Beyond individual-centric privacy
Information technology in social systems

Pieters, Wolter

DOI
10.1080/01972243.2017.1354108

Publication date
2017

Document Version
Accepted author manuscript

Published in
Information Society

Beyond individual-centric privacy: Information technology in social systems

Wolter Pieters, Faculty of Technology, Policy and Management, Delft University of Technology, Delft, The Netherlands

This is an Accepted Manuscript of an article published by Taylor & Francis in *The Information Society* on 3 Oct 2017, available online: http://www.tandfonline.com/doi/full/10.1080/01972243.2017.1354108.

Abstract

In the public debate, social implications of information technology are mainly seen through the privacy lens. Impact assessments of information technology are also often limited to privacy impact assessments, which are focused on individual rights and well-being, as opposed to the social environment. In this paper, I argue that this perspective is too narrow, in terms of understanding the complexity of the relation between information technology and society, as well as in terms of directions for managing this relation. I use systems theory to show that current approaches focus mostly on individual impact of information technology developments rather than their mediating role in society itself. I argue that this should be complemented by an analysis of impact on individuals (psychic systems) *via* co-construction of the environment (social system). I then take up the question what the role of information technology in social systems would look like in terms of the social relations of trust and power, and how this can complement privacy in discussions on impacts of information technology.

Keywords: impact assessment, information technology, privacy, social sustainability, social systems, systems theory

Introduction

The preoccupation with personal data and privacy in the public debate has a spillover effect on the discourse on other concerns raised by the spread of information technology (IT). What is particularly problematic is that with its focus on access to *personal* data it skews the overall discourse towards impacts of IT-related developments on *individuals* rather than the role of IT on the societal level. For instance, legal compliance with privacy and data security regulation is the main driver of security implementation in companies, as opposed to protection of operational capabilities of critical infrastructure from cyber attacks (Ponemon Institute 2016). Given the increasing reliance of our society on information technology, I consider the focus on privacy, and thereby individual impacts of IT-related developments, quite problematic. This paper therefore aims at providing a basis for discussing the (in)adequacy of the individual-centric privacy lens, and proposing an alternative one.

This is not the first paper trying to extend the scope of privacy discussions. In 2004 Marlin-Bennett (2004) pointed out that privacy regulation is just another instance of policy for governing information flows. She went on to connect the discussion on privacy to the discussion on intellectual property. Similarly, the European Union’s Directive on Network and Information Security (NIS) focuses on the protection of societal infrastructure rather than personal data. Also, informed by the discourse on technology and values, approaches such as value-sensitive design (Friedman et al. 2014; Van den Hoven 2007) advance a broader perspective, and would in principle be applicable to any type of affected value, such as consent, fairness and wellbeing. The specific contribution of this paper is that it draws on systems theory to propose an alternative lens that takes into account the role of IT-related developments in the *social environment* of individuals – thereby affecting the individuals as well – rather than as direct consequences for the individuals themselves. This draws attention to the mediating role of IT in societal developments and in the construction of social systems, which in turn enable and constrain individual experience and action.

The fact that I speak of effects, impact or influence of IT in this paper is not intended as an endorsement of theoretical frameworks that attribute agency to technology and artefacts (cf. Verbeek 2005). I do not aim to engage in that discussion here. Rather, depending on the position taken, the effects can be attributed to human-technology constellations of which IT becomes part, or to human actions only, mediated by the technology. From a system-theoretic perspective, the focus is rather on interactions between systems of different kinds, where systems may act as each other's environment. This is why I prefer to speak of impact of IT-related *developments*. The core argument – a plea for more focus on the social environment – applies regardless of where exactly the system boundaries are drawn, as long as the basic distinction between individuals and social environment is upheld.

Moreover, assessment of the impact of IT is not meant to imply that the influence is unidirectional. Technology, individuals and social systems co-evolve, and social forces co-shape technology. Nevertheless, when introducing new technologies in society, we need to pursue some understanding of how they would fit within a social context, and what changes that might imply for individuals and society, notwithstanding the possibility that these can affect the technology themselves. In fact, one of the motivations for conducting an impact assessment is to enable early intervention in the design of the technology at hand. Thus, rather than understanding the impact of IT as impact of the "pure" technology, it should be understood as the impact of the embedding of the technology in a socio-technical context. This holds for both the impact on the individual and impact on the social environment.

The discussion proceeds as follows. I first illustrate the limitations of the privacy impact framing of values affected by IT in more detail with two examples – the demise of electronic voting in the Netherlands, and the discussion on the impact of social networking services. I then analyse the limitations more systematically, and show that they are connected to related problems in impact assessment and social sustainability. Finally, I will discuss how a social systems approach can contribute to a more balanced view.

Examples of problematic privacy-centric framing

There are several cases in which discussion on the role of new IT in society has focused on privacy, reducing emphasis on other impacts. In this section I will discuss two of those, in order to get a better understanding of the limitations of such privacy framing.

Electronic voting

The Dutch e-voting controversy (Jacobs and Pieters 2009; Pieters, Hadžiosmanović and Dechesne 2015) illustrates how the focus on privacy, or framing an issue in terms of privacy, may obscure other impacts of IT-related developments.

From the early 1990s onwards, ballot boxes in the Netherlands got replaced with electronic voting machines. By 2006, almost all of the precincts used electronic voting machines. When Amsterdam introduced electronic voting in 2006, a pressure group argued for a return to paper voting because it enabled citizens to observe the process. It used an excellent media strategy to make its case. It took apart voting machines and showed how chips with the counting programs could be replaced with fraudulent ones. Furthermore, the group found that it was possible to violate the secrecy of the votes by a TEMPEST attack, wherein a radio antenna is used to capture electromagnetic radiation emitted by the device (Gonggrijp and Hengeveld 2007). Because of the radiation problems, the certification of some machines was suspended before the 2006 elections. Subsequently, the Election Process Advisory Commission studied both the past and the future of electronic voting (Hermans and Van Twist 2007; Election Process Advisory Commission 2007). Since the radiation problems could not be solved, all forms of electronic voting were abandoned.

Now, the reason why the machines *should* have been abolished is the lack of verifiability of the result of the election. Fraudulent machines could have a major impact on the future of the nation, and would be very hard to detect. Instead, the whole move towards abolishment was focused on the TEMPEST attack, and thereby on voter privacy. Whereas the secret ballot is obviously important to prevent coercion and vote buying, the likelihood of this attack would have been much lower, as the gain for the attacker is rather minimal (except maybe in case of capturing the votes of celebrities). Moreover, the likelihood of detecting a TEMPEST attack is higher.

The reason for focusing on privacy is nonetheless simple. Nowhere in the law, nor in lower-level legislation, was there any mention of transparency or verifiability of election results. Thus, the only legal means the government had to “fight the machines” was *privacy-type regulation*, namely the provision of the secret ballot in the constitution and the election law. This was the reason given for the suspension of the first certification, and this was also the reason given for not implementing the “future” commission’s proposal. According to many, the verifiability problems were far worse, but there was nothing in either law or lower level regulation that addressed this issue. The existence of privacy legislation, as opposed to legislation on other facets of information technology use, blurs the real issues here, and creates a false picture of what to expect with emerging technologies. As a result of the focus on privacy, the *power of both the manufacturers and external attackers,* in terms of the opportunity to manipulate the machines undetected and the *risk for trust in the democratic process,* were largely ignored.

Therefore, although the Dutch electronic voting controversy was *framed* as a privacy-type issue (Pieters 2009), there was certainly more at stake. This shows that social issues related to IT cannot be understood in terms of privacy only. In addition, the Dutch case spotlights *the temptation to interpret problems in terms of the existing privacy-based legal and policy infrastructure*. The fact that the current legal framework applicable to IT focuses on privacy, mediates perception in such a way that every social problem induced by IT appears as a privacy problem. As shown here, this is unsatisfactory for the electronic voting case.

Social media

Also in case of impact of the introduction of social networking services in society, the emphasis is mostly put on how these services handle customer data, i.e. privacy (cf. e.g. Boyd 2008; Hull, Lipford, & Latulipe 2011). While it seems natural to give social network users more control over the visibility of their data to others (privacy settings and associated defaults), as we will see, there are several points of view that challenge this framing of the problem.

Firstly, privacy settings only control the visibility of personal data with respect to other users. They do not affect the visibility of data to the social networking service provider itself. So, even if you hide data for your friends, it could still be used for, say, targeted advertisements. In effect, limiting access to other users does not in any way limit what the social networking service provider can do based on its own access. Assuming that users value privacy, there is then an incentive for the provider to frame the privacy problem as a matter of getting the inter-user settings right, so that the users see that something is being done about privacy. This obscures the fundamental power issue that has to do with the access and power of the *provider*, not the other users.

Secondly, the power issues are not only about accessibility of data. In a controversial experiment, Facebook manipulated the timelines of users to study the effect this had on their own posts.[1] Although the results may be scientifically interesting, problems of consistency with the Data Use Policy and general principles of consent in research are obvious, as no consent was obtained for such manipulation. However, the issue is broader than just manipulation for research purposes. Manipulation could occur for any purpose, and it is almost impossible to find out when something has been manipulated. This holds for inclusion of items in timelines, ranking of search results, etc. Many "promoted" items on social media are highlighted as such, but how can we know that other manipulations do not occur? As in elections, integrity of the information provided is a key issue here.

Thirdly, how the use of social networking services affects our social lives, for instance what they mean for the value of friendship or for values associated with self-presentation (Fröding and Peterson 2012; Rosen 2007; Vallor 2012), is also out of scope when the focus is on privacy. These topics do get some attention, but not as much as privacy. Again, the focus on the potential harm for an individual in a privacy violation detracts attention from potential harm for society (e.g. decaying social capital because of lack of "real" friendships).

Limitations

[1] http://www.forbes.com/sites/gregorymcneal/2014/06/28/facebook-manipulated-user-news-feeds-to-create-emotional-contagion/#b4ddd9c5fd8c, consulted February 26, 2016

This leads us to two limitations of the current perspective on privacy as the primary social value to be protected in technological developments. Firstly, social structures and relations can be changed through developments involving IT *without undue access to and use of personal data*. Even though privacy problems may themselves mediate broader social changes (Hillyard and Knight 2004), privacy does not need to be an intermediate variable here, and social issues related to information technology do not always need to be explained in terms of personal data of individuals. Secondly, a key issue here is the *integrity* of the information, not the confidentiality. In both changing of election results and changing of people's Facebook timelines, information is not so much used inappropriately, but changed inappropriately. Not all values affected by information technology are therefore related to confidentiality (or opacity) of (personal) information.

After considering these concrete examples, let us now turn to a more theoretical perspective on why privacy is insufficient as an instrument for discussing social impacts of information technology.

The institutionalisation of the problem

In this section, I will discuss the institutionalisation of the problem – how the focus on privacy has become embedded in society. I will spotlight three problematic aspects of privacy in the social impact of IT context: (1) privacy as a human right instead of an instrumental value or duty (moral status), (2) privacy impact assessment as the principal approach, as opposed to social impact assessment, and (3) the focus on increasing individual control as a solution to privacy problems (control as a solution).

Privacy as a human right

Especially in the legal and political debate, privacy often tends to be seen as a human right, going back to the "right to be left alone" judgment of the US Supreme Court (Warren & Brandeis 1890). This makes it an intrinsic value, in the sense that it is worth pursuing for its own sake. However, there are also reasons for protecting privacy to realise other objectives, rendering it an instrumental value. Not surprisingly, systematic argumentations relating privacy for such goals come from philosophy, for example the moral reasons for protecting privacy as provided by Van den Hoven (2008):

- Prevention of information-based harm;
- Prevention of informational inequality;
- Prevention of informational injustice and discrimination;
- Safeguarding autonomy.

Such moral reasons are obscured when privacy is conceived as an intrinsic value or human right. Again the case of voting illustrates the limitations. Typically the rules for the voting process mention the secret ballot as one of the integral requirements of the voting process as part of modern democracies, sometimes even safeguarding it in the constitution. However, the historical reasons for the introduction of the secret ballot were related to prevention of vote buying and coercion (Park 1931). Thus the secret ballot was instrumental for realising other objectives. Apart from that, there does not appear to be any reason for wanting to keep the choices secret. In fact, many people opposed the secret ballot when it was introduced, as it was seen as introducing an undesirable opacity to what was considered a public duty (Park 1931). Contemporarily, Estonia introduced Internet voting on the rationale that voting secrecy will be less of an imperative, if the voter would have the possibility to override her vote later (Drechsler 2003). Although such measures obviously do not provide complete protection, they illustrate that there are instrumental reasons for protecting privacy, and also instrumental reasons for replacing it by something else if this is judged beneficial in new circumstances. In the case of voting, these instrumental reasons may have been lost sight of over the course of history.

Thus, the privacy concerns in electronic voting are not exactly privacy concerns in the human rights sense. Not only should my vote be kept secret, it should be kept secret *even if I wished to reveal it*. The aim is not only to protect citizens from consequences of unintentionally having their vote revealed (e.g. by means of coercion), but also from intentionally revealing their vote (e.g. in order to sell it). The latter constraint protects not so much individual rights or interests, but rather imposes individual *duties* (voting secretly) that are in turn meant to protect society (from large-scale vote buying). A case in point is the recent discussion on whether "selfies" should be allowed in the voting booth – pictures of oneself with the marked ballot (The Economist 2014). Ultimately, the protection is against parties with economic or other forms of power gaining political influence.

Privacy impact assessment as the principal approach

The most widely approach for assessing the social impact of IT is the privacy impact assessment. It is conceived of as an analogy to the environmental impact assessment, which deals with potential impact of a technology or development of an area on the environment (Clarke 2009; Wright 2013). Not surprisingly, the focus in a privacy impact assessment is on impacts related to privacy and personal data.

A much broader concept is social impact assessment (Freudenberg 1986; Becker 2001). The scope of a social impact assessment can include both micro-level impact (including privacy), but also meso- and macro-level (e.g. organisations and nations, respectively; see Becker

2001). The key observation here is that, when discussing impacts of IT, the public discourse has centered on privacy impact assessment rather than social impact assessment, thereby emphasising individual rather than social impact. This leads to the question whether it would be feasible to use the broader social impact assessment instead, and if so, how.

Control as a solution

Beyond framing of the problem itself, the solution frames are also skewed when impact of IT is understood in terms of privacy. Solutions to problems are often framed in terms of increasing people's control over their personal data, by giving them choices or asking them for consent. This is a relatively straightforward solution. However, it is also too limited in several respects. First of all, people only have a limited capacity for making choices. Decision making capacities can be exhausted, causing people to make quick choices (e.g. clicking consent on privacy policies). Secondly, not all people can be assumed to have this ability (e.g. children). Finally, as indicated above, there may be reasons not to give people a choice (e.g. privacy as a duty). Schermer, Custers, and Van der Hof (2014) have discussed in detail why consent as a solution to privacy issues is problematic. In the context of the present paper, the key insight is that such solutions focus on individuals and their privacy decisions, without considering that both the problems and the solutions may lie somewhere else. Individual-centric framing of impact foregrounds individual-centric solutions and backgrounds possible interventions at societal level.

We have seen how our conceptions of privacy encourage a privacy-centric framing, despite its limitations, of issues raised by IT. The limitations indicated above provide reasons for a move towards a framework that is not privacy- and individual-centric. But social impact assessment also has its complications. A major problem here is that we do not have a well-developed concept of *social sustainability* as a basis for understanding social impact.

Social sustainability as a key concept

Sustainability refers to the use of resources in such a way that future generations are not deprived of using them for their own needs. It is categorised into environmental, economic and social sustainability. It is widely acknowledged that social sustainability is the hardest aspect to define (McKenzie 2004; Littig and Griessler 2005; Lindblad-Gidlund 2010). There are extensive lists of factors that are said to contribute to social sustainability, including sense of community, equity between generations, and mechanisms for political advocacy (McKenzie 2004).

Not only is social sustainability hard to define, its application is also limited. The focus tends to be on environmental and economic sustainability and social sustainability is usually regarded as an additional condition (McKenzie 2004). Social sustainability is typically viewed along the following lines: while protecting the environment, we should not forget to meet the needs of the local people.

Thus, social impact assessments suffer from an ill-defined notion of *social sustainability*. When an alternative perspective on values appears, as in the human rights perspective on privacy, it is tempting to leverage this other framework for impact assessment, replacing social impact assessment with privacy impact assessment. This explains at least partly why a relatively restricted domain of privacy has tended to be the focus of impact assessment of IT, and why in general little attention is paid to social impact. Without the tools to describe social impact in a similar sense as environmental impact, it is much easier to focus on the impact of

IT-related developments on individuals and their personal data rather than on the impact on the social environment.

In sum, one way out of the limitations we encounter lies in properly defining the social environment. In order to apply broader notions of sustainability and impact assessment to social impact of information technology, we need to be more precise about what it is that constitutes a social environment, and how it can be affected by IT. I will pursue this direction further by focusing on the concept of social systems.

A systems theory solution

In this paper, I will use systems theory as a basis for broadening the discussion. This is not the only possible choice, and any framework focusing primarily on relations rather than entities can provide valuable contributions. Similar analyses are for example possible from the point of view of phenomenology (Pieters 2011b). However, precisely because systems theory makes the relation between individuals and their social environment explicit, I choose to use it for the purpose of the argument in this paper. I will first introduce the notion of social systems, and then focus on power and trust as values in them.

Social systems

In systems theory, systems are characterised as "creating and maintaining a difference from their environment" (Luhmann 1995, 17). Niklas Luhmann makes a distinction between psychic and social systems from the perspective of systems theory. *Psychic systems* (representing people) and *social systems* (representing communication and social structures) both process meaning, but they act as each other's environment. Whereas psychic systems represent the individual minds, social systems represent the communication structure between them. According to Luhmann, there exists a mutual dependency of psychic and social systems. Interactions between the two types of systems take place when individuals (psychic systems) engage in communication (social system). The social system serves as the environment of the psychic systems, and vice versa.

The focus on the individual and her rights puts emphasis on the psychic systems, and regards the social systems as more elusive, and therefore less amenable to regulation and legislation. The notion that the spread of IT may erode my privacy and thereby limit my functioning as a psychic system can be understood as a conception wherein protection of personal information is seen as protection of private property rather than that of the public good (cf. Post 1990). Following Luhmann's theory, any impact on the psychic systems (individuals) will be accompanied by an impact on the social system (communication and social structures). In fact, IT developments might *primarily* affect the social system of communication, changing the environment of the psychic systems, thereby affecting those as well. The social system then acts as the environment of individuals, and thereby generates second-order impact of IT-related developments on psychic systems. Luhmann's theory can thus explain (1) why privacy provides a too limited picture on the effects, and (2) the focus on privacy can be understood as a focus on individuals (psychic systems) as opposed to communication and societal structures (social systems).

Based on the analysis above, I argue for a solution directed towards *including social systems and psychic systems as complements* in the analysis of social impact of IT-related developments. If impact occurs on both psychic systems and social systems in their mutual dependency, what would such impact look like?

Let us first turn towards the concept of sustainability. One of the reasons why social sustainability has not been properly defined is that the distinction between the *satisfaction of needs of individuals* and the *quality of the social environment* has not been drawn clearly. Is taking the needs of local people into account really social sustainability? Typically, sustainability refers to maintaining an *environment* that enables people to thrive, so it is focused on the environment rather than individual people and their rights or needs per se. The concept of sustainability spotlights precisely that individual needs may be met *through* such an environment. Thus for social sustainability this would imply that the social environment should be the central concept. In a high-quality social environment, values are embedded that enable individuals to thrive, for example in the form of separation of powers. Again, the distinction between individual impact and social impact is vital for understanding the issues at hand. The analytical advantage of following Luhmann here is that social systems can be thought of in a similar way to ecosystems – just like biotechnology may influence the ecosystem, information technology may influence the social environment.

We can therefore redefine social sustainability as the property of a development that *maintains or enhances the quality of a social system as an environment for psychic systems*. This, in turn, may induce positive effects for the individuals (psychic systems) that are dependent on it. This does not mean that the social system should be static or centrally controlled; rather, dynamism and participation are often essential for the stability of a system.

Power

In this context, we can thus rephrase the effect of IT-related developments as impacting individuals also *indirectly*, via impact on the *social environment* or social system. I argue that the notion of *power* should have a central place in social impact assessments of information technology, as it is a relation within the social system that can easily be affected, since information provides a basis for controlling one’s environment. This control is not an individual property, but a relation of communication between people that forms part of the social system, and from this position influences the individuals involved.

Recent research on power signifies either a relation between power and negative sanctions, or a focus on the functional dimension, i.e. its role in constraining actions (Borch 2005). Following Luhmann’s systems theory, power can be interpreted as a means of reducing social complexity, by regulating the action of others and self. Various authors differ in their opinion whether the means of this regulation need to be specified further. Luhmann himself (1979) points to negative sanctions, but Borch considers only the functional aspects important. Borch considers “the reliance on negative sanctions as only one among many ways of conditioning action through action” (161).

Certainly, information is an important prerequisite for regulation of action, whether of self or of others. This holds both in case of enabling the possibility of negative sanctions as well as in case of other means. For example, in the case of (electronic) voting, coercion or vote buying is only possible if it can be reasonably ascertained whether the voter complied. This does not always imply individual proof of one’s vote, as reference can also be made to precinct results or prevailing moral sentiments of compliance (Brusco et al. 2004). Conversely, if one wants to influence the results of an election by means of manipulation of results, one needs to make sure that certain information (i.e. information about the manipulation) does *not* spread.

Within the relation between information and power, a distinction can be made between optimising one’s own actions by means of information and influencing others’ actions by means of information. In the latter case, the flow of information is such that others are “invited” to act differently than they would have done otherwise, e.g. in the coercion example. This “invitation” is possibly related to negative sanctions, but for example in vote buying, the sanctions can also be positive. In the former case, the flow of information is such that one can act differently oneself by means of acquired information, such that one’s actions can contribute better to achieving one’s goals.

In both cases, information is a means to achieve certain goals, but in the latter case (influencing others’ actions), others also seem to be used as means for achieving these goals. It can therefore be considered the ethically more problematic form. However, to understand social impact of information technology, a focus on this negative form is inadequate. For example, the discussions on the acceptability of the personal information collection by companies such as Google and Facebook (e.g. Dwyer 2011; Rosen 2011) can only be understood by including the power they acquire for achieving their own goals. The big problems are not necessarily related to impact on an individual user, but rather to acquiring loads of information about the *collective* of users, beneficial to deciding on the owners’ actions (e.g. targeted advertisements). As a side effect, this may also lead to users behaving differently, but this is not the goal. (It *is* the goal in case of surveillance cameras.) Voters may also behave differently if they have the impression that the secrecy of their vote is not guaranteed, independently of whether they are actually being coerced (Oostveen and Van den Besselaar 2005).

As a means for action, information itself can become a goal as well, requiring more information to steer other actions towards achieving this information as a goal. Thus, such social system impact in terms of power can change social relations and communication, thereby impacting the action possibilities of psychic systems (individuals).

Trust

Another factor in social system impact of IT-enabled information rearrangements is *trust*, which is often connected to 'social capital' (see e.g. Portes 1998). Again, information plays a profound role in trust relations. In earlier work (Pieters 2006), I used Luhmann's distinction between confidence and trust (Luhmann 1988) to specify the notion in more detail, where confidence means reliance without a conscious decision, and trust means reliance with a conscious choice between alternatives. With regards to information, trust requires information about alternatives, whereas confidence does not.

Provision of too much information can in fact reduce trust in a system. For example, a system for verifying the correct counting of one's vote in an election can reduce trust in the system if the procedure reveals too much detail (Hubbers et al. 2005). This in turn may influence trust in democracy and government. Complexities of this relation between explanation of an information technology system and trust are discussed elsewhere (Pieters 2011a). In particular, technology can induce shifts between confidence and trust in relations of assurance. Electronic voting technology may make inspection of the system impossible to the general public, possibly transforming trust into confidence. On the other hand, information technologies can provide information to the public based on which they can compare alternatives, changing confidence into trust. Certainly, the increasing availability of countless sources of information can be said to shift expectations towards trust rather than confidence. Comparison websites are just one example here. Conversely, such sites may invite precisely the behaviour of not consciously deciding oneself, which would point in exactly the other direction (towards confidence). This shows that the impacts of IT-related developments on trust relations are not unequivocal, and that actual changes need to be subjected to empirical study. That changes do occur seems likely though, and if implemented wrongly, developments could harm confidence or trust (as in the vote verification example).

This also points to a relation with the choices that information technology makes available or does not make available to users. In psychology, it has been determined that giving too many options (i.e. too much information) to customers reduces the number of sold products *and* customer satisfaction (Iyengar and Lepper 2000). The latter can again influence the trust of the customer in the provider. Current product comparison websites may induce similar effects. This possibility is only hinted at (and deemed unlikely for their particular data) by Wilson and Waddams Price (2010), but would be worthy of further study, as it could shed light on influences of IT on general trust relations. Social system impact on trust also explains why more individual control as a solution does not work well. Giving the user a choice assumes that she has sufficient information and time to make that choice. If not, then distrust can be the result.

Here, the most important lesson is that the design of information technologies can change trust relations, not only between users and the system, but also between other actors. This change in the social system can then affect the wellbeing of the associated individuals. Again, the change in trust relations and associated communication – social system impact – can in turn change the action possibilities of individuals.

Causal insulation

In the discussions on trust and power, I have shown which relations in social systems can serve as starting points for analysing social impact of information technology. However, the system-theoretic perspective on how such impact comes about needs additional detail. In particular, how can systems theory help to explain why and how information technology influences social systems? For this, we need to look into how systems theory handles causation in relation to information.

In systems theory, Luhmann (2005) developed the notion of causal insulation to describe the separation of a technological system from its environment (Pieters 2011c). According to Luhmann, technology can only function if it has such a protective boundary. This would mostly relate to keeping unwanted causes outside of the system. However, when we also include preventing certain causes within the technology to influence the outside, this directly points to safety issues in technology. For example, one does not want the nuclear contents of a power plant to influence its environment, or genetically modified organisms to influence their natural surroundings. Safety properties of technology can thus be established by designing the proper causal insulation. Safety impacts of technological developments are then related to causes that "escape" and cause harm in the environment.

In the domain of information in social systems, things are slightly different. Firstly, we will have to deal with security rather than safety properties, meaning that the origin of a threat is to be found in intentional action, for example an individual or organisation having an interest in acquiring or changing certain information. In this case, there is an agent in the social system that, by means of the technology under consideration and associated possibilities for accessing information, can change relations in the social system**.** In addition, the notion of causes in information is different, as information is usually associated with *reasons* for action. So, rather than causing a direct effect in the environment, IT *enables* agents to achieve impact in the social environment. These actions by agents then affect trust and power.

Similarly, Floridi (2005) uses the term *ontological friction* to describe restrictions on the flow of information in the so-called infosphere (Floridi 1999), i.e. a topology based on information access rather than physical distance. He employs it in the context of privacy, where privacy increases as actors encounter more ontological friction when attempting to access personal information. Hofkirchner (2010) interprets friction as something bad that needs to be overcome, but here it would be more meaningful to consider it as something that contributes to privacy, and security of information in general. Vuorinen and Tetri (2012) use the concepts of machine and territory for similar purposes. All these approaches point to the distribution of and access to information as a central property in social systems that can be changed by information technology. This distribution of and access to information can thus be used to describe the manifestations of trust and power in society that information technology can influence, thereby impacting the action possibilities of individuals as well as social sustainability. For example, the power obtained by personalised search results based on large-scale data collection inhibits individuals from gathering information that does not fit their "profile" (the so-called filter bubble; Bozdag & Van den Hoven 2015).

Thus, causal insulation can be interpreted in an informational sense. It can then represent protection against social impacts of IT analogous to protection against environmental impact of technology. We then speak of causal insulation between meaningful pieces of data and people (potentially malevolent) seeking access as information security properties, like one would speak of causal insulation between potentially dangerous artefacts and their surroundings as environmental safety properties. This allows us to describe how information technology can influence the distribution of access to information, and thereby social system properties such as trust and power.

Information ethics as an alternative ontology

As a final note, I would like to consider the relation of the broader view on IT-related impacts *via the environment* with information ethics (Floridi 1999; 2005) in more detail. In particular, if we follow Floridi in interpreting *all of the environment* in informational terms (infosphere), what would be the emerging picture?

Floridi (2005), in his ontological interpretation of privacy, draws attention to information flows and access to information as the fundamental variables for issues studied in IT and society area. Information technologies change the amount of effort required for certain actors to access certain information and thereby enable new flows of information. For example, Facebook makes it easier for the user to acquire information about her friends, but it also makes it easier for advertisers to gain information about who are most likely to be interested in their products.

When applied to personal information, i.e. information about natural persons, this framework enables accounts of how information technology influences privacy, by making it easier or harder for other actors to access information about persons. It also applies to election integrity, in the sense that electronic voting technologies may make it easier (or harder) for certain actors to access (and change) the election results. In general such changed access relations, in turn, change the way in which the actors involved are able to act. Actions are typically based on available information, and when it is easier to use additional information, this may lead to other actions, or even enable new kinds of actions. We therefore need to be mindful that the information technology has a bearing not just on flow of *personal* information.

Compared to the causal insulation perspective, where the notion of infosphere is merely a pragmatic topology denoting access relations between pieces of information, Floridi goes one step further and develops ethical principles for the infosphere. He proposes a generalised ontology in terms of information, where the infosphere does not only cover entities that we typically associate with information, i.e. humans and information technologies, but all of reality. In this sense, Floridi's information ethics can be seen as a generalisation of environmental ethics.

Floridi argues that information ethics should be based on the principle of entropy reduction. In ethical analysis, entities can then be investigated *as* informational entities, with their moral status related to their informational status, rather than for example their status as a human or other living creature. The value of entities is thus expressed in terms of these entities being informational entities, contributing to the flourishing of the infosphere. Destruction or corruption of such informational entities contributes to entropy, which, according to information ethics, ought to be prevented in the infosphere. The reason for protecting systems would then be the preservation of these systems *as* informational entities.

The move from a social systems ontology to an informational ontology immediately poses the question how the relational concepts from systems theory would translate to the infosphere. For example, can we still speak of trust and power?

A first attempt to answer this question would take us back to environmental sustainability. Here we will need to describe relations in ecosystems in terms of trust and power, when the composing organisms are conceived as informational entities. One could then, speculatively, try to explain symbiosis relations in terms of trust, and ways in which organisms control their environment in terms of power. As the modest aim of this section is merely to point to the similarities between information ethics and the broader perspective of IT-related impacts, and highlight the benefits of future research into their connections, I leave further development of these ideas to follow-up studies.

The conclusion drawn here is that *if* one accepts the premises of information ethics in terms of a generalised informational ontology, *then* impacts in terms of the distribution of information can apply to all of the infosphere, ontologically interpreted. As said, this either requires broadening definitions of social relations beyond social systems, or including non-social relations in the list of relations that contribute to information preservation.

Conclusions

At the beginning of this paper, I expressed a concern with respect to the (over)emphasis on privacy as the core value affected by information technology. Inspired by the analytical framework of systems theory, I have argued for a focus on social systems as a complement to psychic systems, where social systems constitute an environment in which individuals can (or cannot) thrive.

I have illustrated the current state of understanding with the examples of electronic voting in the Netherlands, where privacy replaced verifiability as the political and legal justification for abolishing electronic voting, and social media, where privacy settings obscure power relations between the provider and the users. I have also pointed to discussions on impact assessment and sustainability as potential sources of confusion, because social impact assessment has been replaced by privacy impact assessment in the IT context, and the notion of social sustainability is ill-defined.

In terms of an alternative lens, I have built upon Luhmann's work in systems theory to advance trust and power as values in particular affected by information technology, within a more general framework of changes in information access. Rather than focusing on the effect of IT-related developments on individuals and their privacy, this frames the problem in terms of impact on the *environment* of individuals. In systems theory, this can be thought of in terms of changes in causal insulation. In Floridi's information ethics, ontological friction points to the same issue, and can even pave the way towards a more general understanding of ethics as dealing with distribution of information. And, in terms of private property versus public goods, we can start to understand the implications of current private data harvesting developments such as social media as a tragedy of the commons: as individuals we all benefit, but we exhaust the public good of power balances in society, by contributing to new forms of information and capital accumulation (Fuchs 2010).

To operationalise this broader view, methods need to be devised that guide designers and policy makers in dealing with the uncertainties of technology to be developed or already in existence. In this context, privacy impact assessment is only a micro-level social impact assessment, and inadequate to cover meso- and macro-levels (Becker 2001). The notion of social impact assessment, as discussed earlier, has the potential of broadening the scope of the assessment to include meso- and macro-level impact. However, as we have also seen, the domain of information certainly poses specific challenges to the impact assessment, which include 1) the problem of intentional action and 2) the notions of confidentiality and integrity, in addition to availability. To broaden the scope from privacy to other impacts, *and* to emphasise the specific characteristics of information, I advocate using the social impact assessment for impact of information technologies, instead of the too narrow privacy impact assessment. Rather than focusing on privacy only, such an assessment would include the impact on social relations including trust, power, and others such as friendship. Alternatively, this investigation of the impact of IT-related developments on social sustainability could be called *information impact assessment*.[2] Developing contents and procedure of such an assessment would need to draw upon existing work in both computer science (information security) and ethics of technology.

I hope that this paper shows that from the perspective of technology and human values, the discussion on social impact of information technology should be broadened beyond privacy, and that investigating the distribution of information access, with its impact on trust and power, would be the key conceptual endeavour here. Correspondingly, empirical studies in which the two-step impact of IT-related developments on environment and then individuals is investigated would be extremely valuable.

Acknowledgements

The author wishes to thank Shannon Spruit and Marlies van de Voort for substantial help with the revision, and Marga Groothuis for helpful comments at an earlier stage. Many thanks also to the editor-in-chief for very detailed suggestions. The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement number ICT-318003 (TREsPASS). This publication reflects

[2] Although information impact assessment has been considered before in the context of development projects in developing countries (Menou 1995), its application to the impact of information technology seems to be new. Menou defines the central question in information impact assessment as “What, if any, is/was the contribution of information to the effective solution of problem X?” Here, I am interested in the question “What, if any, is/was the contribution of treatment Y to the distribution of information in the infosphere?” Similarly, this may also require broadening the notion of privacy by design (Kroener and Wright 2014).

only the authors' views and the Union is not liable for any use that may be made of the information contained herein.

References

Becker, Henk A. 2001. "Social impact assessment." *European Journal of Operational Research* 128.2: 311-321.

Borch, Christian. 2005. "Systemic Power Luhmann, Foucault, and analytics of power." *Acta Sociologica* 48.2: 155-167.

Boyd, Danah. 2008. “Facebook's Privacy Trainwreck.” *Convergence: The International Journal of Research into New Media Technologies* 14.1: 13-20.

Bozdag, Engin, and Van den Hoven, Jeroen. 2015. “Breaking the filter bubble: democracy and design.” *Ethics and Information Technology* 17.4: 249-265.

Brusco, Valeria, Marcelo Nazareno, and Susan Carol Stokes. 2004. "Vote buying in Argentina." *Latin American Research Review* 39.2: 66-88.

Clarke, Roger. 2009. "Privacy impact assessment: Its origins and development." *Computer law & security review* 25.2: 123-135.

Drechsler, Wolfgang. 2003. "The Estonian e-voting laws discourse: Paradigmatic benchmarking for central and Eastern Europe". Accessed March 21, 2014, http://unpan1.un.org/intradoc/groups/public/documents/nispacee/unpan009212.pdf.

Dwyer, Catherine. 2011. "Privacy in the Age of Google and Facebook." *Technology and Society Magazine, IEEE* 30.3: 58-63.

The Economist. 2014. "The ‘boothies’ craze." The Economist, accessed May 23, 2014. http://www.economist.com/blogs/charlemagne/2014/05/european-elections.

Election Process Advisory Commission. 2007. "Voting with confidence." Kiesraad, Accessed 26 November 2010, http://www.kiesraad.nl/nl/Overige_Content/Bestanden/pdf_thema/Pdf_voor_Engelse_site/Voting_with_confidence.pdf.

Floridi, Luciano. 1999. "Information ethics: on the philosophical foundation of computer ethics." *Ethics and information technology* 1.1: 33-52.

Floridi, Luciano. 2005. "The ontological interpretation of informational privacy." *Ethics and Information Technology* 7.4: 185-200.

Friedman, Batya, Peter H. Kahn Jr., and Alan Borning. 2014. In N. Doorn, D. Schuurbiers, I. van de Poel, and M.E. Gorman (Eds), "Value sensitive design and information systems." *Early engagement and new technologies: Opening up the laboratory*, 55-95. Dordrecht, the Netherlands: Springer.

Freudenburg, William R. 1986. "Social impact assessment." *Annual review of sociology* (1986): 451-478.

Fröding, Barbro, and Martin Peterson. 2012. "Why virtual friendship is no genuine friendship." *Ethics and information technology* 14.3: 201-207.

Fuchs, Christian. 2010. Labor in Informational Capitalism and on the Internet. *The Information Society,* 26.3: 179-196.

Gonggrijp, Rop, and Willem-Jan Hengeveld. 2007. "Studying the Nedap/Groenendaal ES3B voting computer: A computer security perspective." In *Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology*, p. 1. Berkeley, CA: USENIX Association.

Gutwirth, Serge, and Paul De Hert. 2008. "Regulating profiling in a democratic constitutional state." In M. Hildebrandt and S. Gutwirth (eds), *Profiling the European citizen*, 271-302. Dordrecht, the Netherlands: Springer.

Hermans, L.M.L.H.A., van Twist, M.J.W. 2007. "Stemmachines: een verweesd dossier." Rapport van de commissie besluitvorming stemmachines. Accessed 19 August 2013. http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2007/04/17/stemmachines-een-verweesd-dossier/rapportstemmachineseenverweesddossier.pdf.

Hillyard, Daniel P., and Sarah M. Knight. 2004. "Privacy, technology, and social change." *Knowledge, Technology & Policy* 17.1: 81-101.

Hofkirchner, Wolfgang. 2010. "How to design the infosphere: The fourth revolution, the management of the life cycle of information, and information ethics as a macroethics." *Knowledge, Technology & Policy* 23.1-2: 177-192.

Hubbers, Engelbert, Jacobs, Bart, and Pieters, Wolter. 2005. "RIES: Internet voting in action." In *COMPSAC 2005: Proceedings of the 29th Annual International Computer Software and Applications Conference*, 417-424. Washington, DC: IEEE Computer Society.

Hull, Gordon, Lipford, Heather R., and Latulipe, Celine. 2011. “Contextual gaps: Privacy issues on Facebook.” *Ethics and information technology* 13.4: 289-302.

Iyengar, Sheena S., and Mark R. Lepper. 2000. "When choice is demotivating: Can one desire too much of a good thing?" *Journal of personality and social psychology* 79.6: 995-1006.

Jacobs, Bart, & Pieters, Wolter. 2009. “Electronic Voting in the Netherlands: from early Adoption to early Abolishment.” In *Foundations of security analysis and design V* (pp. 121-144). Springer Berlin Heidelberg.

Kroener, Inga, and David Wright. 2014. "A Strategy for Operationalizing Privacy by Design." *The Information Society* 30.5: 355-365.

Lindblad-Gidlund, Katarina 2010. "The reflexive designer–a method for sustainable IT development." *International journal of sustainable society* 2.4: 406-419.

Littig, Beate, and Erich Griessler. 2005. "Social sustainability: a catchword between political pragmatism and social theory." *International Journal of Sustainable Development* 8.1: 65-79.

Luhmann, Niklas. 1995. *Social Systems*. Stanford, CA: Stanford University Press.

Luhmann, Niklas. 1979. *Trust and Power: Two Works by Niklas Luhmann*. Chichester, UK: Wiley.

Luhmann, Niklas. 1988. Familiarity, Confidence, Trust: Problems and Alternatives. In D. Gambetta (Ed.), *Trust: Making and Breaking Cooperative Relations* (chapter 6, pp. 94-107). Oxford, UK: Basil Blackwell.

Luhmann, Niklas. 2005. *Risk: a sociological theory*. New Brunswick, NJ: Transaction.

Marlin-Bennett, Renée. 2004. *Knowledge Power: Intellectual Property, Information, and Privacy*. Boulder, CO: Lynne Rienner.

McKenzie, Stephen. 2004. *Social Sustainability: Towards some definitions* (Working Paper Series No 27). Adelaide, Australia: Hawke Research Institute, University of South Australia. Accessed 21 October 2014. https://www.sapo.org.au/binary/binary141/Social.pdf.

Menou, Michel J. 1995. "The impact of information—I. Toward a research agenda for its definition and measurement." *Information Processing & Management* 31.4: 455-477.

Oostveen, Anne-Marie, and Peter Van Den Besselaar. 2005. "Trust, identity, and the effects of voting technologies on voting behavior." *Social Science Computer Review* 23.3: 304-311.

Park, Joseph H. 1931. "England's controversy over the secret ballot." *Political Science Quarterly* (1931): 51-86.

Pieters, Wolter. 2006. "Acceptance of voting technology: between confidence and trust." In K. Stølen, W.H. Winsborough, F. Martinelli, and F. Massacci (eds), *Trust Management: 4th International Conference, iTrust 2006*, 283-297 (Lecture Notes in Computer Science 3986). Berlin: Springer.

Pieters, Wolter. 2009. "Combatting electoral traces: the Dutch tempest discussion and beyond." In P.Y.A. Ryan and B. Schoenmakers (eds), *E-Voting and Identity: Second International Conference, VOTE-ID 2009,* 172-190 (Lecture Notes in Computer Science 5767). Berlin: Springer.

Pieters, Wolter. 2011a. "Explanation and trust: what to tell the user in security and AI?" *Ethics and Information technology* 13.1: 53-64.

Pieters, Wolter. 2011b. "Rev{a,i}ling the Risks: A phenomenology of information security." *Techné: Research in Philosophy and Technology* 14.3: 194-206.

Pieters, Wolter. 2011c. "The (social) construction of information security." *The Information Society* 27.5: 326-335.

Pieters, Wolter, Hadžiosmanović, Dina, & Dechesne, Francien. 2015. “Security-by-experiment: Lessons from responsible deployment in cyberspace.” *Science and engineering ethics* 22.3: 831-850.

Ponemon Institute. 2016. *2016 Global Encryption Trends Study*. https://www.thales-esecurity.com/~/media/Files/Thales%20e%20Security/Global/Analyst%20Reports/Global%20Encryption%20Trends%20Study%20eng%20ar.pdf. Consulted April 13, 2016.

Portes, Alejandro. 1998. “Social capital: Its origins and applications in modern sociology.” *Annual review of sociology* 24.1: 1-24.

Post, Robert C. 1990. “Rereading Warren and Brandeis: Privacy, Property, and Appropriation.” *Case Western Reserve Law Review* 41: 647-680.

Rosen, Christine. 2007. "Virtual friendship and the new narcissism." *The New Atlantis: A Journal of Technology and Society* 17.2: 15-31.

Rosen, Jeffrey. 2011. "The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google." *Fordham Law Review,* 80: 1525-1538.

Schermer, Bart W., Bart Custers, and Simone Van der Hof. 2014. "The crisis of consent: how stronger legal protection may lead to weaker consent in data protection." *Ethics and Information Technology* 16.2: 171-182.

Som, Claudia, Lorenz M. Hilty, and Andreas R. Köhler. 2009. "The precautionary principle as a framework for a sustainable information society." *Journal of Business Ethics* 85.3: 493-505.

Vallor, Shannon. 2012. "Flourishing on facebook: virtue friendship & new social media." *Ethics and Information technology* 14.3: 185-199.

Van den Hoven, Jeroen. 2007. "ICT and value sensitive design." In P. Goujon and S. Lavelle (eds), *The information society: Innovation, legitimacy, ethics and democracy in honor of Professor Jacques Berleur S.J.*, 67-72. New York: Springer.

Van den Hoven, Jeroen. 2008. "Information technology, privacy, and the protection of personal data." In *Information technology and moral philosophy*, edited by Jeroen van den Hoven and John Weckert, 301-322. Cambridge: Cambridge University Press.

Verbeek, Peter-Paul. 2005. *What things do: Philosophical reflections on technology, agency, and design*. Penn State Press.

Vuorinen, Jukka, and Pekka Tetri. 2012. "The order machine–the ontology of information security." *Journal of the Association for Information Systems* 13.9: 695-713.

Warren, Samuel D. and Louis D. Brandeis. 1890. “The Right to Privacy.” *Harvard Law Review,* 4.5: 193–220.

Wilson, Chris M. and Catherine Waddams Price. 2010. “Do consumers switch to the best supplier? *Oxford Economic Papers* 62.4: 647-668.

Wright, David. 2013. "Making privacy impact assessment more effective." *The Information Society* 29.5: 307-315.