# eLaw
# Working Paper Series

No 2018/008 - ELAW– 24 April 2019

## Consent and Privacy

Bart Custers, Francien Dechesne, Wolter Pieters, Bart Schermer, and Simone van der Hof

Universiteit Leiden
eLaw

# 22
# CONSENT AND PRIVACY

*Bart Custers, Francien Dechesne, Wolter Pieters,*
*Bart Schermer, and Simone van der Hof*

## 22.1 Introduction

Consent to personal data-processing practices has become quite a mundane activity in the digital world. When downloading apps to our smartphones, we – almost automatically – consent to the privacy policies associated with the particular services they provide. Also, when subscribing to social networking services, consenting to their privacy policies is inescapable. Another particularly visible practice is to ask internet users to accept cookies (i.e., small pieces of data stored on people's computers to "remember" their actions and preferences).

The (consent to) disclosure of personal data and the subsequent use of such data is the domain of privacy and data protection. This chapter explores the discussion on the role of consent in privacy and personal data protection. It is shown how legal, ethical, economic and technological studies point to similar core issues related to the limitations of communication and decision making, inhibiting the effectiveness of consent for privacy protection. In section 22.2 the relation between privacy and consent is examined. In section 22.3 ethical and legal requirements for (informed) consent in relation to privacy and personal data protection are discussed. Special attention is given to the issues concerning children's consent. Next, the limits of consent in privacy and personal data protection are discussed from a technological perspective (section 22.4) and from the perspectives of legal, social and (behavioral) economics (section 22.5). In section 22.6 potential solutions to the issues regarding privacy and consent are offered and analyzed. In section 22.7 conclusions are provided.

## 22.2 Privacy, data protection and consent

In relation to privacy and personal data, informed consent is often described in terms of informational self-determination (Westin 1967), stating that each person should have a right to determine for himself when, how and to what extent information about him or her is communicated to others. Consent requests fulfil a practical purpose, as they allow individuals to express their preferences. In a sense, a consent transaction also functions as a warning that there may be consequences of a particular choice, consequences that may be beneficial for the individual, but also consequences that may be non-beneficial or potentially harmful.

In the context of information technology, sharing and disclosing personal data by organizations typically requires consent of the person whose personal data are involved. However, when

not all conditions for informed consent are met, the consent may be ethically and/or legally flawed (see section 22.3), and even when all such conditions are met, the consent may not always be effective (see sections 22.4 and 22.5). For instance, informed consent to the use of personal data can only be given if the context of such data use is clear – a concept referred to as *contextual integrity* (Nissenbaum 2010). In other words, the consent is only valid against a fixed and clear (knowable) setting of roles, activities, norms and values for the use of the data.

Before addressing these ethical issues of (the limits of) consent in privacy and personal data protection, a short note on the concepts of privacy and personal data protection may be useful. Privacy has many connotations and perceptions of privacy can be different depending on individual preferences and historical, cultural or social contexts. One such conception of privacy is control over personal data or informational self-determination. On such a conception, personal data protection can be subsumed under the broader notion of privacy. However, privacy and data protection are sometimes also perceived as different legal tools to regulate our private (information) spheres. Privacy as an opacity tool (i.e., protection of the private life) has a prohibitive nature and aims at the protection of individual liberty and autonomy against state interference. Contrastingly, personal data protection schemes (i.e., fair processing of personal data) are of a regulatory rather than a prohibitive nature and focus on "channeling, regulating and controlling legitimate powers" (Gutwirth & De Hert 2008).

Privacy is often contrasted with security and law enforcement. This is particularly the case when interests of national security (such as counterterrorism) lead to requests for access to personal data, such as private communications. In such situations consent to collect and process personal data may not be required, if specific laws (e.g., criminal law, anti-terrorism legislation) overrule privacy and data protection legislation. It is argued that, in order to protect security in society, it is sometimes justified to override consent. The privacy versus security distinction only applies to actors from the public sector. The government has a duty to protect citizens (security) and may, in this context, sometimes violate individual rights (such as privacy) and override consent. Private actors typically are not authorized to violate such rights and may depend on consent as a basis for processing personal data.

## 22.3 Requirements for consent

### *22.3.1 Criteria for valid consent*

In the context of privacy and data protection, it is usually assumed that consent is only valid when it is informed consent. An essential aspect of informed consent is that the person who is asked for consent should be properly informed of what exactly he or she is consenting to and is to some extent (made) aware of the consequences such consent may have. In the context of information technology, consent decisions concern the sharing and disclosure of personal data. From an ethical and legal perspective, several crucial criteria can be identified in the context of automated information processing.

Criteria for informed *consent* may include criteria regarding the person who consents (is the person an adult, capable and competent to consent?) and criteria on how to give consent (for instance, is the consent written or oral, is the consent partial or full, is the conviction behind the consent reasonably strong and is the consent an independent decision?) (Custers et al. 2013).

Criteria for *informed* consent can include criteria regarding the extent to which persons are enabled to consider the consent decision well, such as what information should be provided and how this information should be provided (Custers et al. 2013). It is generally held that the information that should be provided includes at least contextual information about which data

*Table 22.1* Overview of the criteria for consent

| | | |
|---|---|---|
| Criteria regarding the *decision to consent* | Criteria regarding the *person who consents* | Is the person who consents an adult? If not, is there parental consent? |
| | | Is the person who consents capable of consenting? If not, is there a legal representative to consent? |
| | | Is the person who consents competent to consent? If not, is there a legal representative to consent? |
| | Criteria on *how to give consent* | Is the consent written? |
| | | Is the consent partial or full? In case of partial consent, does the consent cover the purpose? |
| | | Is the conviction behind the consent decision reasonably strong? |
| | | Is the consent an independent decision? |
| | | Is the consent up to date? |
| Criteria enabling the *well-consideredness of the decision to consent* | Criteria regarding *what information should be provided* | Is it clear which data are collected? |
| | | Are the purposes clear? |
| | | Is it clear which security measures are taken? |
| | | Is it clear who is processing the data and who is accountable? |
| | | Is it clear which rights can be exercised? Is it clear how these rights can be exercised? |
| | Criteria regarding *how information should be provided* | Is the information provided specific and sufficiently detailed? |
| | | Is the information provided understandable? |
| | | Is the information provided reliable and accurate? |
| | | Is the information provided accessible? |

are collected, used and shared and for which purposes the data are used. Furthermore, information on which security measures are taken, information about who is processing the data and who is accountable as well as information on user rights and how they can be exercised are potentially relevant for the consent decision. Moreover, it is generally held that the information provided should be specific, sufficiently detailed, understandable, reliable, accurate and accessible. Apart from situations in which it is obvious that some of these criteria are not met (such as absent policies, or policies in a completely different language), it is not clear for many of these criteria when they are sufficiently met. An overview of these criteria for valid informed consent is shown in Table 22.1. This overview includes the legal criteria for the validity of individual consent, which will be discussed in more detail in the next subsection.

### *22.3.2 Consent in data protection legislation*

Through official guidelines and legislation, many of the criteria mentioned in Table 22.1 are included in the legal frameworks for personal data protection in many countries, including the US and the EU. Therefore, these criteria are not only ethical criteria but also legal criteria that a consent decision must meet in order not to be flawed. In the US, the criteria can be found in the Fair Information Practice Principles (FIPPs) of the Federal Trade Commission. Although these principles are only recommendations, they form the basis of specific legislation, including the Fair Credit Reporting Act, the Right to Financial Privacy Act, the Electronic Communications Privacy Act and the Video Privacy Protection Act.

In the EU, the legal framework for informational privacy and personal data protection is established by the Data Protection Directive,[1] which will be replaced by the General Data Protection Regulation (GDPR) as of 25 May 2018.[2] Both these laws contain most of the criteria mentioned in Table 22.1.

In European data protection legislation, consent plays a vital role, because it is one of the most important reasons legitimizing personal data processing. The Data Protection Directive and its successor, the GDPR, stipulate that personal data may be processed based on the unambiguous consent of the person to whom the data relate.[3] Consent under EU data protection legislation must be freely given, specific and informed in order to be valid. Furthermore, EU data protection legislation sets requirements for the form in which consent is given: consent must be unambiguous and, in certain cases, explicit.

For consent to qualify as "unambiguous" there must be no uncertainty about the intent of the person to whom the data relate. This intent can be expressed in the form of an action carried out by the person who must give the consent (e.g., ticking a checkbox), but also through a more general action carried out by the individual (e.g., walking through a door with a sign above it saying "if you enter you consent to having your picture taken"). Inferring consent from *in*action can never count as an unambiguous consent. However, inferring consent from an action that is not specifically or solely aimed at consent is possible, given that it is unambiguous. The burden of proof for the unambiguity of the consent rests upon the organization responsible. In the GDPR, the requirements for consent are strengthened by requiring that consent is expressed "either by a statement or a clear affirmative action". This will likely leave less room for the inference of consent.

For special categories of data that are more sensitive (e.g., health data), the higher standard of *explicit* consent needs to be met in order to legitimize data processing. For explicit consent, individuals need to be asked to agree or disagree with a particular use or disclosure of their personal information and they need to respond actively to the question.[4]

### *22.3.3 Children's consent*

Both the US Children's Online Privacy Protection Act (hereafter: COPPA) and the GDPR hold special provisions on children's consent that take into account the level of maturity of children in determining whether they are capable of consenting to the processing of their personal information. Their level of maturity is mostly derived from their cognitive abilities to sufficiently understand their (legal) position and, hence, to give consent to certain actions. In the landmark case of Gillick, the UK House of Lords formulated the capacity to consent as: *a sufficient understanding and intelligence to be capable of making up his own mind on the matter requiring decision* as well as the capability *of understanding what is proposed, and of expressing his or her own wishes*.

When it comes to the provision of online commercial services, such as social media, video websites and games, both COPPA[5] and the GDPR[6] aim to provide children with special protection from (re)use of their personal data for marketing and other commercial purposes. Basically, children's capability to consent can be challenged in three ways. First, children might not be capable of understanding the *nature* of personal data processing. What personal data are used? How are they being used and by whom? Second, children might not be capable of understanding the *consequences* of personal data practices. Third, children might not be capable of understanding their *legal position* and of effectively using their privacy and data protection rights.

In privacy and data protection law in the US and the EU, the required level of maturity is reflected in the ages set for children's consent. From a certain age, children are considered to be

capable of consenting on their own to the use of their personal information. However, this age can vary depending on the particular legal system. Under COPPA, the age is set at 13 years, whereas the GDPR provides that children are capable of consenting at the age of 16. However, the GDPR also leaves room for EU member states to set lower ages as long as they are not below 13. Below the age of consent, children require the consent of their parents to use online commercial services, even if such services are for free. Both COPPA and the GDPR require that parental consent is *verifiable*.

Verifiable parental consent entails that "reasonable efforts" must be taken by the responsible organization to make sure that it actually is the parent who is consenting. What verifiability of consent means more precisely and how it can be ensured is a matter for further scrutiny and not easily determined (Van der Hof 2014).

The provisions on children's consent are problematic in a number of ways (Van der Hof 2016). Remarkably enough, parental consent requirements might lead to tensions between parents and children in terms of privacy. Social media are, for instance, not only a venue for teens to socialize with their peers but also provide private spaces unbeknownst to parents (boyd 2008, 2014). Additionally, these requirements potentially encourage intrusive parental surveillance (Van der Hof 2014). Moreover, given the limits to consent discussed in the next sections, it might be questioned whether the provision indeed protects the use of children's personal data as envisioned by COPPA and the GDPR.

## 22.4 Limits of consent: the technological view

When one or more criteria for consent mentioned in Table 22.1 are not met, the individual consent is likely to be invalid, for example, in the case where a person is not properly informed.[7] However, even if the individual consent is valid, a consent mechanism may still be inadequate in the context in which it is used. Since informed consent is a mechanism that is used to ensure that people make well-considered decisions, the consent mechanism may also be *ineffective* and not very meaningful when people do not take notice of the information offered (e.g., because it is too much information or hard to understand). This section discusses limits of effective consent mechanisms from a technological perspective and the next section discusses the limits of consent from legal, social and (behavioral) economics perspectives.

From a technological perspective, a first issue is that information on the use of personal data may be difficult to provide. As data-processing tools in the context of Big Data, including data mining and profiling tools, continue to evolve, it can be extremely difficult to predict future data-processing technologies and the future potential of personal data. Developments in information and communication technology allow data, including personal data, to be aggregated, archived and analyzed ("mined") across domains on an increasingly vast scale and for longer periods of time. For example, if a person consents to the sharing of electricity consumption data with a network provider for network management and billing purposes, such consent does not cover selling the data to marketing firms.

Big Data developments (exponentially more data, more real-time data and more diverse datasets) provide opportunities for data coupling across domains such that unexpected relations and patterns may be discovered in the data. The increasing reuse of data in new ways and contexts may not be transparent or understandable for everyone and potentially undermines the possibility to make well-considered consent decisions. On top of that, Big Data allows so-called Privacy Merchants to combine apparently innocuous facts not privileged by law into highly sensitive personally identifiable information. Etzioni (2012) suggests calling such processes "privacy violating triangulation". In this respect, the combination of data across domains and across time

means the use of the data is re-contextualized ("context creep"), in some cases beyond the scope of the original consent. Changing or even discarding the context under which the data were consensually collected, and the impossibility to be truly informed about the consequences of granting data use, means the informed consent loses its validity.

A second issue is that withholding consent (i.e., refusing to disclose personal data) does not necessarily guarantee better privacy protection. The use of Big Data increasingly enables the prediction of characteristics of people who withheld consent on the basis of the information available from people who did consent. When large numbers of people consent to the use of their personal data, it is possible to predict missing values of other people (Custers 2012). This may be pretty accurate: Kosinski et al. (2013) show how a range of highly sensitive personal characteristics, including sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances and parental separation can be predicted very accurately on the basis of what a person has "liked" on Facebook. Such predictions limit the effectiveness of withholding consent. Obviously, predicting missing values is also possible for people who provided partial consent or for people who (whether on purpose or not) provided false information. Nevertheless, when data are inaccurate or incomplete, for instance because they are outdated, such predictions may become less accurate, resulting in wrong conclusions about people.

A third issue is that consent has a temporal aspect that may become increasingly important given the rapid technological developments. For instance, consent is usually asked for when registering for social media or websites, but rarely renewed afterwards. As a result, consenting once often implies consent "forever" (i.e., until it is actively withdrawn), even though the consent may rapidly get outdated (i.e., no longer match the initial preferences of a user), for instance, because the user has changed her mind, the technology and design of the service or website have changed, the terms and conditions or policies have changed or because the data-processing practices have changed significantly. Custers (2016) has suggested starting a debate on expiry dates for consent.

Given this temporal aspect, a fourth issue concerns the difficulties of withdrawing consent. Here it is important to focus on the debate on the right to be forgotten. This right enables people to have personal data about themselves deleted after it has become public. Amongst others, the right is relevant in situations in which an individual withdraws consent (or objects to the processing of his or her personal data). The right is of particular importance as it allows individuals to start again with a clean (online) slate. Reasons for consent withdrawal can be manifold, including changes in privacy policies, augmented concerns about the use of personal data, contextual changes (e.g., implementation of privacy-intrusive technologies or practices). The discontinuation of a particular service or transaction (e.g., by closing and deleting a social media account or exercising the right of withdrawal from an online consumer contract) could entail consent withdrawal. After consent withdrawal, the personal data initially collected may no longer be pertinent to the contractual relationship, once completely finished, and, hence, new obligations arise, one of which might be to erase such personal data. In that respect, the right to be forgotten is often more adequately referred to as "the right to erasure". For instance, the GDPR indeed requires subsequent erasure of data upon consent withdrawal, unless other lawful grounds for processing personal data of the individual remain. However, in practice this obligation might not always be easy to comply with or may potentially even be ineffective, given that the internet architecture largely undermines the ability to control data flows as a result of its open, end-to-end character. Unless personal data have been contained within a system strictly controlled by the service provider, it might be hard or even impossible to meet this requirement.

## 22.5 Limits of consent: the legal, social and (behavioral) economics view

Besides the technological perspective, the effectiveness of informed consent mechanisms as a means to establish informational self-determination in the context of personal data processing can also be challenged from a legal, social and economic point of view (Pollach 2007; Acquisti 2009; Böhme & Köpsell 2010; Adjerid et al. 2013; Solove 2013).

The first issue is that models for informed consent based on informational self-determination fail to offer adequate protection to people, as such models have too many hurdles (Solove 2013). *First*, people do not read privacy policies. Each time consent is asked for, the information provided is often very extensive. It may take a lot of time to read privacy policies and to make a decision based on this information. McDonald & Cranor (2010) have estimated that if people actually read all the privacy policies presented to them, it would take them 244 hours annually. This may explain findings of empirical studies indicating that people simply consent whenever confronted with a consent request (Custers et al. 2013). Such consent mechanisms are likely to be ineffective and their value may be disputed. *Second*, if people do read privacy policies, they may not understand them, as the information provided may be too difficult. In many situations, the text is highly legalistic in nature or contains technical details beyond the comprehension of the average user. *Third*, if people read and understand the policies, they often lack sufficient background knowledge to make an informed decision. While an abbreviated, plain-language policy would be quick and easy to read, it is the hidden details that carry significance (Toubiana & Nissenbaum 2011). Related to this issue is the asymmetry in power distribution. Those who collect and process the data have technological expertise that the average user usually lacks (Acquisti & Grossklags 2005; LaRose & Rifon 2007). *Fourth*, if people read privacy policies, understand them and can make an informed decision, they are not always offered the choice that reflects their preferences.

A second issue is related to this: people seem to become increasingly disengaged in the consent processes, such that the consent decision fails to have the intended moral effect of giving agency to individuals as autonomous decision makers (Hurd 1996; Kleinig 2010). Using the internet, there are (too) many requests for consent (Schermer et al. 2014). Most of the time, users blindly accept consent boxes when they resemble other dialog boxes (Böhme & Köpsell 2010). Browsing and surfing would take a lot of time if internet users were to actually consider every consent request. Moreover, it feels as if they have no choice when encountering consent decisions, since these are framed as take-it-or-leave-it offers: refusing consent means that access to a website or internet service is plainly denied or severely hampered. People are concerned about their privacy, but at the same time they routinely disclose personal information out of convenience or a lack of understanding of the consequences, or for discounts and other incentives (Dutton & Blank 2013; Regan 2002). People may consider this a trade-off in which they "pay" with their personal data, but it may also be the case that they feel they do not have a real choice. There is an important difference between accepting terms and conditions and agreeing with their contents: the former may yield legally valid consent, but the latter regards the actual effectiveness and meaningfulness of the consent mechanism.

A third issue is information asymmetry. A decision to consent to data processing may depend on the level of protection of personal data. However, how to communicate this information adequately is unclear, which makes it difficult for online service providers to compete on the quality of privacy protection,[8] or, more generally, information security (Anderson 2001). From an economic point of view, this creates a "market of lemons", in which high-quality goods are outcompeted by low-quality goods, as the difference cannot be perceived by buyers. A high

level of privacy protection cannot be distinguished from low(er) levels of protection, making it difficult for users to decide whether to give consent to a particular scheme based on their security preferences, the consequence being that they may simply consent to anything.

A fourth issue with consent is framing. For instance, social network services usually collect user data for a variety of purposes and provide users with extensive access to each other's profiles. The privacy settings can allow users to distinguish between different (groups of) contacts that have access to (particular parts of) their personal profile. This is referred to as audience segregation (Van den Berg & Leenes 2010; Van den Berg & Van der Hof 2012). In such a situation, privacy is framed as an issue of inter-user access. However, framing privacy as inter-user access potentially takes attention away from data-processing practices by service providers. Hence, the questions asked in a consent request may be used to frame or mediate the interpretation of the problem and may become part of a strategic game (Adjerid et al. 2013; Johnson et al. 2002; Pieters 2010).

A fifth issue is that there are limits to the idea that privacy and consent are always about data that persons themselves control (or ought to be able to control). Developments in social media and Big Data already make that assumption problematic, as many data are being generated without the individual being aware (for instance, cell phones generating location data or smart watches collecting biometrics) and control cannot be expected given the volume of the data (for instance, when datasets are too large for human intuition to overview). What is more, data collected and used may be(come) anonymous or aggregated data, and both are not necessarily *personal* data. In that case, consent may not be required or may be difficult to obtain as it is not clear whom to address; yet such anonymous or aggregated data can be used to generate (sensitive) profiles that can have an impact on individual people nonetheless. An example is the (alleged) relation between crime and ethnicity. In establishing or verifying such a relation, using anonymous or aggregated data can circumvent consent decisions. However, such correlations can have a serious impact on individuals and society, as it may result in stigmatization, discrimination and social polarization.

Under the GDPR, individuals will have a right to object to profiling for direct marketing purposes. It remains to be seen to what extent such a right can be effectively implemented in practical processes and how it pertains to the concept of consent. Moreover, there may be data that a person does not want to control or does not want to know of (e.g., life expectancies). In such cases, consent may be required for providing particular information to a subject, for example, in the case where genetic data point to a high likelihood of contracting a serious disease (Tavani 2004; Van den Hoven et al. 2014). Subjects may choose *not to know* such data and forcing it upon them without consent could be problematic (Chadwick et al. 1997).

## 22.6 Potential ways forward

A possible solution for addressing some of the limits of consent lies in simplifying the consent process. This can be done in several ways. First, the representation of the information in the consent process can be simplified. Rather than presenting a long text to the user, the information can be condensed in privacy icons, colors, etc. (e.g., Holtz et al. 2011). The obvious question is whether such simplified representations contain enough information to be able to speak of informed consent. The subtleties of different privacy policies, risk profiles, etc. could be lost in the process of simplification. In this approach, the user would still have to consent separately for each service, but the individual indications of consent may take less time, assuming that the meaning of the simplified representations is clear to the user or becomes clear after getting used to the system.

A different approach entails reducing the number of acts of consent. If users can specify once which policies and risks they find acceptable or unacceptable, it may be possible to reuse this

information when being asked for consent for different services. Typically, the choices would be formally represented in a privacy profile for the user. Similarly, each service would provide a formalized privacy policy. By matching the user policy against the service policy, acceptability of the conditions to the user could be derived (e.g., Broenink et al. 2010). If there is a match, consent could be given automatically or a positive advice could be given to the user. If the policies do not match, the system could indicate where the policies differ. In this case, the reduction of complexity lies not in the simplification of the policy representation, but in the reduction of the number of acts of consent. The user may still need to confirm, but the policy matching is done automatically.

Another solution that may improve the current situation is to move from take-it-or-leave-it consent to empowering users to choose a balance between functionality and privacy. For example, rather than giving a travel advice app access to all requested data including location (app permissions), a user may choose to keep the location private at the cost of not being able to use the current location in the app. This requires a different interface and consent mechanism for app permissions (and probably more effort on the part of the developers, in order to be able to work under different access conditions).

Anonymization of data has long been regarded as an important solution to protect privacy, and as such is often included in consent forms. However, research demonstrates that the digital traces that people leave behind, for example, by using credit cards or streaming video, can nowadays be effectively used for de-anonymizing (meta)data (e.g., Narayanan & Shmatikov 2008).

Another important concept in the solutions discourse is privacy-by-design (see e.g., Cavoukian 2010; Langheinrich 2001; Schaar 2010). The central idea is that, when designing information systems, architectural choices can be made that are beneficial to privacy protection. In particular, distributed rather than centralized storage of data can be an important choice, because decentralized storage makes it more difficult to process large volumes of data. Less fundamentally tied to the system architecture, default settings also form a crucial factor in the actual distribution of privacy-sensitive data. The idea is that the way in which choices are presented influences the resulting choice behavior. Default settings provide a so-called choice architecture (Thaler & Sunstein 2003) that encourages (nudges) people to stick with the default, and to change the settings only if they consider it worth the effort. Therefore, privacy-friendly defaults can contribute significantly to the protection of personal data. In the privacy context, this often involves opt-in (giving explicit consent, with non-consent being the default) in contrast to opt-out (explicitly withdrawing consent, with consent being the default) (Johnson et al. 2002). Following the consent criteria we outlined, opt-in would then be preferred, as it involves explicit consent, whereas opt-out assumes implicit consent. At the same time, if users cannot get what they want done without opting in too often, they may simply click without reading the information. An example is the EU legislation on web browser cookies, requiring explicit permission for storing (tracking) cookies, used among other things for personalized advertisements (Bond 2012). Apart from design criteria, it is also important to consider procedures in which citizens can report violations of the consent requirement in data processing. This solution concept focuses on monitoring and feedback, which have been put forward as requirements for responsible experimentation with new technologies in society (Pieters et al. 2014). User education is crucial to make such solutions work in practice.

## 22.7 Conclusions

Consent is a fundamental concept in privacy and personal data protection. In this context, consent is often characterized in terms of informational self-determination. From a legal perspective,

there are several criteria to determine the validity of individual consent. However, even when individual consent is valid, the consent mechanisms may be ineffective (or not meaningful) when they do not meet several additional criteria. An assessment of these criteria shows that it may be extremely difficult to meet all these criteria in the context of digital technologies, as there are many hurdles. For instance, people do not read privacy policies, may not understand them, lack background knowledge or are offered choices that do not reflect their preferences. Things get more complicated when children's consent is required. Furthermore, it may be extremely difficult to predict the future potential of personal data, data may be processed and used for data mining and profiling that yields unpredictable results and withholding consent may not prevent undisclosed data being predicted anyway. Finally, on the internet people are confronted with so many consent requests that they increasingly become disengaged in the consent process. When consent mechanisms are not effective or meaningful, their value may be disputed.

Several solutions have been offered to address these issues. The consent process can be simplified, the number of consent requests can be reduced, more privacy settings can be offered and privacy-preserving measures can be built into the architecture of information technology. Anonymization can be a useful tool, but may not always guarantee privacy. Note, however, that all these solutions only address one or several of the issues of consent. Hence, a combination of measures is recommended in order to ensure that consent decisions actually make people pause for a moment and make them think actively about the consequences of consent.

## Notes

1 Directive 95/46/EG of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ EU, L281/31, 23.11.1995.
2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ EU, L119/1, 4.5.2016.
3 Apart from consent, the GDPR also offers other legal grounds for the processing of personal data. For instance, when the 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, for compliance with a legal obligation to which the controller is subject, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
4 Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, 01197/11/EN WP187.
5 See Electronic Privacy Information Center, Children's Online Privacy Protection Act (COPPA), available at: https://epic.org/privacy/kids/ (last accessed: 11 May 2016).
6 See recital 38 of the GDPR.
7 Note that, in this respect, validity of consent depends on the jurisdiction and the specific situation or context.
8 The quality of privacy protection may be improved by, for instance, transparency, clear purpose specifications, not outsourcing data processing, limiting third-country data transfers, not selling data to data brokers, etc.

## References

Acquisti, A. (2009) "Nudging Privacy: The Behavioral Economics of Personal Information," *Security & Privacy Economics* 7(6): 72–5.
Acquisti, A. and J. Grossklags (2005) "Privacy and Rationality in Decision Making," *IEEE Security and Privacy* 3(1): 26–33.

Adjerid, I., A. Acquisti, L. Brandimarte and G. Loewenstein (2013) "Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency," *Proceedings of the Ninth Symposium on Usable Privacy and Security*. Newcastle, 24–6 July. New York: ACM.

Anderson, R. (2001) "Why Information Security Is Hard – an Economic Perspective," *Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC)*. IEEE.

Böhme, R. and S. Köpsell (2010) "Trained to Accept? A Field Experiment on Consent Dialogs," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2403–6.

Bond, R. (2012) "EU E-Privacy Directive and Consent to Cookies," *The Business Lawyer* 68: 215–24.

boyd, d. (2008). *Taken Out of Context: American Teen Sociality in Networked Publics. Managing*. https://doi.org/10.1056/NEJMcps0801308.

boyd, d. (2014). *It's Complicated: The Social Lives of Networked Teens*. New Haven, CT: Yale University Press.

Broenink, G., J.-H. Hoepman, C. van't Hof, P. van Kranenburg, D. Smits and T. Wisman (2010) "The Privacy Coach: Supporting Customer Privacy in the Internet of Things," in *Pervasive 2010 Conference Workshop on What Can the Internet of Things Do for the Citizen*. pp. 72–81. *arXiv preprint arXiv:1001.4459*. Helsinki, May 17.

Cavoukian, A. (2010) "Privacy by Design: The Definitive Workshop. A Foreword by Ann Cavoukian," *Identity in the Information Society* 3(2): 247–51.

Chadwick, R., M. Levitt and D. Shickle (1997) *The Right to Know and the Right Not to Know*. Aldershot: Ashgate Publishing.

Custers, B. (2012) "Predicting Data that People Refuse to Disclose; How Data Mining Predictions Challenge Informational Self-Determination," *Privacy Observatory Magazine*, Issue 3. www.privacyobservatory.org/

Custers, B. (2016) "Click Here to Consent Forever: Expiry Dates for Informed Consent," *Big Data and Society*, January–June 2016: 1–6. doi: 10.1177/2053951715624935.

Custers, B., S. Van der Hof, B. Schermer, S. Appleby-Arnold and N. Brockdorff (2013) "Informed Consent in Social Media Use. The Gap between User Expectations and EU Personal Data Protection Law," *SCRIPTed, Journal of Law, Technology and Society* 10(4): 435–57.

Dutton, W.H. and G. Blank (2013) *Cultures of the Internet: The Internet in Britain*. Oxford Internet Survey 2013. http://oxis.oii.ox.ac.uk/reports.

Etzioni, A. (2012) "The Privacy Merchants: What is to Be Done?" (March 1, 2012). *University of Pennsylvania Journal of Constitutional Law* 14(4): 929–51.

Gutwirth, S. and P. De Hert (2008) "Regulating Profiling in a Democratic Constitutional State," in M. Hildebrandt and S. Gutwirth (ed.), *Profiling the European Citizen*. Heidelberg: Springer, pp. 271–302.

Holtz, L., H. Zwingelberg and M. Hansen (2011) "Privacy Policy Icons," in J. Camenisch, S. Fischer-Hübner and K. Rannenberg (ed.), *Privacy and Identity Management for Life*. Heidelberg: Springer, pp. 279–85.

Hurd, H.M. (1996) "The Moral Magic of Consent (I)," *Legal Theory* 2: 121–46.

Johnson, E.J., S. Bellman and G.L. Lohse (2002) "Defaults, Framing and Privacy: Why Opting in-Opting Out," *Marketing Letters* 13(1): 5–15.

Kleinig, J. (2010) "The Nature of Consent," in F. Miller and A. Wertheimer (ed.), *The Ethics of Consent: Theory and Practice*. New York: Oxford University Press, pp. 3–25.

Kosinski, M., D. Stillwell and T. Graepel (2013) *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*. PNAS. www.pnas.org/cgi/doi/10.1073/pnas.1218772110.

Langheinrich, M. (2001) "Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems," in G.D. Abowd, B. Brumitt and S. Shafer (ed.), *Ubicomp 2001: Ubiquitous Computing*. Heidelberg: Springer, pp. 273–91.

LaRose, R. and N. Rifon (2007) "Promoting i-Safety: Effects of Privacy Seals on Risk Assessment and Online Privacy Behaviour," *Journal of Consumer Affairs* 41(1): 127–49.

McDonald, A.M. and L.F. Cranor (2010) "The Cost of Reading Privacy Policies," *I/S Journal for Law and Policy for the Information Society* 4(3): 543–68. www.aleecia.com/authors-drafts/readingPolicyCost-AV.pdf

Narayanan, A. and V. Shmatikov (2008) "Robust De-anonymization of Large Sparse Datasets (How to Break Anonymity of the Netflix Prize Dataset)," in *Proceedings of 29th IEEE Symposium on Security and Privacy*. Oakland: IEEE Computer Society. May 2008, pp. 111–25.

Nissenbaum, H. (2010) *Privacy in Context – Technology, Policy and the Integrity of Social Life*. Stanford: Stanford University Press.

Pieters, W. (2010) "Reve {a, i} ling the Risks: A Phenomenology of Information Security," *Techné: Research in Philosophy and Technology* 14(3): 194–206.

Pieters, W., D. Hadžiosmanović and F. Dechesne (2014) "Cyber Security as Social Experiment," in *Proceedings of the 2014 workshop on New Security Paradigms Workshop*, ACM, pp. 15–24.
Pollach, I. (2007) "What's Wrong with Online Privacy Policies?" *Communications of the ACM* 50(9): 103–8.
Regan, P.M. (2002) "Privacy and Commercial Use of Personal Data: Policy Developments in the US," Paper Presented at the Rathenau Institute Privacy Conference. January 17, Amsterdam.
Schaar, P. (2010) "Privacy by Design," *Identity in the Information Society* 3(2): 267–74.
Schermer, B.W., B.H.M. Custers and S. Van der Hof (2014) "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection," *Ethics & Information Technology* 16(2): 171–82.
Solove, D.J. (2013) "Privacy Self-Management and the Consent Dilemma," *Harvard Law Review* 126: 1880–903.
Tavani, H.T. (2004) "Genomic Research and Data-Mining Technology: Implications for Personal Privacy and Informed Consent," *Ethics and Information Technology* 6(1): 15–28.
Thaler, R.H. and C.R. Sunstein (2003) "Libertarian Paternalism," *American Economic Review* 93(2): 175–9.
Toubiana, V. and H. Nissenbaum (2011) "An Analysis of Google Logs Retention Policies," *Journal of Privacy and Confidentiality* 3(1): Article 2, 3–26.
Van den Berg, B. and R. Leenes (2010) "Audience Segregation in Social Network Sites," in *Proceedings for SocialCom2010/PASSAT2010 (Second IEEE International Conference on Social Computing/Second IEEE International Conference on Privacy, Security, Risk and Trust)*. Minneapolis (Minnesota, USA): IEEE: 1111–17.
Van den Berg, B. and S. Van der Hof (2012) "What Happens to My Data? A Novel Approach to Informing Users of Data Processing Practices," *First Monday* 17(7). http://firstmonday.org/ojs/index.php/fm/article/view/4010.
Van den Hoven, J., M. Blaauw, W. Pieters and M. Warnier (2014) "Privacy and Information Technology," in E.N. Zalta (ed.), *The Stanford Encyclopedia of Philosophy* (Winter 2014 Edition). http://plato.stanford.edu/archives/win2014/entries/it-privacy/.
Van der Hof, S. (2014) "No Child's Play: Online Data Protection for Children," in S. van der Hof, B. van den Berg and B. Schermer (ed.), *Minding Minors Wandering the Web: Regulating Online Child Safety*. The Hague: TCM Asser Press/Springer Press, pp. 127–41.
Van der Hof, S. (2016) "I Agree . . . or Do I? — A Rights-based Analysis of the Law on Children's Consent in the Digital World," *Wisconsin International Law Journal* 34(2): 409–45.
Westin, A. (1967) *Privacy and Freedom*. London: Bodley Head.

## Related topics

Ch.8 Valid consent
Ch.24 Informed consent