The **Human Rights, Big Data and Technology** Project

Background Paper on Consent Online

E·S·R·C ECONOMIC & SOCIAL RESEARCH COUNCIL

Human Rights Centre | University of Essex

Consent Background Document

Contents

Introduction 2
Defining Consent 2
Consent in a human rights context 3
Background 4
Models of consent 4
Presumed consent 4
Informed consent 4
Active consent 4
Specific models of consent 5
Parameters of valid consent 5
Informed consent 6
Clarity and accessibility 6
Foreseeability 6
Specificity 6
Free consent 6
Control 7
Negotiating position 7
Unambiguous consent 7
Context of collection 7
Nature of data collected 7
Sample of issues to be addressed 8
Overarching questions to consider: 9

Introduction

'Datafication' of life[1] has led to individuals continuously generating data through their online and offline activities, without being fully aware of the kind of data they generate, how that data is collected, retained, or processed and what the implications of such uses may be. Problems thereby raised are made more complex as the value of information no longer solely resides in its primary purpose but is commonly collected with a – frequently unspecified or unknown - secondary use in mind.[2] These developments are at odds with the norms underpinning the central role assigned to individual consent to data gathering and use, raising questions as to the adequateness of existing legal mechanisms and safeguards.

Existing literature suggests that there is a considerable gap between the practice of informed consent and its intended goals, [3] revealing a need to reconcile the practical strategies and the normative principles meant to guide that practice. The concept and contours of consent need to be revisited. [4] Suggestions for improvement and development of the consent model focus on reducing risks and encouraging participation of the individual data subject. How can individuals have ongoing knowledge, access, control and ownership of their personal data? Is there a more fundamental question to be asked – is greater individual autonomy in this contractual relationship the linchpin? How can it help the individual to manage the increasing complexity of the information ecosystem?[5]

This paper will briefly introduce some background of the development of consent models and illustrate some of the key issues that must be addressed to close the gap between the intended goals of consent and the current practice. While the issues with consent online are not limited to the EU region, the General Data Protection Regulation (GDPR) will be used as a recent point of reference in which consent is heavily emphasized.

Defining Consent

GDPR defines consent in Article 4 (11) as follows.

> "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Consent is however only one of the legal basis for processing data. GDPR states that processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

---

[1] Datafication is defined as 'taking information about all things under the sun— including ones we never used to think of as information at all, such as a person's location, the vibrations of an engine, or the stress on a bridge— and transforming it into a data format to make it quantified'. See V. Mayer-Schönberger and K. Cukier, *Big Data. A Revolution That Will Transform How We Live, Work and Think* (John Murray Publishers, London, 2014), at 15. See also *ibid*., Chapter V.

[2] See, for example, G. D'Acquisto et al., 'Privacy by Design in Big Data. An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics', European Union Agency for Network and Information Security (2015), in particular Chapter 4.

[3] Christine Grady, "Enduring and Emerging Challenges of Informed Consent", The New England Journal of Medicine (2015), Vol. 372(9), p 856-857

[4] Ibid, p 857

[5] Omer Tene and Jules Polonetsky, "Privacy in the Age of Big Data: A Time for Big Decisions", Stanford Law Review Online (2012), Vol. 64, p 67

or, in the absence of consent,

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Consent in a human rights context

The requirement that consent must be given to use personal data draws strength from its link to the right to self-determination, within which is located the need to respect individual and group autonomy.

Respect for individual autonomy underpins international human rights law, given the law's focus on respecting and fulfilling *individual* rights and freedoms. This may be demonstrated, for example, by the importance attributed to the rights to privacy and freedom of expression.[6] In the context of data processing an individual's autonomy 'should make him – master of all those facts about his own identity, such as his name, health, sexuality, ethnicity, his own image […] and also of the "zone of interaction" […] between himself and others. He is the presumed owner of these aspects of his own self'.[7] To facilitate this autonomy, informational self-determination is a tool to allow the free development of an individual's personality, including interaction with other members of society on a free basis, thereby enabling free participation in society without fear of persecution.[8]

It is important to see what practical difference is made to the features of valid consent by this linkage to such a central feature of human rights.

[6] See, Articles 8 and 10, European Convention on Human Rights.
[7] *Wood v. Commissioner of Police for the Metropolis* [2009] EWCA Civ 414, para. 21.
[8] See, Brendan Van Alsenoy, Eleni Kosta & Jos Dumortier, 'Privacy notices versus informational self-determination: Minding the gap' (2014) 28 International Review of Law, Computers & Technology, p. 188.

Background

Models of consent

Consent is not a new requirement developed under GDPR but rather has been used historically in a wide range of settings, with some of its most active development originating in the medical industry. Below are three overarching models that demonstrate the origins of consent as can be found in regulation today. These three models have various impacts on the way an individual interacts with consent requests and what is required of any particular controller.[9]

Presumed consent

Under the presumed consent model the consent of the user is presumed; i.e. it is presumed that, by using a service, the user consents to the associated data processing. No explicit expression of consent on the part of the user is required, and so silence may be taken to signify consent. This model is dependent on two factors: first, the possibility of obtaining information in relation to how the data is processed, and, second, the ability to withdraw consent. It is argued that this model is consistent with the 1995 EU Directive, and that as such it resulted in 'the widespread adoption of an approach to compliance which comprised the publication of a privacy policy, a default presumption of consent, and a residual entitlement to opt-out.'[10]

Informed consent

The informed consent model represents a refinement of the presumed consent model. In light of developments relating to '[n]ew advanced digital technologies'[11] the informed consent model adopted under the 2002 Directive intended to particularise the definition of consent developed in the 1995 EU Directive by ensuring that the user actually received 'relevant, specific and comprehensible information as part of the process of providing his or her consent.'[12] The emphasis on informed consent was intended to overcome issues with the presumed consent model whereby, although information was in principle available on request, it was not in fact easily accessed by the user.

Active consent

The active consent model requires the active engagement of the user, and was intended to overcome problems of user passivity associated with both the presumed consent and informed consent models. As stated by the Article 29 Working Party: '[i]n practice, in the absence of active behaviour of the data subject, it will be problematic for the data controller to verify whether silence was intended to mean acceptance or consent.'[13] The Article 29 Working Party suggested dialogue boxes, layered notices and granular privacy settings as means by which active consent may be obtained.[14]

---

[9] Data "controller means the natural or legal person, public authority, agency or other body which, alone or jointly with other determines the purposes and means of the processing of personal data _GDPR Art 4(7)

[10] Eoin Carolan, 'The continuing problems with online consent under the EU's emerging data protection principles' (2016) Computer Law and Security Review, p. 4.

[11] Purposes paragraph 5, 2002 Directive.

[12] Supra n 10, p. 4.

[13] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the definition of consent', 01197/11/EN, WP 187, 13 July 2011, p. 12.

[14] Ibid p. 20.

Specific models of consent

Model	Description
Obligatory opt-in	In this model the use of a certain service is treated as consent. Rather than providing an option to consent, or opt-in, no real choice is given, such as "Yes, I'd like to opt in" or as an alternative "Yes, but only email me once a month", is given. This is often criticised as not providing an adequate set of choices.
Default opt-in	In this model consent is implied, leading to an opt-in to share data by default. Critics point out that this model is often associated with confusing opt-out procedures and misleading options.
Pay to opt-out	This model allows paying account holders to opt out but not those who use the service for free.
Delegation of opt-out	In this model a site shares data automatically with third parties and requires users to visit sites of the third parties to "opt-out", typically requiring an opt-in on the third party site to do so.[15]
Restricted opt-out	This model allows a user to opt-out of being targeted by certain algorithms and alters the service a user receives but does not allow an opt-out of having user data used, analysed, or shared by other means of processing[16]
Misleading opt-in or opt-out	As with the "restricted opt-out model", this model uses misleading wording and usually allows for opt-out of only one source of data, but other sources still can be used.; This is an abusive variant of opt- in or opt-out. It is one that relies on consumer not giving complete attention to the options in order to give misleading options. Individuals are informed in such a way that they are likely to accept what they would otherwise not accept. This sees success as a result of consensual exhaustion.

Parameters of valid consent

Data protection rules in many jurisdictions provide that, in order to be validly expressed, consent needs to be informed, free and unambiguous. Some challenges to achieving this

[15] An example of this would be Travel Agent X requesting users to log in via an external social media platform in order to access Travel Agent X website and its services.

[16] For example, a user can choose to opt-out of targeted advertising on a social media site, but cannot opt out of declining all data processing, storage and analysis. Similarly, one can turn off background location service on your phone, but while using the particular app it may be necessary to collect the information. Questions of necessity and legitimate business interest must be considered here.

quality of consent are highlighted below. While this paper addresses the categories separately, they are interlinked and provide merely an introduction to the topics.

Informed consent

Informed consent can be described as including the following elements: 1) clarity and accessibility; 2) foreseeability; and 3) specificity.

Clarity and accessibility

For consent to qualify as informed, information about the nature of the data gathered, the period of retention and the use to which it will be put has to be reasonably clear and accessible. The onus to ensure that this information is conveyed in non-technical language should be on the data controller who must ensure that it is accessible and non-discriminatory

Foreseeability

Informed consent requires the individual to have sufficient information to enable them to foresee the consequences and implications of their data being collected, retained and processed. Foreseeability does not need to be absolute but must be enough to enable the data subject to anticipate the implications of their consent to a degree that is reasonable under the circumstances.

An examination of the adequacy and necessity of imposing time limits on consent, as well as potential mechanisms and safeguards, could be a means to obtaining clearer guidance on the requirement of foreseeability

Specificity

Following on from the concern linked to predictability of the implications of data collection, retention and processing, data protection laws in many jurisdictions provide for purpose limitation or purpose binding. This means that personal data obtained for a specific legitimate purpose must not be processed for a different purpose. Consent is therefore based on the particular purpose and context of information processing, necessitating that data controllers keep track not only of who consented but also for what purpose. The implementation of this requirement may pose special challenges in the big data supply chain and may require the reconceptualization of due diligence obligations of supply chain links.

A further aspect that raises issues of both foreseeability and specificity is the collection and retention of information for subsequent use, unknown at time of collection. As noted above, a ‘vacuum-cleaner’ approach to data collection is the cornerstone of data-driven business models. However, it is difficult to conceive how informed consent can be given by the data subject when at the time of consenting he or she lacks the information to assess the implications of doing so.

Free consent

Two main ways in which the data subject’s freedom and consent are connected are through 1) the control that an individual is able to obtain over what is known about him or her, and 2/ the way in which such decisions impact their access to important resources, including the data subject’s ability to negotiate specific conditions attached to accessing these resources.

Control

As a person cannot meaningfully opt out of being part of the information society, the role of consent and control focus on a more narrow concern with a person's leeway in choosing how – rather than whether – they participate in sharing information.

Big data and associated technologies impact the level of control a person can exert over the generation and use of their data. This, however, raises the question of whether and to what extent consent can still play a meaningful role in the circumstances where the individual's control over the different phases of the use of their personal information is reduced.

Negotiating position

Individuals frequently consent to the collection, retention and processing of their data in the context of service contracts with businesses. In the overwhelming majority of such cases, individuals are in no position to negotiate contractual terms and conditions governing the collection, retention and processing of their data, given the unequal relationship between individual and business. As decisions to not use certain services may bear - at times significant - collateral costs, this puts into question whether consent to such terms and conditions can be considered valid and raises the need for additional safeguards to govern such relationships.

Unambiguous consent

Another issue that arises is with unambiguous consent in which questions arise about when it may be implied and when the need to avoid ambiguity requires consent to be explicit. The responses to these questions depend on: 1) the context in which the data is collected; and 2) the nature of information collected.

Context of collection

It may be argued that in cases when data collection constitutes a reasonable and foreseeable part of an activity or service, by engaging in the activity or using the service, a person implicitly agrees to the associated collection and/or processing of data. This would mean that by walking into a store equipped with security cameras a person will be deemed to have agreed to footage of them being registered. Similarly, a person ordering home delivery of a product agrees to the store collecting their address for the purposes of executing the delivery. For data collection, retention, or processing that goes beyond what is necessarily associated with the activity or service, consent should arguably be explicit, covering the specific type of use. For example, if the customer's address will be kept on file after the provision of the specific service or shared with third parties, the explicit consent of the data subject would be required. The same goes to datasets resulting from store video footage being corroborated with data collected through sensing technologies. However, what counts as 'foreseeable' and 'reasonable' part of specific services is not without controversy.

Nature of data collected

The conditions for validity of consent also depend on the nature of data that is being collected, retained or processed. In line with the EU General Data Protection Regulation, consent to the collection of personal data defined as 'sensitive' must always be explicit.14 Therefore, implicit consent to the collection and processing of such data would run short of these requirements. As relevant technologies become more sophisticated, 'non-sensitive' data may, through processing, become 'sensitive' data and the corresponding consent required to its gathering and use shifts accordingly into the explicit category.

Sample of issues to be addressed

1. **Overload/consensual exhaustion**- the ubiquity of technology and applications that individuals utilise on a daily basis risks an information overload, and consent transaction overload on data subjects, which compromises the meaningfulness of consent.
2. **Lack of meaningful choice** - even if there are other providers in the market providing similar services, they often have such similar terms that the individual user cannot decline in favour of an alternative that reflects their preferences
3. **Not informed consent**- Solove argues that consent models fail to offer adequate protection for people, as such models have too many hurdles: (1) people do not read privacy policies; (2) if they do read them, they do not understand them; (3) if people read and understand them, they often lack enough background knowledge to make an informed decision; [17].
4. **Problem of scale**: A person may be able to manage his/her privacy with a few entities, but privacy self-management does not scale well. Even if every entity provided people with an easy and clear way to manage their privacy, there are simply too many entities that collect, use, and disclose people's data for the rational person to handle. [18]
5. **Problem of aggregation**: even if people made rational decisions about sharing individual pieces of data in isolation, they greatly struggle to factor in the way in which their data might be aggregated in the future[19]
6. **Privacy self-management**: addresses privacy in a series of isolated transactions guided by particular individuals. Privacy costs and benefits, however, are more appropriately assessed cumulatively and holistically — not merely at the individual level – as individual decisions about privacy affect society and not just the individual making the decision.[20]
7. **Problem of assessing harm / Presenting bias**: The aggregation effect shows that privacy is an issue of long-term information management, while most decisions to consent to the collection, use, or disclosure of data are tied to a short-term benefit.[21] Present bias: the tendency to choose immediate gratification and disregard future costs or disadvantages.
8. **Risk perception**: The individual is expected to make decision as a rational and informed subject, however this overlooks the fact that individuals can be susceptible to flawed decision-making models. Consent models require individuals to make a choice by balancing the risks to their personal data and benefits they can accrue from sharing their information in exchange for a particular service. Depending on how this information is framed, there can be an underestimate or overestimate of the probability of the risks that are presented.[22] A decision that relies on intuition,[23] with instant gratification and seemingly distant risks if consent is given, questions how meaningful consent can really be. Tests for evaluating informed consent assess recall of information, but that the ability to recall is different from the capacity to

[17] Custers, B. (2016). Click here to consent forever: Expiry dates for informed consent. *Big Data & Society*. https://doi.org/10.1177/2053951715624935
[18] Daniel J. Solove, "Introduction: Privacy self-management and the consent dilemma", Harvard Law Review (2013), Symposium, p 1888
[19] Ibid, p 1888
[20] Ibid, 1881
[21] Ibid, p 1891
[22] William W. Reynolds and Robert M. Nelson, "Risk perception and decision processes underlying informed consent to research participation", Social Science & Medicine (2007), Vol. 65, p 2105
[23] Ibid, 2111

comprehend complex information and make rational decisions on a well-balanced risk assessment.[24]

9. **Renewal**: Consent is usually only obtained at the outset, for initial disclosure of information, but rarely renewed, which results in consent being treated as permanent. Even if terms and policies are amended, users are typically notified without a request for renewed consent, with the assumption that continued use constitutes acceptance and consent.[25] User expectations can change and consent can become outdated when it does not match the initial preferences of a user, if his preferences have changed or if the data processing practices have changed.[26]
10. **Tyranny of the minority**: even if particular individuals have chosen not to participate and do not consent to their information being processed, the information of others can result in the derivation of conclusions that similarly affect those that did not consent, independent of their consent. This diminishes the incremental value of an individual's consent as the dataset is increasingly representative.[27]
11. **Status quo bias**: the tendency to stick with default options (and in relation to consent desensitisation)
12. **Reasonable expectation of privacy:** what are expectations of privacy in a public space?
13. **Inalienability of rights: recalling the earlier point about the relevance of human rights in shaping consent,** even if consent is informed, are there cases in which you cannot consent to giving up a right because the inalienability of the right in question?
14. **Overriding consent:** when can consent be lawfully overridden? What are the limitations?

Overarching questions to consider:

1. How can we close the practical gap between the intended purpose of consent and its current practice?
2. Should different types of consent be considered for different types of data requests?
3. Are there alternatives to individual consent that may prove more effective in providing protection for personal data?

[24] Ibid, 2106
[25] Custers, B. (2016). *Click here to consent forever: Expiry dates for informed consent*, p 1-3
[26] Custers, B. (2016). *Click here to consent forever: Expiry dates for informed consent*, p 2
[27] Barocas, S., & Nissenbaum, H. (2014). Big Data's End Run around Anonymity and Consent. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (pp. 44-75). Cambridge: Cambridge University Press, p 62

The Human Rights, Big Data and Technology Project

Human Rights Centre,
University of Essex,
Colchester CO4 3SQ
+44 (0)1206 872877

@HRBDTNews
www.hrbdt.ac.uk