensuring that consent is valid" [12].

Another important issue relates to how consent is signified and the timing of this signification. Thus, although not explicitly stated in legislation, the use of consent implies that processing cannot start until consent is granted, so consent must generally be given before processing starts. This is related to, but different from, the right of objection [cf. 18]. Consent, broadly defined, can be any form of "indication" of the data subject's wishes, although the working party argues that it should really involve some purposeful action (rather than consent being inferred from a lack of action). At present, continued use (for example of an online service) is frequently taken to be an "indication" that the data subject provides consent for processing to be performed.

Consent must also be 'freely given' and this condition raises the prospect that consent choices might be engineered (see below) and the set of default values for consent options is also important (cf. opt-in versus opt-out considerations [19]). Moreover, to avoid consent being seen as "Hobson's consent" [20] the data subject must have a choice of options available. For example, if consent (perhaps to be added to a marketing mailing list) must be given in order for an online purchase to be completed then this consent is arguably not freely given.

Another requirement of consent articulated by the Working Party is that it should be "specific". Indeed, the opinion states that "blanket consent without specifying the exact purpose of the processing is not acceptable" [12, p. 17]. That is, consent "should refer clearly and precisely to the scope and the consequences of the data processing. It cannot apply to an open-ended set of processing activities" [12, p. 17], although there are important distinctions between telling a person how you are going to use their personal information and getting their consent for this [21, p. 8]. Informed consent also raises important issues of the intelligibility of the description of the purposes for which data is processed [21–23] and their readability [e.g. 24,25].

2. Consent and Control

The Article 29 Working Party review of consent [12] emphasizes the relationship between consent and control. Indeed, many surveys of the literature on privacy identify the central role played by an individual's control over the use of their personal data [26,27]. For example, Introna's [28] review 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 judgment 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 [29], who developed a right of privacy, namely "the right to let alone", based on an earlier judgment by Thomas Cooley, who proposed "the right to one's person and a right of personal immunity" [see 30, 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.

The Warren and Brandeis definition, therefore, both falls within Introna's first and second categories 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 [31], 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 judgment 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 [32].

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?" [28, 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).

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 [33] 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" [33, 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 organizations. 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.

2.1. Academic Studies of Informational Privacy Control

In the literature, online privacy concerns have been particularly associated with issues of trust in e-commerce [34], internet use [35] and personalization [36] with many studies noting that concerns about privacy may limit the ways in which individuals interact with organizations online, for example by refusing to disclose data or misrepresenting themselves to the company [35].

Issues of control and procedural fairness [37] are frequently mentioned in these studies, for example, Hann et al. [38] note in a footnote that "Control was commonly operationalized by allowing information to be disclosed only with the subjects' permission" [23, footnote 3] and Alge et al. [39] add 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)" [22, p. 222].

Similarly, Son and Kim [35] suggest that online companies "need to give their customers a certain level of control over the collection and use of their personal information" to increase perceived fairness. Unfortunately, the example they give of this level of control is limited to giving consumers the choice of whether to be included in the database to receive targeted marketing messages [see also 40].

Indeed, for some authors consumer control is limited to something that is "communicated on behalf of companies when they state on application forms that any personal information collected will not be shared with any other organization" [41, p. 40].

2.2. Engineered Consent

Questions about the nature of human agency have attracted the attention of numerous philosophers and social scientists. In relation to privacy, discussions have ranged from Jeremy Bentham's Panopticon [42] through Foucault's disciplinary structures [43] to contemporary discussions about behavioral 'nudges' [44].

This last category of studies highlights the important role of a "choice architect" setting appropriate default settings and taking advantage of norms of behavior. For example, if the empirical evidence suggests that most people don't actively monitor and manage their pension funds then a libertarian paternalist position would propose setting up individuals with a well-performing generalist pension as a default whilst also allowing them to change their pension provider if they choose to.

In the context of privacy and consent, Kerr et al. [45] examine the ways in which the consent-gathering process is frequently "engineered to skew individual decision making" [45, p. 8]. Whilst such activities create an illusion of free choice, they call into question the underlying premise of truly informed, freely given consent. In particular, they highlight the risk that "the full potential of the consent model may be compromised in practice due to predictable psychological tendencies that prevent people from giving fully considered consent, and withdrawing it once given" [45, p. 15].

To illustrate this point, Kerr et al. [45] present a hypothetical example of a privacy-concerned individual being told about a useful "breaking news story alert" functionality provided by their favorite newspaper. Unfortunately, in order to obtain this functionality, they are required to register with the online newspaper, disclose various pieces of personal data and consent to various uses of this data.

Thus, for the individual to gain the immediate benefits of the service, they must accept loss of control over the personal data that is disclosed to the newspaper. Although legally they are able to revise this initially given consent, Kerr et al. [45] argue that people will tend to provide the required personal information and offer their consent if the perceived benefits of the alerting service outweigh the perceived costs.

From a 'nudge' perspective, it is apparent that subscribing to the alerting service results in an immediate and positive gain. Against this needs to be balanced the subjective loss of control and important future consequences regarding uses of the data. Similarly, revoking consent at some point will result in an immediate loss of benefit (no more alerting messages received) and a potential long term advantage (data not being (mis)used by unknown third parties).

In each case, Kerr et al. [45] point out that the subjective utility of the decisions are heavily skewed. A variety of behavioral studies have shown that, in general, the subjective utility of a benefit change is more pronounced when it happens now rather than at

some point in the future. There is also evidence that the rate of change in subjective utility is faster for gains than for losses. Accordingly, "an immediate gain against a temporally distant loss of privacy, rendered less negative precisely because it occurs in the future" is more likely to result in consent being given than "if both outcomes occurred at the same time" [45, p. 17].

Similarly, a decision to revoke consent would evaluate an immediate loss against "a temporally distant gain whose value is much reduced because it occurs in the future" [45, p. 18]. Furthermore, there is growing evidence that losses are weighted more heavily in decision making than gains [e.g. 46].

Other academics question the true role of seeking informed consent in many organizational settings. For example, Heimer [47] studies the use of consent forms in the context of HIV/AIDS health care. She suggests that a primary use of the signed form is to act "as a shield for the organization should questions be raised about the study" [47, p. 21]. Moreover, "the 'consenting' of research subjects often follows rather than precedes the decision to participate. People arrive at the point of being 'consented' having already made a considerable investment in research participation" [47, p. 23].

A similar point is made by Anderson and Agarwal [48] who, noting the effect of emotions on health decisions, raise important policy questions regarding the timing of the consent process. "If people's judgments vary with their emotions related to their health at a given point in time, should consent be sought at every interaction with a healthcare professional?" [48, p. 486].

3. Towards a Dynamic Model of Consent Data

These concerns about consent shaped a large inter-disciplinary research project into informational privacy, undertaken collaboratively by UK industry and academia. The EnCoRe project [49] ran from June 2008 to April 2012 and included Hewlett Packard Laboratories, HW Communications Ltd, the London School of Economics and Political Science, QinetiQ, the Computer Science Department and the Centre for Health, Law and Emerging Technologies (HeLEX), University of Oxford as partners. The project ran alongside two other projects (VOME [50]; and PVNets [51]) within the same funding program.

EnCoRe's work started with what might be termed "natural consumer behaviour". For the reasons outlined above, it soon became clear that despite the legal and ethical requirements underlying consent, it was unreasonable to expect that all forms of consent would really be informed and freely given, instead consent is often given without individuals reading the terms and conditions of the proposed service or reflecting on the implications of their choice. As a result, EnCoRe came to consider consent as a dynamic (and changeable), rather than static, process.

To achieve this, the project sought to develop scalable, cost effective and robust consent and revocation methods for controlling the usage, storage, location and dissemination of personal data that would offer effective, consent based control over that data and would help restore individual confidence in participating in the digital economy.

In particular, by recognizing that the initially given consent might not have been fully informed or that the consent process might have been engineered to encourage the giving of consent, EnCoRe sought to develop mechanisms that would allow individuals to change their consent preferences over time (for example, when they became more

informed about the implications of the choices they had previously made or when their circumstances changed) rather than requiring them to be stuck with the initial consent choices made. Technological measures such as cryptographic 'sticky policies' helped ensure that these consent preferences remained associated with the data they referred to.

The underlying technical architecture for EnCoRe contains a number of core components [52] that support easy integration with bespoke or legacy systems. These components include a client-side, *Consent & Revocation Privacy Assistant* that supports data subjects' privacy preferences, a *System Configuration Database* that provides a centralized store of the schema, defined by administrators, describing how various types of privacy preferences are associated to personal data and the mapping of internal representations of types of personal data (e.g. names of data items within legacy databases, LDAP, etc.) to higher-level definitions used by EnCoRe.

Another component provides *Consent & Revocation Provisioning* and is the contact point between the organization's web server/portal and the EnCoRe components. Its purpose is to provide workflow-based coordination and provisioning capabilities. The *Data Registry Manager* is in charge of storing data subjects' privacy preferences, along with associations to the related personal data. This component also keeps track of the whereabouts of personal data, within and across organizations. The *Privacy – Aware Access Control Policy Enforcement* component is in charge of enforcing security & privacy access control policies on personal data, driven by data subjects' preferences. These policies takes account of preferences such as purposes for accessing data, entities the data may/may not be disclosed to, etc. It works in conjunction with the *Obligation Management System*. The system generates Audit Logs as each EnCoRe component is instrumented with a configurable agent to provide logging data. The *Audit Logs* component provides key information to support compliance checking.

Finally, the *Trust Authority* component is in charge of dealing with checking the fulfillment of sticky policies; the release of cryptography keys, subject to the fulfillment of policy constraints; audit logging; and forensic analysis [52].

The latest iteration of the dynamic consent model is currently being evaluated in the context of biobanking research in Oxford and Manchester. Biobanks are repositories of tissue samples and associated data that are available for researchers to use, subject to the consent of donors. The very nature of biobanks means that it is frequently impossible to specify all potential future uses of tissue samples, and biobanks often rely on broad consent and ethical oversight to determine acceptable uses of the tissue sample.

In this next stage of research, the study has been broadened to include consideration of interface issues. In particular, project partners HW Communications have developed a tablet-based implementation of the dynamic consent mechanism and integrated them with a broader, education and awareness portal that offers videos and other information about biobanking to patients as well as allowing them to manage their consent preferences dynamically, see Fig. 1.

Figure 2 shows how the biobank donor can learn more about their specific interactions with the biobank and update their consent choices. Figure 3 illustrates potential consent choices open to donors. The range of available consent choices is determined by the biobank and allows the donor to provide fine level control over the use of their sample and data; decisions that are normally made on behalf of patients by research governance committees. Such an approach will clearly have consequences for the ethical oversight of research and the views of researchers whose practices might have been

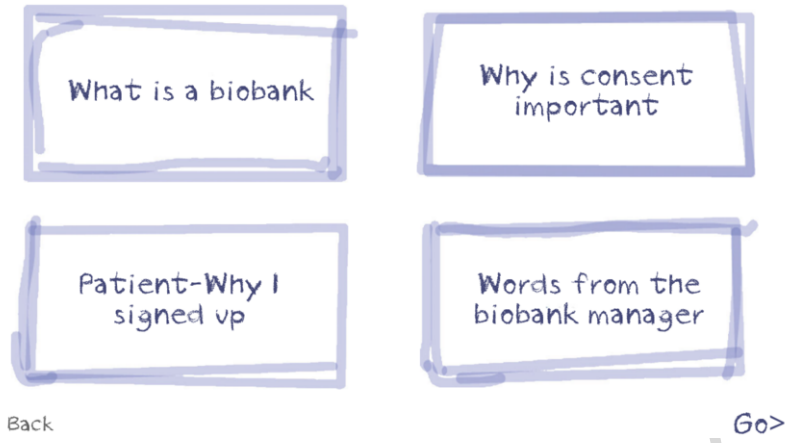

Figure 1. Interface that helps explain what biobanking involves.

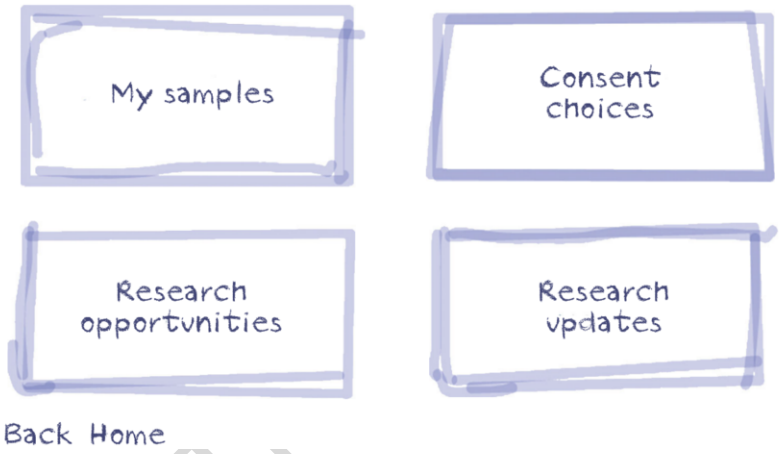

Figure 2. Information for the user.

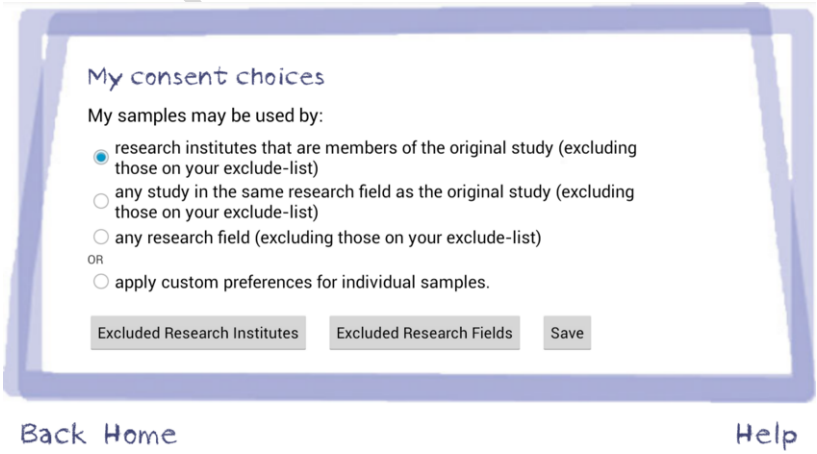

Figure 3. Sample consent choices.

affected by dynamic forms of consent were sought [53]. The attitudes of potential donors to dynamic consent are also being studied.

All too often, questions of consent are left black-boxed or treated as secondary to questions of privacy. This chapter has presented an overview of current thinking that seeks to explore the limits of consent as it is currently understood and operationalized. The chapter has presented an alternative, dynamic model of consent. The model emerges from a multi-disciplinary research group and combines technical architecture considerations with real-time risk assessment and compliance monitoring, as well as insights into the changing ethical and governance issues surrounding consent.

References

All URLs checked 24 June 2013

[1] S. Davies, The Privacy Surgeon: Predictions for privacy 2013. *LSE Enterprise* (January) 2013. Archived at http://www.privacysurgeon.org/blog/wp-content/uploads/2013/01/PS-future-issues-full-report.pdf.
[2] EU Commission proposes a comprehensive reform of the data protection rules (25 January) 2012. Archived at http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.
[3] OPSI Data Protection Act 1998. Archived at http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1.
[4] K. Hoeyer, Informed consent: the making of a ubiquitous rule in medical practice. *Organization* **16(2)**, (2009), 267–288.
[5] Department of Health Information: To share or not to Share: Information Governance Review (26 April) 2013. Archived at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf.
[6] Information Commissioner's Office Guidance on the rules on use of cookies and similar technologies (May) 2012. Archived at http://www.ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/~/media/documents/library/Privacy_and_electronic/Practical_application/cookies_guidance_v3.ashx.
[7] Facebook Facebook Legal Terms of Service. *Last modified 8 June 2012* 2013. Archived at http://www.facebook.com/legal/terms.
[8] D. Boyd, E. Hargittai, J. Schultz and J. Palfrey, Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act'. *First Monday* **16(11)**, (2011).
[9] EU Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (24 October) 1995. Archived at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.
[10] EU Data protection reform: Frequently asked questions (25 January) 2012. Archived at http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/41&format=HTML&aged=0&language=EN&guiLanguage=en.
[11] Madrid Resolution Data protection authorities from over 50 countries approve the "Madrid Resolution" on international privacy standards. *31st International Conference of Data Protection and Privacy* 2009. Archived at http://www.privacyconference2009.org/media/notas_prensa/common/pdfs/061109_estandares_internacionales_en.pdf.
[12] Article 29 Data protection working party Opinion 15/2011 on the definition of consent. *Article 29 Data Protection Working Party* (13 July) 2011. Archived at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.
[13] C. Raab and B. Goold, Protecting information privacy. *Equality and Human Rights Commission* 2011. Archived at http://www.equalityhumanrights.com/uploaded_files/research/rr69.pdf.
[14] Article 29 Data protection working party about us 2013. Archived at http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.
[15] Article 29 Data protection working party Opinion 1/2008 on data protection issues related to search engines. *WP 148* (4 April) 2008. Archived at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf.

[16] Article 29 Data protection working party Opinion 1/2010 on the concepts of "controller" and "processor". *WP 169* (16 February) 2010. Archived at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.
[17] Article 29 Data protection working party Opinion 16/2011 on on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising. *WP 188* (8 December) 2011. Archived at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf.
[18] L. Curren and J. Kaye, Revoking consent: A 'blind spot' in data protection law? *Computer Law & Security Review* **26(3)**, (2010), 273–283.
[19] N. Lundblad and B. Masiello, Opt-in Dystopias. *script-ed* **7(1)**, (2010), 155–165.
[20] C. Pounder, Facebook passwords and employment: why data protection works and Facebook's promise to take legal action to protect privacy doesn't. *Amberhawk* (28 March) 2012. Archived at http://amberhawk.typepad.com/amberhawk/2012/03/facebook-passwords-and-employment-why-data-protection-works-and-facebooks-promise-to-take-legal-action-to-protect-privacy.html.
[21] Information Commissioner's Office Privacy notices code of practice. *ICO* 2009. Archived at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_notices_cop_final.pdf.
[22] S. McRobb and S. Rogerson, Are they really listening?: An investigation into published online privacy policies at the beginning of the third millennium. *Information technology and people* **17(4)**, (2004), 442–461.
[23] I. Pollach, A typology of communicative strategies in online privacy policies: Ethics, power and informed consent. *Journal of Business Ethics* **62(3)**, (2005), 221–235.
[24] P.G. Kelley, L. Cesca, J. Bresee and L.F. Cranor, Standardizing privacy notices: An online study of the nutrition label approach. *CyLab, Carnegie Mellon University* (12 January) 2010. Archived at http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09014.pdf.
[25] G.R. Milne, M.J. Culnan and H. Greene, A Longitudinal Assessment of Online Privacy Notice Readability. *Journal of Public Policy and Marketing* **25(2)**, (2006), 238–249.
[26] F. Belanger and R.E. Crossler, Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly* **35(4)**, (2011), 1017–1041.
[27] H.J. Smith, T. Dinev and H. Xu, Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly* **35(4)**, (2011), 989–1015.
[28] L.D. Introna, Privacy and the computer: Why we need privacy in the information society. *Metaphilosophy* **28(3)**, (1997), 259–275.
[29] S. Warren and L. Brandeis, The right to privacy. *Harvard Law Review* **4**, (1890), 193–220.
[30] J. DeCew, *In pursuit of privacy: Law, ethics and the rise of technology.* Cornell University Press, Cornell, 1997.
[31] P. De Hert, Identity management of e-ID, privacy and security in Europe. A human rights view. *Information Security Technical Report* **13(2)**, (2008), 71–75.
[32] D.J. Willison, V. Steeves, C. Charles, L. Schwartz, J. Ranford, G. Agarwal, J. Cheng and L. Thabane, Consent for use of personal information for health research: Do people with potentially stigmatizing health conditions and the general public differ in their opinions? *BMC Medical Ethics* **10(1)**, (2009), 10.
[33] A.F. Westin, *Privacy and Freedom* Atheneum Press, New York, 1967.
[34] T. Dinev and P. Hart, An extended privacy calculus model for e-commerce transactions. *Information Systems Research* **17(1)**, (2006), 61–80.
[35] J.-Y. Son and S.S. Kim, Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly* **32(3)**, (2008), 503–529.
[36] N.F. Awad and M.S. Krishnan, The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly* **30(1)**, (2006), 13–28.
[37] M.J. Culnan and P.K. Armstrong, Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation *Organization Science* **10(1)**, (1999), 104–115.
[38] I.-H. Hann, K.-L. Hui, T.S. Lee and I.P.L. Png, Online information privacy: Measuring the cost-benefit trade-off. In *Twenty-Third International Conference on Information Systems*, 2002.
[39] B.J. Alge, G.A. Ballinger, S. Tangirala and J.L. Oakley, Information Privacy in Organizations: Empowering Creative and Extrarole Performance. *Journal of applied psychology* **91(1)**, (2006), 221–232.
[40] E.A. Whitley, Informational privacy, consent and the "control" of personal data. *Information security technical report* **14(3)**, (2009), 154–159.
[41] K.A. Stewart and A.H. Segars, An empirical examination of the concern for information privacy instrument. *Information Systems Research* **13(1)**, (2002), 36–49.
[42] J. Bentham, *Panopticon; Or, The Inspection-House: Containing The Idea of a New Principle of Construction applicable to any Sort of Establishment, in which Persons of any Description are to be kept under Inspection: And In Particular To Penitentiary-Houses, Prisons, Houses Of Industry, Work-*

Houses, Poor Houses, Manufactories, Mad-Houses, Lazarettos, Hospitals, And Schools: With A Plan Of Management adapted to the principle: in a series of letters, written in the year 1787, from Crecheff in White Russia. T. Payne, London, 1791.
[43] M. Foucault, *Discipline and punish.* Random House, New York, 1977.
[44] R.H. Thaler and C.R. Sunstein, *Nudge: Improving decisions about health, wealth and happiness.* Penguin, London, 2008.
[45] I. Kerr, J. Barrigar, J. Burkell and K. Black, Soft surveillance, hard consent: The law and psychology of engineering consent. In *Lessons from the identity trail: Anonymity, privacy and identity in a networked society* (I. Kerr, V. Steeves and C. Lucock, Eds.), pp. 5–22, Oxford University Press, Oxford 2009.
[46] A. Acquisti and J. Grossklags, What Can Behavioral Economics Teach Us About Privacy? *International Conference on Emerging Trends in Information and Communication Security (ETRICS),* (June) 2006.
[47] C.A. Heimer, Inert facts and the illusion of knowledge: Strategic uses of ignorance in HIV clinics. *Economy and Society* **41(1)**, (2012), 17–41.
[48] C.L. Anderson and R. Agarwal, The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research* **22(3)**, (2011), 469–490.
[49] EnCoRe About EnCoRe – Ensuring Consent and Revocation 2012. Archived at www.encore-project.info.
[50] VOME Visualisation and other means of expression 2012. Archived at http://www.vome.org.uk/.
[51] PVNets Privacy value networks 2012. Archived at http://www.pvnets.org/.
[52] EnCoRe Technical architecture (18 November) 2011. Archived at http://www.encore-project.info/ deliverables.html.
[53] E.A. Whitley, N. Kanellopoulou and J. Kaye, Consent and Research Governance in Biobanks: Evidence from Focus – groups with Medical Researchers. *Public health genomics* **15(5)**, (2012), 232–242.