Stanford Encyclopedia of Philosophy

Privacy and Information Technology

First published Thu Nov 20, 2014; substantive revision Wed Oct 30, 2019

Human beings value their privacy and the protection of their personal sphere of life. They value some control over who knows what about them. They certainly do not want their personal information to be accessible to just anyone at any time. But recent advances in information technology threaten privacy and have reduced the amount of control over personal data and open up the possibility of a range of negative consequences as a result of access to personal data. In the second half of the 20th century data protection regimes have been put in place as a response to increasing levels of processing of personal data. The 21st century has become the century of big data and advanced information technology (e.g. forms of deep learning), the rise of big tech companies and the platform economy, which comes with the storage and processing of exabytes of data.

The revelations of Edward Snowden, and more recently the Cambridge Analytica case (Cadwalladr & Graham-Harrison 2018) have demonstrated that worries about negative consequences are real. The technical capabilities to collect, store and search large quantities of data concerning telephone conversations, internet searches and electronic payment are now in place and are routinely used by government agencies and corporate actors alike. The rise of China and the large scale of use and spread of advanced digital technologies for surveillance and control have only added to the concern of many. For business firms, personal data about customers and potential customers are now also a key asset. The scope and purpose of the personal data centred business models of Big Tech (Google, Amazon, Facebook, Microsoft, Apple) has been described in detail by Shoshana Zuboff (2018) under the label "surveillance capitalism".

At the same time, the meaning and value of privacy remains the subject of considerable controversy. The combination of increasing power of new technology and the declining clarity and agreement on privacy give rise to problems concerning law, policy and ethics. Many of these conceptual debates and issues are situated in the context of interpretation and analysis of the General Data Protection Regulation (GDPR) that was adopted by the EU in spring 2018 as the successor of the EU 1995 Directives, with application far beyond the borders of the European Union.

The focus of this article is on exploring the relationship between information technology and privacy. We will both illustrate the specific threats that IT and innovations in IT pose for privacy and indicate how IT *itself* might be able to overcome these privacy concerns by being developed in ways that can be termed "privacy-sensitive", "privacy enhancing" or "privacy respecting". We will also discuss the role of emerging technologies in the debate, and account for the way in which moral debates are themselves affected by IT.

1. Conceptions of privacy and the value of privacy

Discussions about privacy are intertwined with the use of technology. The publication that began the debate about privacy in the Western world was occasioned by the introduction of the newspaper printing press and photography. Samuel D. Warren and Louis Brandeis wrote their article on privacy in the Harvard Law Review (Warren & Brandeis 1890) partly in protest against the intrusive activities of the journalists of those days. They argued that there is a "right to be left alone" based on a principle of "inviolate personality". Since the publication of that article, the debate about privacy has been fuelled by claims regarding the right of individuals to determine the extent to which others have access to them (Westin 1967) and claims regarding the right of society to know about individuals. Information being a cornerstone of access to individuals, the privacy debate has co-evolved with – and in response to – the development of information technology. It is therefore difficult to conceive of the notions of privacy and discussions about data protection as separate from the way computers, the Internet, mobile computing and the many applications of these basic technologies have evolved.

1.1 Constitutional vs. informational privacy

Inspired by subsequent developments in U.S. law, a distinction can be made between (1) *constitutional* (or decisional) *privacy* and (2) *tort* (or informational) *privacy* (DeCew 1997). The first refers to the freedom to make one's own decisions without interference by others in regard to matters seen as intimate and personal, such as the decision to use contraceptives or to have an abortion. The second is concerned with the interest of individuals in exercising control over access to information about themselves and is most often referred to as "informational privacy". Think here, for instance, about information disclosed on Facebook or other social media. All too easily, such information might be beyond the control of the individual.

Statements about privacy can be either descriptive or normative, depending on whether they are used to describe the way people define situations and conditions of privacy and the way they value them, or are used to indicate that there ought to be constraints on the use of information or information processing. These conditions or constraints typically involve personal information regarding individuals, or ways of information processing that may affect individuals. Informational privacy in a normative sense refers typically to a non-absolute moral right of persons to have direct or indirect control over access to (1) information about oneself, (2) situations in which others could acquire information about oneself, and (3) technology that can be used to generate, process or disseminate information about oneself.

1.2 Accounts of the value of privacy

The debates about privacy are almost always revolving around new technology, ranging from genetics and the extensive study of bio-markers, brain imaging, drones, wearable sensors and sensor networks, social media, smart phones, closed circuit television, to government cybersecurity programs, direct marketing, RFID tags, Big Data, head-mounted displays and search engines. There are basically two reactions to the flood of new technology and its impact on personal information and privacy: the first reaction, held by many people in IT industry and in R&D, is that we have zero privacy in the digital age and that there is no way we can protect it, so we should get used to the new world and get over it (Sprenger 1999). The other reaction is that our privacy is more important than ever and that we can and we must attempt to protect it.

In the literature on privacy, there are many competing accounts of the nature and value of privacy (Negley 1966, Rössler 2005). On one end of the spectrum, *reductionist* accounts argue that privacy claims are really about other values and other things that matter from a moral point of view. According to these views the value of privacy is reducible to these other values or sources of value (Thomson 1975). Proposals that have been defended along these lines mention property rights, security, autonomy, intimacy or friendship, democracy, liberty, dignity, or utility and economic value. Reductionist accounts hold that the importance of privacy should be explained and its meaning clarified in terms of those other values and sources of value (Westin 1967). The opposing view holds that privacy is valuable in itself and its value and importance are not derived from other considerations (see for a discussion Rössler 2004). Views that construe privacy and the personal sphere of life as a human right would be an example of this non-reductionist conception.

More recently a type of privacy account has been proposed in relation to new information technology, which acknowledges that there is a cluster of related moral claims underlying appeals to privacy, but maintains that there is no single essential core of privacy concerns. This approach is referred to as cluster accounts (DeCew 1997; Solove 2006; van den Hoven 1999; Allen 2011; Nissenbaum 2004).

From a descriptive perspective, a recent further addition to the body of privacy accounts are epistemic accounts, where the notion of privacy is analyzed primarily in terms of knowledge or other epistemic states. Having privacy means that others don't know certain private propositions; lacking privacy means that others do know certain private propositions (Blaauw 2013). An important aspect of this conception of having privacy is that it is seen as a relation (Rubel 2011; Matheson 2007; Blaauw 2013) with three argument places: a subject (S), a set of propositions (P) and a set of individuals (I). Here S is the subject who has (a certain degree of) privacy. P is composed of those propositions the subject wants to keep private (call the propositions in this set 'personal propositions'), and I is composed of those individuals with respect to whom S wants to keep the personal propositions private.

Another distinction that is useful to make is the one between a European and a US American approach. A bibliometric study suggests that the two approaches are separate in the literature. The first conceptualizes issues of informational privacy in terms of 'data protection', the second in terms of 'privacy' (Heersmink et al. 2011). In discussing the relationship of privacy matters with technology, the notion of data protection is most helpful, since it leads to a relatively clear picture of what the object of protection is and by which technical means the data can be protected. At the same time it invites answers to the question why the

data ought to be protected, pointing to a number of distinctive moral grounds on the basis of which technical, legal and institutional protection of personal data can be justified. Informational privacy is thus recast in terms of the protection of personal data (van den Hoven 2008). This account shows how Privacy, Technology and Data Protection are related, without conflating Privacy and Data Protection.

1.3 Personal Data

Personal information or data is information or data that is linked or can be linked to individual persons. Examples include explicitly stated characteristics such as a person's date of birth, sexual preference, whereabouts, religion, but also the IP address of your computer or metadata pertaining to these kinds of information. In addition, personal data can also be more implicit in the form of behavioural data, for example from social media, that can be linked to individuals. Personal data can be contrasted with data that is considered sensitive, valuable or important for other reasons, such as secret recipes, financial data, or military intelligence. Data used to secure other information, such as passwords, are not considered here. Although such security measures (passwords) may contribute to privacy, their protection is only instrumental to the protection of other (more private) information, and the quality of such security measures is therefore out of the scope of our considerations here.

A relevant distinction that has been made in philosophical semantics is that between the referential and the attributive use of descriptive labels of persons (van den Hoven 2008). Personal data is defined in the law as data that can be linked with a natural person. There are two ways in which this link can be made; a referential mode and a non-referential mode. The law is primarily concerned with the 'referential use' of descriptions or attributes, the type of use that is made on the basis of a (possible) acquaintance relationship of the speaker with the object of his knowledge. "The murderer of Kennedy must be insane", uttered while pointing to him in court is an example of a referentially used description. This can be contrasted with descriptions that are used attributively as in "the murderer of Kennedy must be insane, whoever he is". In this case, the user of the description is not – and may never be – acquainted with the person he is talking about or intends to refer to. If the legal definition of personal data is interpreted referentially, much of the data that could at some point in time be brought to bear on persons would be unprotected; that is, the processing of this data would not be constrained on moral grounds related to privacy or personal sphere of life, since it does not "refer" to persons in a straightforward way and therefore does not constitute "personal data" in a strict sense.

1.4 Moral reasons for protecting personal data

The following types of moral reasons for the protection of personal data and for providing direct or indirect control over access to those data by others can be distinguished (van den Hoven 2008):

1. Prevention of harm: Unrestricted access by others to one's bank account, profile, social media account, cloud repositories, characteristics, and whereabouts can be used to harm the data subject in a variety of ways.
2. Informational inequality: Personal data have become commodities. Individuals are usually not in a good position to negotiate contracts about the use of their data and do not have the means to check whether partners live up to the terms of the contract. Data protection laws, regulation and governance aim at establishing fair conditions for drafting contracts about personal data transmission and exchange and providing data subjects with checks and balances, guarantees for redress and means to monitor compliance with the terms of the contract. Flexible pricing, price targeting and price gauging, dynamic negotiations are typically undertaken on the basis of asymmetrical information and great disparities in access to information. Also choice modelling in marketing, micro-targeting in political campaigns, and nudging in policy implementation exploit a basic informational inequality of principal and agent.
3. Informational injustice and discrimination: Personal information provided in one sphere or context (for example, health care) may change its meaning when used in another sphere or context (such as commercial transactions) and may lead to discrimination and disadvantages for the individual. This is

related to the discussion on contextual integrity by Nissenbaum (2004) and Walzerian spheres of justice (Van den Hoven 2008).

4. Encroachment on moral autonomy and human dignity: Lack of privacy may expose individuals to outside forces that influence their choices and bring them to make decisions they would not have otherwise made. Mass surveillance leads to a situation where routinely, systematically, and continuously individuals make choices and decisions because they know others are watching them. This affects their status as autonomous beings and has what sometimes is described as a "chilling effect" on them and on society. Closely related are considerations of violations of respect for persons and human dignity. The massive accumulation of data relevant to a person's identity (e.g. brain-computer interfaces, identity graphs, digital doubles or digital twins, analysis of the topology of one's social networks) may give rise to the idea that we know a particular person since there is so much information about her. It can be argued that being able to figure people out on the basis of their big data constitutes an epistemic and moral immodesty (Bruynseels & Van den Hoven 2015), which fails to respect the fact that human beings are subjects with private mental states that have a certain quality that is inaccessible from an external perspective (third or second person perspective) – however detailed and accurate that may be. Respecting privacy would then imply a recognition of this moral phenomenology of human persons, i.e. recognising that a human being is always more than advanced digital technologies can deliver.

These considerations all provide good moral reasons for limiting and constraining access to personal data and providing individuals with control over their data.

1.5 Law, regulation, and indirect control over access

Acknowledging that there are moral reasons for protecting personal data, data protection laws are in force in almost all countries. The basic moral principle underlying these laws is the requirement of informed consent for processing by the data subject, providing the subject (at least in principle) with control over potential negative effects as discussed above. Furthermore, processing of personal information requires that its purpose be specified, its use be limited, individuals be notified and allowed to correct inaccuracies, and the holder of the data be accountable to oversight authorities (OECD 1980). Because it is impossible to guarantee compliance of all types of data processing in all these areas and applications with these rules and laws in traditional ways, so-called "privacy-enhancing technologies" (PETs) and identity management systems are expected to replace human oversight in many cases. The challenge with respect to privacy in the twenty-first century is to assure that technology is designed in such a way that it incorporates privacy requirements in the software, architecture, infrastructure, and work processes in a way that makes privacy violations unlikely to occur. New generations of privacy regulations (e.g. GDPR) now require standardly a "privacy by design" approach. The data ecosystems and socio-technical systems, supply chains, organisations, including incentive structures, business processes, and technical hardware and software, training of personnel, should all be designed in such a way that the likelihood of privacy violations is a low as possible.

2. The impact of information technology on privacy

The debates about privacy are almost always revolving around new technology, ranging from genetics and the extensive study of bio-markers, brain imaging, drones, wearable sensors and sensor networks, social media, smart phones, closed circuit television, to government cybersecurity programs, direct marketing, surveillance, RFID tags, big data, head-mounted displays and search engines. The impact of some of these new technologies, with a particular focus on information technology, is discussed in this section.

2.1 Developments in information technology

"Information technology" refers to automated systems for storing, processing, and distributing information. Typically, this involves the use of computers and communication networks. The amount of information that can be stored or processed in an information system depends on the technology used. The capacity of the technology has increased rapidly over the past decades, in accordance with Moore's law. This holds for storage capacity, processing capacity, and communication bandwidth. We are now capable of storing and processing data on the exabyte level. For illustration, to store 100 exabytes of data on 720 MB CD-ROM discs would require a stack of them that would almost reach the moon.

These developments have fundamentally changed our practices of information provisioning. The rapid changes have increased the need for careful consideration of the desirability of effects. Some even speak of a digital revolution as a technological leap similar to the industrial revolution, or a digital revolution as a revolution in understanding human nature and the world, similar to the revolutions of Copernicus, Darwin and Freud (Floridi 2008). In both the technical and the epistemic sense, emphasis has been put on connectivity and interaction. Physical space has become less important, information is ubiquitous, and social relations have adapted as well.

As we have described privacy in terms of moral reasons for imposing constraints on access to and/or use of personal information, the increased connectivity imposed by information technology poses many questions. In a descriptive sense, access has increased, which, in a normative sense, requires consideration of the desirability of this development, and evaluation of the potential for regulation by technology (Lessig 1999), institutions, and/or law.

As connectivity increases access to information, it also increases the possibility for agents to *act* based on the new sources of information. When these sources contain personal information, risks of harm, inequality, discrimination, and loss of autonomy easily emerge. For example, your enemies may have less difficulty finding out where you are, users may be tempted to give up privacy for perceived benefits in online environments, and employers may use online information to avoid hiring certain groups of people. Furthermore, systems rather than users may decide which information is displayed, thus confronting users only with news that matches their profiles.

Although the technology operates on a device level, information technology consists of a complex system of socio-technical practices, and its context of use forms the basis for discussing its role in changing possibilities for accessing information, and thereby impacting privacy. We will discuss some specific developments and their impact in the following sections.

2.2 Internet

The Internet, originally conceived in the 1960s and developed in the 1980s as a scientific network for exchanging information, was not designed for the purpose of separating information flows (Michener 1999). The World Wide Web of today was not foreseen, and neither was the possibility of misuse of the Internet. Social network sites emerged for use within a community of people who knew each other in real life – at first, mostly in academic settings – rather than being developed for a worldwide community of users (Ellison 2007). It was assumed that sharing with close friends would not cause any harm, and privacy and security only appeared on the agenda when the network grew larger. This means that privacy concerns often had to be dealt with as add-ons rather than by-design.

A major theme in the discussion of Internet privacy revolves around the use of cookies (Palmer 2005). Cookies are small pieces of data that web sites store on the user's computer, in order to enable personalization of the site. However, some cookies can be used to track the user across multiple web sites (tracking cookies), enabling for example advertisements for a product the user has recently viewed on a totally different site. Again, it is not always clear what the generated information is used for. Laws requiring user consent for the use of cookies are not always successful in terms of increasing the level of control, as the consent requests interfere with task flows, and the user may simply click away any requests for consent (Leenes & Kosta 2015). Similarly, features of social

network sites embedded in other sites (e.g. "like"-button) may allow the social network site to identify the sites visited by the user (Krishnamurthy & Wills 2009).

The recent development of cloud computing increases the many privacy concerns (Ruiter & Warnier 2011). Previously, whereas information would be available from the web, user data and programs would still be stored locally, preventing program vendors from having access to the data and usage statistics. In cloud computing, both data and programs are online (in the cloud), and it is not always clear what the user-generated and system-generated data are used for. Moreover, as data are located elsewhere in the world, it is not even always obvious which law is applicable, and which authorities can demand access to the data. Data gathered by online services and apps such as search engines and games are of particular concern here. Which data are used and communicated by applications (browsing history, contact lists, etc.) is not always clear, and even when it is, the only choice available to the user may be not to use the application.

Some special features of Internet privacy (social media and big data) are discussed in the following sections.

2.3 Social media

Social media pose additional challenges. The question is not merely about the moral reasons for limiting access to information, it is also about the moral reasons for limiting the *invitations* to users to submit all kinds of personal information. Social network sites invite the user to generate more data, to increase the value of the site ("your profile is …% complete"). Users are *tempted* to exchange their personal data for the benefits of using services, and provide both this data and their attention as payment for the services. In addition, users may not even be aware of what information they are tempted to provide, as in the aforementioned case of the "like"-button on other sites. Merely limiting the access to personal information does not do justice to the issues here, and the more fundamental question lies in steering the users' behaviour of sharing. When the service is free, the data is needed as a form of payment.

One way of limiting the temptation of users to share is requiring default privacy settings to be strict. Even then, this limits access for other users ("friends of friends"), but it does not limit access for the service provider. Also, such restrictions limit the value and usability of the social network sites themselves, and may reduce positive effects of such services. A particular example of privacy-friendly defaults is the opt-in as opposed to the opt-out approach. When the user has to take an explicit action to share data or to subscribe to a service or mailing list, the resulting effects may be more acceptable to the user. However, much still depends on how the choice is framed (Bellman, Johnson, & Lohse 2001).

2.4 Big data

Users generate loads of data when online. This is not only data explicitly entered by the user, but also numerous statistics on user behavior: sites visited, links clicked, search terms entered, etc. Data mining can be employed to extract patterns from such data, which can then be used to make decisions about the user. These may only affect the online experience (advertisements shown), but, depending on which parties have access to the information, they may also impact the user in completely different contexts.

In particular, big data may be used in profiling the user (Hildebrandt 2008), creating patterns of typical combinations of user properties, which can then be used to predict interests and behavior. An innocent application is "you may also like …", but, depending on the available data, more sensitive derivations may be made, such as most probable religion or sexual preference. These derivations could then in turn lead to inequal treatment or discrimination. When a user can be assigned to a particular group, even only probabilistically, this may influence the actions taken by others (Taylor, Floridi, & Van der Sloot 2017). For example, profiling could lead to refusal of insurance or a credit card, in which case profit is the main reason for discrimination. When such decisions are based on

profiling, it may be difficult to challenge them or even find out the explanations behind them. Profiling could also be used by organizations or possible future governments that have discrimination of particular groups on their political agenda, in order to find their targets and deny them access to services, or worse.

Big data does not only emerge from Internet transactions. Similarly, data may be collected when shopping, when being recorded by surveillance cameras in public or private spaces, or when using smartcard-based public transport payment systems. All these data could be used to profile citizens, and base decisions upon such profiles. For example, shopping data could be used to send information about healthy food habits to particular individuals, but again also for decisions on insurance. According to EU data protection law, permission is needed for processing personal data, and they can only be processed for the purpose for which they were obtained. Specific challenges, therefore, are (a) how to obtain permission when the user does not explicitly engage in a transaction (as in case of surveillance), and (b) how to prevent "function creep", i.e. data being used for different purposes after they are collected (as may happen for example with DNA databases (Dahl & Sætnan 2009).

One particular concern could emerge from genetics and genomic data (Tavani 2004, Bruynseels & van den Hoven, 2015). Like other data, genomics can be used to make predictions, and in particular could predict risks of diseases. Apart from others having access to detailed user profiles, a fundamental question here is whether the individual should know what is known about her. In general, users could be said to have a right to access any information stored about them, but in this case, there may also be a right not to know, in particular when knowledge of the data (e.g. risks of diseases) would reduce the well-being – by causing fear, for instance – without enabling treatment. With respect to previous examples, one may not want to know the patterns in one's own shopping behavior either.

2.5 Mobile devices

As users increasingly own networked devices such as smart phones, mobile devices collect and send more and more data. These devices typically contain a range of data-generating sensors, including GPS (location), movement sensors, and cameras, and may transmit the resulting data via the Internet or other networks. One particular example concerns location data. Many mobile devices have a GPS sensor that registers the user's location, but even without a GPS sensor, approximate locations can be derived, for example by monitoring the available wireless networks. As location data links the online world to the user's physical environment, with the potential of physical harm (stalking, burglary during holidays, etc.), such data are often considered particularly sensitive.

Many of these devices also contain cameras which, when applications have access, can be used to take pictures. These can be considered sensors as well, and the data they generate may be particularly private. For sensors like cameras, it is assumed that the user is aware when they are activated, and privacy depends on such knowledge. For webcams, a light typically indicates whether the camera is on, but this light may be manipulated by malicious software. In general, "reconfigurable technology" (Dechesne, Warnier, & van den Hoven 2011) that handles personal data raises the question of user knowledge of the configuration.

2.6 The Internet of Things

Devices connected to the Internet are not limited to user-owned computing devices like smartphones. Many devices contain chips and/or are connected in the so-called Internet of Things. RFID (radio frequency identification) chips can be read from a limited distance, such that you can hold them in front of a reader rather than inserting them. EU and US passports have RFID chips with protected biometric data, but information like the user's nationality may easily leak when attempting to read such devices (see Richter, Mostowski & Poll 2008, in Other Internet Resources). "Smart" RFIDs are also embedded in public transport payment systems. "Dumb" RFIDs, basically only containing a number, appear in many kinds of products as a replacement of the barcode, and for use in logistics. Still, such chips could be used to trace a person once it is known that he carries an item containing a chip.

In the home, there are smart meters for automatically reading and sending electricity and water consumption, and thermostats and other devices that can be remotely controlled by the owner. Such devices again generate statistics, and these can be used for mining and profiling. In the future, more and more household appliances will be connected, each generating its own information. Ambient intelligence (Brey 2005), and ubiquitous computing, along with the Internet of Things (Friedewald & Raabe 2011), also enable automatic adaptation of the environment to the user, based on explicit preferences and implicit observations, and user autonomy is a central theme in considering the privacy implications of such devices. In general, the move towards a service-oriented provisioning of goods, with suppliers being informed about how the products are used through IT and associated connectivity, requires consideration of the associated privacy and transparency concerns (Pieters 2013). For example, users will need to be informed when connected devices contain a microphone and how and when it is used.

2.7 E-Government

Government and public administration have undergone radical transformations as a result of the availability of advanced IT systems as well. Examples of these changes are biometric passports, online e-government services, voting systems, a variety of online citizen participation tools and platforms or online access to recordings of sessions of parliament and government committee meetings.

Consider the case of voting in elections. Information technology may play a role in different phases in the voting process, which may have different impact on voter privacy. Most countries have a requirement that elections are to be held by secret ballot, to prevent vote buying and coercion. In this case, the voter is supposed to keep her vote private, *even if she would want to reveal it*. For information technology used for casting votes, this is defined as the requirement of receipt-freeness or coercion-resistance (Delaune, Kremer & Ryan 2006). In polling stations, the authorities see to it that the voter keeps the vote private, but such surveillance is not possible when voting by mail or online, and it cannot even be enforced by technological means, as someone can always watch while the voter votes. In this case, privacy is not only a right but also a duty, and information technology developments play an important role in the possibilities of the voter to fulfill this duty, as well as the possibilities of the authorities to verify this. In a broader sense, e-democracy initiatives may change the way privacy is viewed in the political process.

More generally, privacy is important in democracy to prevent undue influence. While lack of privacy in the voting process could enable vote buying and coercion, there are more subtle ways of influencing the democratic process, for example through targeted (mis)information campaigns. Online (political) activities of citizens on for example social media facilitate such attempts because of the possibility of targeting through behavioural profiling. Compared to offline political activities, it is more difficult to hide preferences and activities, breaches of confidentiality are more likely, and attempts to influence opinions become more scalable.

2.8 Surveillance

Information technology is used for all kinds of surveillance tasks. It can be used to augment and extend traditional surveillance systems such as CCTV and other camera systems, for example to identify specific individuals in crowds, using face recognition techniques, or to monitor specific places for unwanted behaviour. Such approaches become even more powerful when combined with other techniques, such as monitoring of Internet-of-Things devices (Motlagh et al. 2017).

Besides augmenting existing surveillance systems, ICT techniques are nowadays mainly used in the digital domain, typically grouped together under the term "surveillance capitalism" (Zuboff 2019). Social media and other online systems are used to gather large amounts of data about individuals – either "voluntary", because users subscribe to a specific service (Google, Facebook), or involuntary by gathering all kinds of user related data in a less transparent manner. Data

analysis and machine learning techniques are then used to generate prediction models of individual users that can be used, for example, for targeted advertisement, but also for more malicious intents such as fraud or micro-targeting to influence elections (Albright 2016, Other Internet Resources) or referenda such as Brexit (Cadwalladr 2019, Other Internet Resources).

In addition to the private sector surveillance industry, governments form another traditional group that uses surveillance techniques at a large scale, either by intelligence services or law enforcement. These types of surveillance systems are typically justified with an appeal to the "greater good" and protecting citizens, but their use is also controversial. For such systems, one would typically like to ensure that any negative effects on privacy are proportional to the benefits achieved by the technology. Especially since these systems are typically shrouded in secrecy, it is difficult for outsiders to see if such systems are used proportionally, or indeed useful for their tasks (Lawner 2002). This is particularly pressing when governments use private sector data or services for surveillance purposes.

The almost universal use of good encryption techniques in communication systems makes it also harder to gather effective surveillance information, leading to more and more calls for "back doors" that can exclusively be used by government in communication systems. From a privacy standpoint this could be evaluated as unwanted, not only because it gives governments access to private conversations, but also because it lowers the overall security of communication systems that employ this technique (Abelson et al. 2015).

3. How can information technology itself solve privacy concerns?

Whereas information technology is typically seen as the *cause* of privacy problems, there are also several ways in which information technology can help to solve these problems. There are rules, guidelines or best practices that can be used for designing privacy-preserving systems. Such possibilities range from ethically-informed design methodologies to using encryption to protect personal information from unauthorized use. In particular, methods from the field of information security, aimed at protecting information against unauthorized access, can play a key role in the protection of personal data.

3.1 Design methods

Value sensitive design provides a "theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process" (Friedman et al. 2006). It provides a set of rules and guidelines for designing a system with a certain value in mind. One such value can be 'privacy', and value sensitive design can thus be used as a method to design privacy-friendly IT systems (Van den Hoven et al. 2015). The 'privacy by design' approach as advocated by Cavoukian (2009) and others can be regarded as one of the value sensitive design approaches that specifically focuses on privacy (Warnier et al. 2015). More recently, approaches such as "privacy engineering" (Ceross & Simpson 2018) extend the privacy by design approach by aiming to provide a more practical, deployable set of methods by which to achieve system-wide privacy.

The privacy by design approach provides high-level guidelines in the form of principles for designing privacy-preserving systems. These principles have at their core that "data protection needs to be viewed in proactive rather than reactive terms, making privacy by design preventive and not simply remedial" (Cavoukian 2010). Privacy by design's main point is that data protection should be central in all phases of product life cycles, from initial design to operational use and disposal (see Colesky et al. 2016) for a critical analysis of the privacy by design approach). The Privacy Impact Assessment approach proposed by Clarke (2009) makes a similar point. It proposes "a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme" (Clarke 2009). Note that these approaches should not only be seen as auditing approaches, but rather as a means to make privacy awareness and compliance an integral part of the organizational and engineering culture.

There are also several industry guidelines that can be used to design privacy preserving IT systems. The Payment Card Industry Data Security Standard (see PCI DSS v3.2, 2018, in the Other Internet Resources), for example, gives very clear guidelines for privacy and security sensitive systems design in the domain of the credit card industry and its partners (retailers, banks). Various International Organization for Standardization (ISO) standards (Hone & Eloff 2002) also serve as a source of best practices and guidelines, especially with respect to information security, for the design of privacy friendly systems. Furthermore, the principles that are formed by the EU Data Protection Directive, which are themselves based on the Fair Information Practices (Gellman 2014) from the early 70s – transparency, purpose, proportionality, access, transfer – are technologically neutral and as such can also be considered as high level 'design principles'. Systems that are designed with these rules and guidelines in mind should thus – in principle – be in compliance with EU privacy laws and respect the privacy of its users.

The rules and principles described above give high-level guidance for designing privacy-preserving systems, but this does not mean that if these methodologies are followed the resulting IT system will (automatically) be privacy friendly. Some design principles are rather vague and abstract. What does it mean to make a transparent design or to design for proportionality? The principles need to be interpreted and placed in a context when designing a specific system. But different people will interpret the principles differently, which will lead to different design choices, with different effects on privacy. There is also a difference between the design and the implementation of a computer system. During the implementation phase software bugs are introduced, some of which can be exploited to break the system and extract private information. How to implement bug-free computer systems remains an open research question (Hoare 2003). In addition, implementation is another phase wherein choices and interpretations are made: system designs can be implemented in infinitely many ways. Moreover, it is very hard to verify – for anything beyond non-trivial systems – whether an implementation meets its design/specification (Loeckx, Sieber, & Stansifer 1985). This is even more difficult for non-functional requirements such as 'being privacy preserving' or security properties in general.

Some specific solutions to privacy problems aim at increasing the level of awareness and consent of the user. These solutions can be seen as an attempt to apply the notion of informed consent to privacy issues with technology (Custers et al. 2018). This is connected to the idea that privacy settings and policies should be explainable to users (Pieters 2011). For example, the Privacy Coach supports customers in making privacy decisions when confronted with RFID tags (Broenink et al. 2010). However, users have only a limited capability of dealing with such choices, and providing too many choices may easily lead to the problem of moral overload (van den Hoven, Lokhorst, & Van de Poel 2012). A technical solution is support for automatic matching of a privacy policy set by the user against policies issued by web sites or apps.

3.2 Privacy enhancing technologies

A growing number of software tools are available that provide some form of privacy (usually anonymity) for their users, such tools are commonly known as privacy enhancing technologies (Danezis & Gürses 2010, Other Internet Resources). Examples include communication-anonymizing tools such as Tor (Dingledine, Mathewson, & Syverson 2004) and Freenet (Clarke et al. 2001), and identity-management systems for which many commercial software packages exist (see below). Communication anonymizing tools allow users to anonymously browse the web (with Tor) or anonymously share content (Freenet). They employ a number of cryptographic techniques and security protocols in order to ensure their goal of anonymous communication. Both systems use the property that numerous users use the system at the same time which provides k-anonymity (Sweeney 2002): no individual can be uniquely distinguished from a group of size k, for large values for k. Depending on the system, the value of k can vary between a few hundred to hundreds of thousands. In Tor, messages are encrypted and routed along numerous different computers, thereby obscuring the original sender of the message (and thus providing anonymity). Similarly, in Freenet content is stored in encrypted form from all users of the system. Since users themselves do not have the necessary decryption keys, they do not know what kind of content is stored, by the system, on their own computer. This provides plausible deniability and privacy. The system can at any time retrieve the encrypted content and send it to different Freenet users.

Privacy enhancing technologies also have their downsides. For example, Tor, the tool that allows anonymized communication and browsing over the Internet, is susceptible to an attack whereby, under certain circumstances, the anonymity of the user is no longer guaranteed (Back, Möller, & Stiglic 2001; Evans, Dingledine, & Grothoff 2009). Freenet (and other tools) have similar problems (Douceur 2002). Note that for such attacks to work, an attacker needs to have access to large resources that in practice are only realistic for intelligence agencies of countries. However, there are other risks. Configuring such software tools correctly is difficult for the average user, and when the tools are not correctly configured anonymity of the user is no longer guaranteed. And there is always the risk that the computer on which the privacy-preserving software runs is infected by a Trojan horse (or other digital pest) that monitors all communication and knows the identity of the user.

Another option for providing anonymity is the anonymization of data through special software. Tools exist that remove patient names and reduce age information to intervals: the age 35 is then represented as falling in the range 30–40. The idea behind such anonymization software is that a record can no longer be linked to an individual, while the relevant parts of the data can still be used for scientific or other purposes. The problem here is that it is very hard to anonymize data in such a way that all links with an individual are removed and the resulting anonymized data is still useful for research purposes. Researchers have shown that it is almost always possible to reconstruct links with individuals by using sophisticated statistical methods (Danezis, Diaz, & Troncoso 2007) and by combining multiple databases (Anderson 2008) that contain personal information. Techniques such as k-anonymity might also help to generalize the data enough to make it unfeasible to de-anonymize data (LeFevre et al. 2005).

3.3 Cryptography

Cryptography has long been used as a means to protect data, dating back to the Caesar cipher more than two thousand years ago. Modern cryptographic techniques are essential in any IT system that needs to store (and thus protect) personal data, for example by providing secure (confidential) connections for browsing (HTTPS) and networking (VPN). Note however that by itself cryptography does not provide any protection against data breaching; only when applied correctly in a specific context does it become a 'fence' around personal data. In addition, cryptographic schemes that become outdated by faster computers or new attacks may pose threats to (long-term) privacy.

Cryptography is a large field, so any description here will be incomplete. The focus will be instead on some newer cryptographic techniques, in particular homomorphic encryption, that have the potential to become very important for processing and searching in personal data.

Various techniques exist for searching through encrypted data (Song et al. 2000, Wang et al. 2016), which provides a form of privacy protection (the data is encrypted) and selective access to sensitive data. One relatively new technique that can be used for designing privacy-preserving systems is 'homomorphic encryption' (Gentry 2009, Acar et al. 2018). Homomorphic encryption allows a data processor to process encrypted data, i.e. users could send personal data in encrypted form and get back some useful results – for example, recommendations of movies that online friends like – in encrypted form. The original user can then again decrypt the result and use it without revealing any personal data to the data processor. Homomorphic encryption, for example, could be used to aggregate encrypted data thereby allowing both privacy protection and useful (anonymized) aggregate information. The technique is currently not widely applied; there are serious performance issues if one wants to apply full homomorphic encryption to the large amounts of data stored in today's systems. However, variants of the original homomorphic encryption scheme are emerging, such as Somewhat Homomorphic Encryption (Badawi et al. 2018), that are showing promise to be more widely applied in practice.

The main idea behind blockchain technology was first described in the seminal paper on Bitcoins (Nakamoto, n.d., Other Internet Resources). A blockchain is basically a distributed ledger that stores transactions in a non-reputable way, without the use of a trusted third party. Cryptography is used to ensure that all

transactions are "approved" by members of the blockchain and stored in such a way that they are linked to previous transactions and cannot be removed. Although focused on data integrity and not inherently anonymous, blockchain technology enables many privacy-related applications (Yli-Huumo et al. 2016, Karame and Capkun 2018), such as anonymous cryptocurrency (Narayanan et al. 2016) and self-sovereign identity (see below).

3.4 Identity management

The use and management of user's online identifiers are crucial in the current Internet and social networks. Online reputations become more and more important, both for users and for companies. In the era of big data correct information about users has an increasing monetary value.

'Single sign on' frameworks, provided by independent third parties (OpenID) but also by large companies such as Facebook, Microsoft and Google (Ko et al. 2010), make it easy for users to connect to numerous online services using a single online identity. These online identities are usually directly linked to the real world (off line) identities of individuals; indeed Facebook, Google and others require this form of log on (den Haak 2012). Requiring a direct link between online and 'real world' identities is problematic from a privacy perspective, because they allow profiling of users (Benevenuto et al. 2012). Not all users will realize how large the amount of data is that companies gather in this manner, or how easy it is to build a detailed profile of users. Profiling becomes even easier if the profile information is combined with other techniques such as implicit authentication via cookies and tracking cookies (Mayer & Mitchell 2012).

From a privacy perspective a better solution would be the use of attribute-based authentication (Goyal et al. 2006) which allows access of online services based on the attributes of users, for example their friends, nationality, age etc. Depending on the attributes used, they might still be traced back to specific individuals, but this is no longer crucial. In addition, users can no longer be tracked to different services because they can use different attributes to access different services which makes it difficult to trace online identities over multiple transactions, thus providing unlinkability for the user. Recently (Allen 2016, Other Internet Resources), the concept of self-sovereign identity has emerged, which aims for users to have complete ownership and control about their own digital identities. Blockchain technology is used to make it possible for users to control a digital identity without the use of a traditional trusted third party (Baars 2016).

4. Emerging technologies and our understanding of privacy

In the previous sections, we have outlined how current technologies may impact privacy, as well as how they may contribute to mitigating undesirable effects. However, there are future and emerging technologies that may have an even more profound impact. Consider for example brain-computer interfaces. In case computers are connected directly to the brain, not only behavioral characteristics are subject to privacy considerations, but even one's thoughts run the risk of becoming public, with decisions of others being based upon them. In addition, it could become possible to change one's behavior by means of such technology. Such developments therefore require further consideration of the reasons for protecting privacy. In particular, when brain processes could be influenced from the outside, autonomy would be a value to reconsider to ensure adequate protection.

Apart from evaluating information technology against current moral norms, one also needs to consider the possibility that technological changes influence the norms themselves (Boenink, Swierstra & Stemerding 2010). Technology thus does not only influence privacy by changing the accessibility of information, but also by changing the privacy norms themselves. For example, social networking sites invite users to share more information than they otherwise might. This "oversharing" becomes accepted practice within certain groups. With future and emerging technologies, such influences can also be expected and therefore they ought to be taken into account when trying to mitigate effects.

Another fundamental question is whether, given the future (and even current) level of informational connectivity, it is feasible to protect privacy by trying to hide information from parties who may use it in undesirable ways. Gutwirth & De Hert (2008) argue that it may be more feasible to protect privacy by transparency – by requiring actors to justify decisions made about individuals, thus insisting that decisions are not based on illegitimate information. This approach comes with its own problems, as it might be hard to prove that the wrong information was used for a decision. Still, it may well happen that citizens, in turn, start data collection on those who collect data about them, e.g. governments. Such "counter(sur)veillance" may be used to gather information about the use of information, thereby improving accountability (Gürses et al. 2016). The open source movement may also contribute to transparency of data processing. In this context, transparency can be seen as a pro-ethical condition contributing to privacy (Turilli & Floridi 2009).

It has been argued that the precautionary principle, well known in environmental ethics, might have a role in dealing with emerging information technologies as well (Pieters & van Cleeff 2009; Som, Hilty & Köhler 2009). The principle would see to it that the burden of proof for absence of irreversible effects of information technology on society, e.g. in terms of power relations and equality, would lie with those advocating the new technology. Precaution, in this sense, could then be used to impose restrictions at a regulatory level, in combination with or as an alternative to empowering users, thereby potentially contributing to the prevention of informational overload on the user side. Apart from general debates about the desirable and undesirable features of the precautionary principle, challenges to it lie in its translation to social effects and social sustainability, as well as to its application to consequences induced by intentional actions of agents. Whereas the occurrence of natural threats or accidents is probabilistic in nature, those who are interested in improper use of information behave strategically, requiring a different approach to risk (i.e. security as opposed to safety). In addition, proponents of precaution will need to balance it with other important principles, viz., of informed consent and autonomy.

Finally, it is appropriate to note that not all social effects of information technology concern privacy (Pieters 2017). Examples include the effects of social network sites on friendship, and the verifiability of results of electronic elections. Therefore, value-sensitive design approaches and impact assessments of information technology should not focus on privacy only, since information technology affects many other values as well.

Bibliography

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., & Rivest, R. L., 2015, "Keys under doormats: mandating insecurity by requiring government access to all data and communications", *Journal of Cybersecurity*, 1(1): 69–79.

Acar, A., Aksu, H., Uluagac, A. S., & Conti, M., 2018, "A survey on homomorphic encryption schemes: Theory and implementation", *ACM Computing Surveys* (CSUR), 51(4): 79.

Allen, A., 2011, *Unpopular Privacy: What Must We Hide?* Oxford: Oxford University Press.

Anderson, R.J., 2008, *Security Engineering: A guide to building dependable distributed systems*, Indianapolis, IN: Wiley.

Baars, D., 2016, *Towards Self-Sovereign Identity using Blockchain Technology*, Ph.D. Thesis, University of Twente.

Back, A., U. Möller, & A. Stiglic, 2001, "Traffic analysis attacks and trade-offs in anonymity providing systems", in *Information Hiding*, Berlin: Springer, pp. 245–257.

Al Badawi, A., Veeravalli, B., Mun, C. F., & Aung, K. M. M., 2018, "High-performance FV somewhat homomorphic encryption on GPUs: An implementation using CUDA", *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2: 70–95. doi: 10.13154/tches.v2018.i2.70-95

Bellman, S., E.J. Johnson, & G.L. Lohse, 2001, "On site: to opt-in or opt-out?: it depends on the question", *Communications of the ACM*, 44(2): 25–27.

Benevenuto, F., T. Rodrigues, M. Cha, & V. Almeida, 2012, "Characterizing user navigation and interactions in online social networks", *Information Sciences*, 195: 1–24.

Blaauw. M.J., 2013, "The Epistemic Account of Privacy", *Episteme*, 10(2): 167–177.

Boenink, M., T. Swierstra, & D. Stemerding, 2010, "Anticipating the interaction between technology and morality: a scenario study of experimenting with humans in bionanotechnology", *Studies in Ethics, Law, and Technology*, 4(2): 1–38. doi:10.2202/1941-6008.1098

Brey, P., 2005, "Freedom and privacy in ambient intelligence", *Ethics and Information Technology*, 7(3): 157–166.

Broenink, G., J.H. Hoepman, C.V.T. Hof, R. Van Kranenburg, D. Smits, & T. Wisman, 2010, "The privacy coach: Supporting customer privacy in the internet of things", *arXiv preprint* 1001.4459 [available online].

Bruynseels, K & M.J van den Hoven, 2015, "How to do Things with personal Big Biodata", in B. Roessler and D. Mokrokinska (eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives*, Cambridge: Cambridge University Press, pp. 122–40.

Cadwalladr, C., and Graham-Harrison, E., 2018, "The Cambridge analytica files", *The Guardian*, 21: 6–7.

Cavoukian, A., 2009, *Privacy by Design*, Ottowa: Information and Privacy Commissioner of Ontario, Canada. [Cavoukian 2009 available online (PDF)].

–––, 2010, "Privacy by Design: The Definitive workshop", *Identity in the Information Society*, 3(2): 121–126.

Ceross, A., and A. Simpson, 2018, "Rethinking the Proposition of Privacy Engineering", in *Proceedings of New Security Paradigms Workshop* (NSPW '18, Windsor, UK), New York: Association for Computing Machinery, 89–102. doi:10.1145/3285002.3285006

Clarke, R., 2009, "Privacy impact assessment: Its origins and development", *Computer law & security review*, 25(2): 123–135.

Clarke, I., O. Sandberg, B. Wiley, & T. Hong, 2001, "Freenet: A distributed anonymous information storage and retrieval system", in *Designing Privacy Enhancing Technologies*, Berlin: Springer, pp. 46–66.

Colesky, M., J.-H. Hoepman, and C. Hillen, 2016, "A critical analysis of privacy design strategies", *IEEE Security and Privacy Workshops* (SPW), first online O4 August 2016, doi:10.1109/SPW.2016.23

Custers, B., et al., 2018, "Consent and privacy", *The Routledge Handbook of the Ethics of Consent*, London: Routledge, pp. 247–258.

Dahl, J. Y., & A.R. Sætnan, 2009, "It all happened so slowly: On controlling function creep in forensic DNA databases", *International journal of law, crime and justice*, 37(3): 83–103.

Danezis, G., C. Diaz, & C. Troncoso, 2007, "Two-sided statistical disclosure attack", in *Proceedings of the 7th international conference on Privacy enhancing technologies*, Berlin: Springer, pp. 30–44.

DeCew, Judith Wagner, 1997, *Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Ithaca, NY: Cornell University Press.

Dechesne, F., M. Warnier, & J. van den Hoven, 2013, "Ethical requirements for reconfigurable sensor technology: a challenge for value sensitive design", *Ethics and Information Technology*, 15(3): 173–181.

Delaune, S., S. Kremer, & M. Ryan, 2006, "Coercion-resistance and receipt-freeness in electronic voting", in the *Proceedings of the 19th IEEE Computer Security Foundations Workshop*, IEEE Computer Society Press, pages 28–39. [Delaune et al. 2006 available online]

Dingledine, R., N. Mathewson, & P. Syverson, 2004, "Tor: The second-generation onion router", in *Proceedings of the 13th conference on USENIX Security Symposium* (Volume 13), Berkeley, CA: USENIX Association, pp. 303–320 [Dingledine et al. 2004 available online (pdf)]

Douceur, J., 2002, "The Sybil attack", in *Peer-to-peer Systems*, Berlin: Springer, pp. 251–260.

Ellison, N. B., 2007, "Social network sites: Definition, history, and scholarship", *Journal of Computer-Mediated Communication*, 13(1): 210–230.

Evans, N.S., R. Dingledine, & C. Grothoff, 2009, "A practical congestion attack on Tor using long paths", in *Proceedings of the 18th conference on USENIX security symposium*, Berkeley, CA: USENIX Association, pp. 33–50. [Evans et al. 2009 available online]

Falgoust, M., 2016, "Data Science and Designing for Privacy", *Techné: Research in Philosophy and Technology*, 20 (1): 51–68.

Floridi, L., 2008, "Artificial intelligence's new frontier: Artificial companions and the fourth revolution", *Metaphilosophy*, 39(4–5): 651–655.

Friedewald, M. & O. Raabe, 2011, "Ubiquitous computing: An overview of technology impacts", *Telematics and Informatics*, 28(2): 55–65.

Friedman, B., P.H. Kahn, Jr, & A. Borning, 2006, "Value sensitive design and information systems", in *Human-computer interaction in management information systems: Foundations*, P. Zhang & D. Galletta (eds.), Armonk: M.E. Sharp, 4.

Gentry, C., 2009, "Fully homomorphic encryption using ideal lattices", in *Proceedings of the 41st annual ACM symposium on Theory of computing*, ACM, pp. 169–178.

Goyal, V., O. Pandey, A. Sahai, & B. Waters, 2006, "Attribute-based encryption for fine-grained access control of encrypted data", in *Proceedings of the 13th ACM conference on Computer and communications security*, ACM, pp. 89–98.

Gürses, S., A. Kundnani, & J. Van Hoboken, 2016, "Crypto and empire: the contradictions of counter-surveillance advocacy", *Media, Culture & Society*, 38(4): 576–590.

Gutwirth, S. & P. De Hert, 2008, "Regulating profiling in a democratic constitutional state", in Hildebrandt and Gutwirth 2008: 271–302.

den Haak, B., 2012, "Integrating user customization and authentication: the identity crisis", *Security & Privacy, IEEE*, 10(5): 82–85.

Heersmink, R., J. van den Hoven, N.J. van Eck, & J. van den Berg, 2011. "Bibliometric mapping of computer and information ethics", *Ethics and information technology*, 13(3): 241–249.

Hildebrandt, M., 2008, "Defining Profiling: A New Type of Knowledge?" in Hildebrandt and Gutwirth 2008: 17–45.

Hildebrandt, M. & S. Gutwirth (eds.), 2008, *Profiling the European Citizen: Cross-disciplinary Perspectives*, Dordrecht: Springer Netherlands.

Hoare, T., 2003, "The verifying compiler: A grand challenge for computing research", in *Proceedings of the 12th international conference on Compiler construction*, Berlin: Springer, pp. 262–272.

Hone, K. & J.H.P. Eloff, 2002, "Information security policy – what do international information security standards say?", *Computers & Security*, 21(5): 402–409.

van den Hoven, J., 1999, "Privacy and the Varieties of Informational Wrongdoing", *Australian Journal of Professional and Applied Ethics*, 1(1): 30–44.

–––, 2008, "Information technology, privacy, and the protection of personal data", in *Information technology and moral philosophy*, J. Van Den Hoven and J. Weckert (eds.), Cambridge: Cambridge University Press, pp. 301–322.

van den Hoven, J., G.J. Lokhorst, & I. Van de Poel, 2012, "Engineering and the problem of moral overload", *Science and engineering ethics*, 18(1): 143–155.

van den Hoven, J., Vermaas, P., & Van de Poel, I. (eds.), 2015, *Handbook of Ethics, Values and Technological Design*, Dordrecht: Springer.

Karame, G., and Capkun, S., 2018, "Blockchain Security and Privacy", *IEEE Security Privacy*, 16(4), 11–12.

Ko, M.N., G.P. Cheek, M. Shehab, & R. Sandhu, 2010, "Social-networks connect services", *Computer*, 43(8): 37–43.

Krishnamurthy, B. & C.E. Wills, 2009. "On the leakage of personally identifiable information via online social networks", in *Proceedings of the 2nd ACM workshop on Online social networks*, ACM, pp. 7–12.

Lawner, K. J., 2002, "Post-September 11th International Surveillance Activity – A Failure of Intelligence: The Echelon Interception System & (and) the Fundamental Right to Privacy in Europe", *Pace International Law Review*, 14(2): 435–480.

Leenes, R., and E. Kosta, 2015, "Taming the cookie monster with dutch law-a tale of regulatory failure", *Computer Law & Security Review* 31(3): 317–335.

LeFevre, K., D.J. DeWitt, & R. Ramakrishnan, 2005, "Incognito: Efficient full-domain k-anonymity", in *Proceedings of the 2005 ACM SIGMOD international conference on Management of data*, ACM, pp. 49–60.

Lessig, Lawrence, 1999, *Code and Other Laws of Cyberspace*, New York: Basic Books.

Loeckx, J., K. Sieber, & R.D. Stansifer, 1985, *The foundations of program verification*, Chichester: John Wiley & Sons.

Matheson, David, 2007, "Unknowableness and Informational Privacy", *Journal of Philosophical Research*, 32: 251–67.

Mayer, J.R. & J.C. Mitchell, 2012, "Third-party web tracking: Policy and technology", in *Security and Privacy (SP) 2012 IEEE Symposium on*, IEEE, pp. 413–427.

Michener, J., 1999, "System insecurity in the Internet age", *Software*, IEEE, 16(4): 62–69.

Motlagh, N. H., Bagaa, M., & Taleb, T., 2017, "UAV-based IoT platform: A crowd surveillance use case", *IEEE Communications Magazine*, 55(2): 128–134.

Nissenbaum, Helen, 2004, "Privacy as Contextual Integrity", *Washington Law Review*, 79: 101–139.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S., 2016, *Bitcoin and cryptocurrency technologies: a comprehensive introduction*, Princeton: Princeton University Press.

Negley, G., 1966, "Philosophical Views on the Value of Privacy", *Law and Contemporary Problems*, 31: 319–325.

OECD, 1980 [2013], *The OECD Privacy Framework*, 2013, available in PDF; revised and expanded from the original *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Organization for Economic Co-operation and Development, [1980 version available online]

Palmer, D.E., 2005, "Pop-ups, cookies, and spam: toward a deeper analysis of the ethical significance of internet marketing practices", *Journal of business ethics*, 58(1–3): 271–280.

Pieters, W., 2011, "Explanation and trust: what to tell the user in security and AI?", *Ethics and information technology*, 13(1): 53–64.

–––, 2013, "On thinging things and serving services: technological mediation and inseparable goods", *Ethics and information technology*, 15(3): 195–208.

–––, 2017, "Beyond individual-centric privacy: Information technology in social systems" *The Information Society*, 33(5): 271–281.

Pieters, W. & A. van Cleeff, 2009, "The precautionary principle in a world of digital dependencies", *Computer*, 42(6): 50–56.

Rössler, Beate (ed.), 2004, *Privacies: Philosophical Evaluations*, Stanford, CA: Stanford University Press.

Rössler, Beate, 2005, *The value of privacy*, Cambridge: Polity Press.

–––, 2001 [2005], *The Value of Privacy*, Cambridge: Polity Press; original German version *Der Wert des Privaten*, Frankfurt am Main: Suhrkamp Verlag, 2001.

Rubel, Alan, 2011, "The Particularized Judgment Account of Privacy", *Res Publica*, 17(3): 275–90.

Ruiter, J. & M. Warnier, 2011, "Privacy Regulations for Cloud Computing: Compliance and Implementation in Theory and Practice", in *Computers, Privacy and Data Protection: an Element of Choice*, S. Gutwirth, Y. Poullet, P. De Hert, and R. Leenes (eds.), Dordrecht: Springer Netherlands, pp. 361–376.

Solove, D., 2006, "A Taxonomy of Privacy", *University of Pennsylvania Law Review*, 154: 477–564.

Som, C., L.M. Hilty, & A.R. Köhler, 2009, "The precautionary principle as a framework for a sustainable information society", *Journal of business ethics*, 85(3): 493–505.

Song, D.X., D. Wagner, & A. Perrig, 2000, "Practical techniques for searches on encrypted data", in *Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on*, IEEE, pp. 44–55.

Sprenger, Polly, 1999, "Sun on Privacy: 'Get Over It'", *Wired*. [Sprenger 1999 available online]

Sweeney, L., 2002, "K-anonymity: A model for protecting privacy", *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05): 557–570.

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.

Taylor, L., L. Floridi, and B. Van der Sloot (eds.), 2017, *Group privacy: New challenges of data technologies* (Philosophical Studies Series: Vol. 126), Dordrecht: Springer.

Thomson, Judith Jarvis, 1975, "The Right to Privacy", *Philosophy and Public Affairs*, 4: 295–314.

Turilli, M. & L. Floridi, 2009, "The ethics of information transparency", *Ethics and Information Technology*, 11(2): 105–112.

Wang, Y., Wang, J., and Chen, X., 2016, "Secure searchable encryption: a survey", *Journal of Communications and Information Networks*, 1(4): 52–65.

Warnier, M., Dechesne, F., and Brazier, F.M.T., 2015, "Design for the Value of Privacy", in J. van den Hoven, P. Vermaas, I. van de Poel (eds.), *Handbook of Ethics, Values, and Technological Design*, Dordrecht: Springer, 431–445.

Warren, Samuel D. & Louis D. Brandeis, 1890, "The Right to Privacy", *Harvard Law Review*, 4(5): 193–220. [Warren and Brandeis 1890 available online]

Westin, Alan F., 1967, *Privacy and Freedom*, New York: Atheneum.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., and Smolander, K., 2016, "Where is current research on blockchain technology? – a systematic review", *PloS One*, 11(10): e0163477. doi:10.1371/journal.pone.0163477

Zuboff, S., 2019, *The age of surveillance capitalism: the fight for the future at the new frontier of power*, London: Profile Books.

Academic Tools

Other Internet Resources

- Albright, J., 2016, "How Trump's campaign used the new data-industrial complex to win the election", LSE, US Centre, USApp-American Politics and Policy Blog.
- Allen, C., 2016, The Path to Self-Sovereign Identity, Coindesk.
- Cadwalladr, C., 2019, Facebook's role in Brexit – and the threat to democracy. TED Talk
- Danezis, G & S. Gürses, 2010, "A critical review of 10 years of Privacy Technology."
- Gellman, R., 2014, "Fair information practices: a basic history,", Version 2.12, August 3, 2014, online manuscript.
- Nakamoto, S., Bitcoin: A Peer-to-Peer Electronic Cash System, www.bitcoin.org.
- PCI DSS (= Payment Card Industry Data Security Standard), v3.2 (2018), PCI DSS related documents, PCI Security Standards Council, LLC.
- Richter, H., W. Mostowski, & E. Poll, 2008, "Fingerprinting passports", presented at NLUUG Spring Conference on Security.
- Electronic Privacy Information Center.
- European Commission, Data protection.
- US Department of State, Privacy Act.

Related Entries

computing: and moral responsibility | ethics: search engines and | information | information technology: and moral values | privacy | social networking and ethics

Stanford | Center for the Study of Language and Information