

PETs under Surveillance: A critical review of the potentials and limitations of the privacy as confidentiality paradigm

Seda Gürses¹, Bart Preneel¹, and Bettina Berendt²

¹ ESAT/COSIC and IBBT

K.U. Leuven

Heverlee, Belgium

`Seda|Bart.Preneel@esat.kuleuven.be`

² HMDB

Departement Computerwetenschappen

K.U. Leuven

Heverlee, Belgium

`Bettina.Berendt@cs.kuleuven.be`

Abstract. "Privacy as confidentiality" has been the dominant paradigm in computer science privacy research. Privacy Enhancing Technologies (PETs) that guarantee confidentiality of personal data or anonymous communication have resulted from such research. The objective of this paper is to show that such PETs are indispensable but are short of being the privacy solutions they sometimes claim to be given current day circumstances. We will argue using perspectives from surveillance studies that the computer scientists' conception of privacy through data or communication confidentiality is techno-centric and displaces end-user perspectives and needs in a surveillance society. We will further show that the perspectives from surveillance studies demand a critical review for their human-centric conception of information systems. Last, we reposition PETs in a surveillance society and argue for the necessity of multiple paradigms for privacy design.

1 Introduction

My concern has been and will continue to be directed solely at striking a balance between democracy and technology, between the advantages of computerization and the potential safeguards that are inherent in it and the right of every citizen to the protection of his right of privacy.[15]

These are the words of Representative Cornelius Gallagher who through a series of hearings in 1966 had brought the problem of computerization and its threats to privacy to public consciousness. Interestingly, today many of the arguments that Gallagher gave in his hearings still prevail. At the time, Gallagher was responding to plans to introduce a National Data Center that would collect information about every U.S. citizen and his hearings articulated important

challenges to the then nascent scientific discipline of computer science. Shortly after these hearings Gallagher was a keynote speaker at the American Federation of Information Processing Societies' 1967 Spring Joint Computer Conference in New Jersey, USA ³ and consequently his words were echoed in the Communications of the ACM [45].

Given that special historical constellation we can state that 1967 was the year in which privacy as a research topic was introduced to the then young field of computer science. ⁴ At the conference a session on privacy problems was introduced and a total of 5 papers were presented on the topic of privacy. ⁵ Privacy was never defined in these papers but assumed to be confidentiality of data, the breach of privacy then meaning the leakage of data to unauthorized principals in military and non-military systems. Although Representative Gallagher defined privacy as the right to freedom of action, speech, belief or conscience and listed potential risks of information collection to these [15], the transposition of the concept to research in computer science was limited to data confidentiality and secrecy of communications.

Research on privacy enhancing technologies that guarantee some type of data confidentiality and hence user privacy have been an important research topic ever since. ⁶ The data that is kept confidential using PETs may be stored data, communicated data, or the conditions of a given communication – most often limited to the anonymity of the sender and/or receiver of the communication. This research has resulted in the development of various systems that have important functions for guaranteeing anonymous speech, encrypted communications and unlinkable electronic activities in a networked world. ⁷

The objective of this paper is to show that data confidentiality and anonymous communication, two important properties of privacy enhancing technologies that represent what we call the *privacy as confidentiality* paradigm, are indispensable but are short of being the privacy solutions they claim to be given current day circumstances. We argue that this is the case because so far computer

³ The series of conferences commenced in 1961 and were dissolved in 1990 [39]

⁴ Although in the presented papers articulations of privacy and security solutions have parallels to the much longer standing tradition of cryptography and security research, we in this paper start our account of computer science privacy research with the explicit introduction of the term "privacy" at the Spring Joint Computer Conference.

⁵ Three of the authors were from the RAND Corporation [48][35], one from M.I.T [16] and one from a company named Allen-Babcock Computing [1].

⁶ In the last 10 years privacy has become one of the central concerns of Pervasive Computing, in Europe often researched under the title Ambient Intelligence. The journal IEEE Security and Privacy, for example, was a side effect of these research fields, giving recent privacy research a visible publication [9].

⁷ Later, other sub-fields in computer science have proposed other types of PETs that often rely on the contractual negotiation of personal data revelation. A review of such PETs can be found in [47] but are not the focus of this paper since they are not based on the same assumptions that "privacy as confidentiality" is dependent on.

scientists' conception of privacy through data or communication confidentiality has been mostly techno-centric and displaces end-user perspectives.

By techno-centric we mean a perspective which is mainly interested in understanding how technology leverages human action, taking a largely functional or instrumental approach that tends to assume unproblematically that technology is largely exogenous, homogenous, predictable, and stable, performing as intended and designed across time and place [32]. This perspective tends to put technology in the center, blend out cultural and historical influences, and produces technologically deterministic claims.

For some critical perspectives on current day conditions and how these escape techno-centric narrations of PETs, we survey perspectives from an emerging field called surveillance studies. We later shortly evaluate the consequences of these perspectives for computer scientists and designers of systems. In this evaluation we point to the human-centric assumptions of the surveillance studies perspectives. Human-centricity focuses on how humans make sense of and interact with technology in various circumstances. The technology is understood to be different depending on meanings humans attribute to it and through the different ways people interact with it. This approach takes cultural and historical contexts into consideration, but has a tendency to minimize the role of technology itself [32].

As suggested in [32] in this paper we study how materiality i.e., in our case technology, and the social are constitutively entangled. Meaning that PETs and social privacy practices in a surveillance world cannot be seen as ontologically distinct matters but constitute each other: social practices in a surveillance world are constituted by existing surveillance practices and by PETs, whereas the latter are the product of humans and their social practices. Hence, we review both techno- and human-centric views on PETs, and propose ways forward that makes use of their constitutive entanglement.

Our main contribution with this paper is a critical interdisciplinary review of PETs that explores their potentials and limitations in a world of rapidly developing technology, ubiquitous surveillance, as well as changing perceptions, legislation and practices of privacy. Similar critique of PETs have been written in the past [37, 42, 44]. We have included the first two of these perspectives in the later sections. In addition to reviewing critiques, the contributions of this paper are valuable for the following: First, confidentiality as *the* way to preserve privacy is a recurring theme in privacy debates generally and in computer science specifically. Therefore, a review whether this holds given changing social conditions is important. Second, we have some additional arguments in the section on "the information perspective" which can provide interesting challenges to privacy research in computer science. Further and most important of all, our argument is not that anonymity and confidentiality tools should be done away with. On the contrary, we believe that they need to be re-contextualized in the surveillance world in order to adapt the assumptions and claims of PETs to changing user requirements.

The paper is organized as follows. In Section 2 we give an overview of computer science research on privacy as data confidentiality and anonymity. Here we also list some of the assumptions common to this type of research. Next, in Section 3 we give accounts of different perspectives on surveillance society and their implications for the privacy as confidentiality paradigm generally and for the use of PETs specifically. We then return to the assumptions in Section 4. In the conclusion we critically review PETs and the surveillance perspectives and identify a multi-paradigm approach for privacy research in computer science.

2 Privacy as Data Confidentiality and Anonymity

2.1 Personal Data as the focus of PETs

In those initial papers on privacy presented at the 1967 Spring Joint Computer Conference [16, 1, 35, 48, 49] the researchers had noticed the importance of sensitive data, but what actually counted as "private" sensitive data was difficult to define. The authors distinguished between military and non-military systems, with the latter meaning industrial or non-military governmental agencies. Their objective was to devise systems such that they could avoid intentional or accidental disclosure of sensitive confidential data belonging to other users [48]. In defining how to classify private information, a pragmatic approach was to ask how the military classification of document confidentiality i.e. confidential, highly-confidential, top secret, could somehow be mapped onto sensitive personal data. It was also discussed, if such a mapping was unrealistic when a central authority and the necessary discipline was lacking in non-governmental/private computer networks [49].

In all the papers, confidentiality, a concept that played an important role in military think, was chosen as the main paradigm for privacy research. The authors were aware that military concepts could not be applied to the society at large, hence all the papers tried to distinguish security (military) from privacy (non-military), yet they had few other frameworks to take as a reference.

Ever since, there has been much progress in "non-military" contexts defining what should count as *informational privacy* [20, 41, 30] and how sensitive data can be defined. Various data protection legislations have defined the category "personal data" as subject to privacy protection. An example is the EU Directive that states: *Personal data* are "any information relating to an identified or identifiable natural person [...]; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (EU Directive 95/46/EC [14], Art. 2 (a)).

Important for our purposes is the emphasis on identity, which is assumed to be unique for one natural person, to which data traces can be linked to. In line with this emphasis, US terminology talks about *personally identifiable* data. This emphasis on identity is coupled with a relative under-specification of content that counts as personally identifiable data. The standard types of personally

identifiable data are profile data describing individuals, including name, address, health status, etc.

It is probably in line with this focus on identity and identifiability that, in comparison to the contributions at the 1967 Spring Joint Computer Conference, from the 80s onwards PETs focusing on the unlinkability of identity from generated digital data gained in popularity. In addition to the legal definitions, in computer science identifiability included inferring the individual to whom data belongs to with certainty but also probabilistically. The construct of probabilistic identification has contributed to the expansion of what could count as personal data.⁸

2.2 Anonymity as a privacy enhancing mechanism

Once data about a person exists in a digital form it is very difficult to provide that person with any guarantees on the control of that data. This lack of control has contributed to personal data leakages and undesirable secondary use of personal data on the Internet⁹, often leading to privacy breaches. Much of the personal data collected using current day technologies represent activities of individuals assumed to be private or shared by a few prior to their digitization. Not digitizing these activities and avoiding the exchange of such digitized data would avoid further parties acquiring knowledge of these activities. But, this would substantially limit many of the technologies we use daily and is often undesirable for reasons we will account for in later sections.

A weaker form of preserving privacy is then to keep personal data confidential from a greater public. This would require the use of cryptography and secure systems: the prior has so far proven difficult for users, while the latter is extremely difficult to accomplish in networked systems.

A yet another form of privacy can be achieved through what is called anonymity. Anonymity keeps the identity of the persons in information systems confidential but is not primarily concerned with how public the traces consequently become. This is also reflected in data protection legislation which by definition cannot and does not protect anonymous data [19]. Anonymity is achieved by unlinking the identity of the person from the traces of his/her activities leave in information systems.

⁸ The consequences of probabilistic identification as legal evidence has been picked up by Sandra Braman [5] but is beyond the scope of this paper. Similarly, in [52] the authors problematize some of the heuristics used to probabilistically infer information about individuals based on the characteristics shared by their network vicinity. The authors argue that the heuristics are comparable to notions like "birds of a feather flock together", "judge a man by the company he keeps", or "guilty by association".

⁹ The focus of this paper is on privacy concerns raised and privacy enhancing technologies used on the Internet. We are aware that breaches also occur with devices that are off-line and on networks other than the Internet. Further, mobile technology has opened up a whole new set of questions about the feasibility of privacy enhancement with respect to location data. Whether the same assumptions and analyses hold for these problems is beyond the scope of this paper.

In technical terms, anonymity can be based on different models. In communications, anonymity is achieved when an individual is not identifiable within a limited set of users, called the anonymity set [36]. An individual carries out a transaction anonymously, if she cannot be distinguished by an observer from others. The observer, often also called the adversary, may obtain some additional information [10]. This means that the observer captures probabilistic information about the likelihood of different subjects having carried out a given transaction. The observing party may be the service provider or some other party with observation capabilities or with the ability to actively manipulate messages. Depending on the observers capabilities different models can be constructed with varying degrees of anonymity for the given anonymity set. Exactly what degree of anonymity is sufficient in a given context is dependent on legal and social consequences of a data breach and is an open question [10].

The capabilities of anonymizers are not only limited by the size of the anonymity set and the powers of the observer but also by the content of the communication. If the communication content includes personally identifiable information, then the communication partners can re-identify the source person. Worse, if the communication content is unencrypted then intermediary observers may also re-identify persons (or institutions) as was shown by Dan Egerstad¹⁰. A last dimension of weaknesses depends on the persistence of communication, meaning after observing multiple rounds of communication, the degree of anonymity may decrease and (probabilistic) re-identification becomes possible.

In databases, the conditions for establishing anonymity sets are somewhat different. The end of the 90s saw the development of a new research field called privacy preserving data mining (PPDM). Initially focusing on databases of so-called "anonymized" personal data, early results showed that simple de-identification is not enough for anonymization. In her seminal work Sweeney [43] showed that she could re-identify 85% of the persons in anonymized hospital reports using the publicly available non-personal attributes i.e. gender, age and zip code. Sweeney proposed methods to achieve k -anonymity in databases: A database listing information about individuals offer k -anonymity protection, if the information contained for each person cannot be distinguished from $k - 1$ individuals whose information also appears in the database. Later work in the field proved k -anonymity itself is not enough to anonymize data sets [22, 25, 38, 12].

The results of PPDM research have shown that what counts as personal data can be broad. The attacks based on communication content have shown that anonymization without encryption can actually produce false perceptions of security, causing the revelation of data meant to be confidential. These results demand that the definition of personal data be expanded and hence privacy as confidentiality be reconsidered. The results also invoke important research questions about the usability and practicability of PETs and PPDM methods. We will come back to some of these issues later. For now, let us look at some of

¹⁰ In 2007 Dan Egerstad set up a number of TOR exit nodes (a popular anonymizer <http://www.torproject.org>) and sniffed over 100 passwords from traffic flowing through his nodes. The list included embassies and government institutions [34]

the assumptions that PETs make when defining confidentiality and anonymity as building blocks of privacy.

2.3 Anonymity and Confidentiality in the Internet: Assumptions of PETs

There are some basic assumptions of the privacy as confidentiality paradigm that inform the logic of PETs. These assumptions are often not made explicit in research papers on privacy technologies. These vary between technical and socio-technical assumptions. These can be listed as follows:

1. *There is no trust on the internet:* Here, the absence of trust refers to a number of things. First, users of the Internet can never be sure: if a communication has been established with the correct party; as the popular analogy states, if the partner they are communicating with is a dog, and if this dog/non-dog is receiving the sent messages; and if the message is received, whether those messages remain unchanged. Further, given an unprotected communication channel and unencrypted messages, there are no guarantees against eavesdropping into the communication. Last, once the communication has been established and message or data transfer has taken place, there are no guarantees that the transmitted data will not be distributed to further parties.
2. *Users are individually responsible for minimizing the collection and dissemination of their personal data:* By suggesting that through the use of PETs privacy can be enhanced or protected, an implicit claim is that personal data on the Internet originates from the users themselves. If the users want to protect their privacy then they have to protect their data individually. This is especially the case because, see assumption (1) there is no trust on the Internet.
3. *If they know your data, then they know you:* although this is not necessarily stated in computer science papers, when discussing the effects of data collection in privacy discourses knowing data about individuals gets mixed up with knowing those individuals. Knowing a user or individual here refers to knowing some or all of the following: intentions, causalities, and reached objectives.¹¹
4. *Collection and processing of personal data, if used against individuals, will have a chilling effect:* The personally identifiable data distributed on the Internet may be used against individuals in unwanted and unclaimed ways. Especially if we make the assumption (3) if they know your data, they know you, then it follows that massive collection of data may have severe consequences. Misuse of personal data in repressive, discriminating, or simply

¹¹ There are numerous court cases in which digital data are used as evidence in ways which claim much more than the data seems at face value to represent. For example, a court in the U.S.A. accepted pictures from a social network site of a young woman enjoying a party a number of weeks after a car accident with casualties. The picture was used as proof that she lacked remorse [46]

undesirable ways may have a chilling effect. Hence keeping personal data confidential is a secure way to avoid such chilling effects.

5. *Technical solutions should be used to protect privacy instead of relying solely on legal measures:* Data may leak legally or illegally since it is difficult to control data and (1) there is no trust on the Internet. In order to avoid such leakage of data despite legal protection technical solutions like anonymity and confidentiality should be preferred.

We would like to argue that all these assumptions, although coherent and strong in their arguments, are techno-centric. In order to show in which ways this is the case, we will look at some of the findings of surveillance studies authors with respect to life in the surveillance society. When appropriate, we will list critiques of PETs based on the privacy as confidentiality paradigm. In Section 4 we will return to these assumptions.

3 Surveillance society and PETs

In the following, we would like to give a short overview of some of the voices that we identify as the surveillance studies¹² perspectives. Each of the perspectives investigate surveillance spaces and their affects in our lives and on our understanding of privacy. We would like to use these perspectives to reconsider the assumptions around PETs that we listed above. We sum up the different perspectives in the daily, marketing, political, performative and information perspectives. We will shortly account for each of these perspectives and their critique of PETs.

3.1 The Daily Perspective on Surveillance

A typical critique of users is that they do not care for their privacy. Even though different types of PETs are available to them, and in different studies users express their concerns for the privacy of their data, when they do make use of systems, these concerns evaporate and PETs are rarely utilized [4]. This low adoption of PETs has been contributed to the usability problems that are associated with PETs. Studies like "Why Johnny can't encrypt?" have argued exactly for this point [51]. In other cases, the users have been accused of being insensitive to the abuse of their data, naive, or simply ignorant of the risks that they are taking [18].

¹² Surveillance studies is a cross-disciplinary initiative to understand the rapidly increasing ways in which personal details are collected, stored, transmitted, checked, and used as means of influencing and managing people and populations [27]. Surveillance is seen as one of the defining features that define and constitute modernity. In that sense, surveillance is seen as an ambiguous tool that may be feared for its power but also for its potential to protect and enhance life chances. Departing from paranoid perspectives on surveillance, the objective of these studies is to critically understand the implications of current day surveillance on power relations, security and social justice.

In a short article Felix Stalder argues otherwise [42]. He states that our societies are increasingly organized as networks underpinned by digital information and communication technologies. He claims:

”In a network, however, the characteristics of each node are determined primarily by its connections, rather than its intrinsic properties, Hence isolation is an undesirable option.”

As an example of the networked society, Stalder talks about how when going to the social services, we have to show information about housing and work, while at work we have to give bank information, which provides us with a credit car, which is a precondition to renting a car, etc. Therefore, it is the connectedness that provides individuals with access to various systems rather than their relationship one-by-one with these institutions.

Therewith, Stalder problematizes PETs that make use of anonymity or even unlinkable pseudonyms for daily encounters¹³. Wide spread use of anonymity and unlinkable pseudonymity tools burdens the individuals, more so than offering them tools of protection. Instead, Stalder argues that the burden to protect their privacy should be taken off the individual’s shoulders and accountability should be asked of database holders.

3.2 The Marketing Perspective on Surveillance

One of the main concerns with the collection of personal data is that of categorization. A typical example of discriminatory categorization is the use of geodemographic systems, which have been critiqued in previous studies [8, 17]. Therewith, marketers and companies can decide on desirable and non-desirable customers, excluding parts of the population. The latter are no exceptions to existing economic models and are often called the *dead weight loss* [2].

Anonymity offers little protection against these systems. The classification of individuals with respect to marketing categories (or for that matter governmental surveillance categories for crime suspects) is not necessarily based on the unique identity of persons but rather on attributes that they carry. In that sense, these systems continue to work even if the individuals using the systems are anonymized. What is important for these systems are behavioral characteristics and user attributes. A newcomer to the system does not have to be identified uniquely, it is enough if their behavior can be matched given a set of categories.

Exactly this critique is picked up and taken a step further by Zwick and Dholakia, marketing specialists critical of existing geodemographic systems and consumer databases [53]. Zwick states that the control of the consumer to determine his digital identity is minimal. Because, Zwick claims:

¹³ Unlinkable pseudonyms refer to systems in which users identify themselves with different pseudonyms for different sets of transactions. For an observer it should not be possible to identify if two pseudonyms are coming from the same user. If implemented in an infrastructure with a trusted third party distributing the pseudonyms, then these can be revoked, ideally only under certain (legally defined) conditions.

”Implicit in the conceptualization of all of these tactics is the assumption that the consumer self is ontologically distinct from its representation in the electronic market-space. Yet, from a poststructuralist perspective, the subject cannot be conceived in this way. Because the consumer is constituted by language and the language governing the electronic market space is constituted by databases. The consumer (as a meaningful cultural representation, not as a body) does not exist outside this constitutive field of discursive power. Hence, the consumers digital identity is his or her real identity because marketing is targeted toward the consumer profile rather than the real person.”

The authors suggest that knowledge is a function of linguistic power and linguistic power in the mode of information resides with database technologies. Hence, very much like Stalder the authors propose that a struggle for consumer identity needs to be fought at the level of the database.

The authors’ critique of PETs is severe. They claim that PETs offer ”customers” only a false perception of autonomy. The consumer categories cannot be manipulated. Indeed, as an alternative the authors argue that consumers must be given direct access to customer databases in order to ensure that he or she regains a viable voice in the act of his or her constitution as a customer. The customer has to be enabled in (co)authoring their own identity.

3.3 The Political Perspective on Surveillance

Within the privacy as confidentiality approach, there is an assumption that the protection of those issues, activities, opinions deemed to be private and the private sphere is ultimately a good thing. David Phillips produces a critique of this normative approach based on feminist and queer theory. He says that:

”Some feminist scholars have argued that it is this creation of a private, domestic sphere apart from the public realm, that is the privacy problem. Certain populations and issues are relegated to this private sphere, particularly women and issues of sexuality. The public/private distinction then serves as a tool of social silencing and repression. From this perspective, the most important privacy issues are not those of freedom from intrusion into the domestic realm, but instead of the social construction of the public/private divide itself.”

If we take a look at newspaper headlines in mainstream media on possible privacy breaches that are articulated in mainstream media with respect to new technologies then Phillips pointer becomes even more interesting. More often than not, these articles are about: drinking and drug habits or sexual preferences being visible to future employers(social networks), bodies becoming visible publicly (the airport scanners), severe illnesses or dissident opinions becoming available to public, etc. We are not arguing that all these things should be public and considering them private is always a matter of repression. But privacy is not uniformly available and uniformly valued. The need for privacy can change

depending on context, as in the case of abuse or violence in the private sphere. For those who have little public power, the apparent invasion of privacy can sometimes seem welcome [28].¹⁴

It is important to recognize that through new technologies and their ability to make things visible and invisible we are forced to re-consider what should remain public and private. This needs to be a social and democratic process and not one defined solely by experts. As expected, in a good number of cases, the suggestions for making issues private are not and will not be devoid of other political messages that may or may not be related to technology. Hence, instead of inscribing into systems absolute values of what should remain private, systems that allow users to negotiate when and if they want to keep their information private and public should be considered. From the political perspective, it is therefore advisable to build technologies that enable individuals or communities to safely push the boundaries between the public and the private.

3.4 The Performative Perspective on Surveillance

The effectiveness of performativity in surveillance space becomes easily evident in the interventions of Stephen Mann. In his series of performances "My Manager" Mann wears a visible camera in stores and restaurants where photography is not permitted by customers, yet where CCTV surveillance is practiced. When approached by security staff, Mann tells them that "my manager" insists he wears the camera to ensure that he is not wasting his time during his errands. This is not photography he explains, since the signals are being beamed off-site where they will be turned into images [28]. Mann blames everything on "My Manager" and watches to see how the power relationships shift, how not taking responsibility for surveillance becomes ridiculous, and managers do all of a sudden appear to question his intervention.

McGrath in his book "Loving Big Brother" very much appreciates the wit and passion of such daily performative interventions. His analysis of surveillance space avoids a value judgement about the morality or desirability of surveillance technology per se. He adds that his objective is to:

"[to] examine ways in which new understandings of surveillance, and particularly spatial understandings, can help us live creatively and productively in post-private society. However, it has also been clear throughout [this book] that the predominant ideologies of surveillance need to be actively and complexly challenged and deconstructed if this is to be achieved."

¹⁴ There are cases, where this is exactly turned around as in the case of Federal Record Keeping and Labeling Requirements which require secondary producers to be responsible for the record keeping procedures primary producers gather when they produce pornography [31] where the lack of public power also leads to both an intrusion of the effected person's privacy and to silencing. So, the argument is not that the private is always repressive and the public intervention is always a positive one, but that the both the private and public needs to be negotiable and questionable, especially when the lives of those with meager public power are disputed.

As a strategy, McGrath demands a shift from anti-surveillance to counter-surveillance. He points to the impossibility of controlling surveillance space itself i.e. once surveillance space exists, it can be used in many unexpected ways by unexpected parties. In that, he accepts that there can be no trust on the Internet but derives different conclusions. Although performances like Mann's, or the use of cameras at demonstrations against police brutality [24], or even the case of Rodney King in the U.S.A [3] are valuable examples of reversing the gaze, McGrath focuses on counter-surveillance that goes beyond the reversal strategy. Instead, he proposes counter-surveillance that opens a space for all sorts of reversals in relation to how the gaze and its imagery may be experienced.

McGrath argues that proliferation of surveillance will produce discontinuities in experience of surveillance and produce excess. The more the surveillance proliferates, and the more surveillances start competing, McGrath argues the more we will see a battle over meaning. If we accept that surveillance space is in suspense, that the way we will take up surveillance, the way we will be affected, and the way we will respond are in suspense, then radical possibilities for counter-surveillance pop-up. And, he argues that the focus of these counter-surveillance strategies should be on deconstructing and subverting the tyranny of meaning given to surveillance material.

But, how? McGrath picks up on the theories of the poststructuralist Mark Poster, who states that: "we are already surrounded by our data bodies in surveillance space." He gives examples of artists' works and everyday surveillance uses that highlight the discontinuities of the surveillance narrative. It follows from the examples that these data bodies are neither simple representations of ourselves, nor straight falsifications, but hybrid versions of ourselves susceptible to our interventions. McGrath is aware that this multiplicity of selves will be distorted and exploited by the consumer-corporate system. But, he concludes, that the real danger lies in disengaging with the surveillance space.

[T]he emergence of surveillance culture is nothing less than a challenge to our consciousnesses. [...] we ignore the circulating, multiple, hybrid versions of ourselves at our peril. if we deny their relation to us in an attempt to maintain the integrity of a unified self - rooted in rights of privacy - we risk surrendering any control, any agency, in relation to our lives and society.

According to these arguments, recent forms of practiced surveillance like reality shows e.g., Big Brother, and even most articulations of web based social networks can be seen as a realization of the fact that we live in a surveillance saturated society, and participation in these programs and environments are actually ways in which we are exploring what to do about it. In that sense, McGrath questions any assumptions on surveillance data being representative for what people are, feel, intend, or achieve, etc. Instead, he encourages members of our society to enter surveillance space, to experience its effects and to challenge any narratives that are limited to those of control and authority or try to monopolize what data means and how it can be used.

3.5 The Information Perspective on Surveillance

In most surveillance systems data receives meaning because of their relationality. A single piece of data about a single person says very little unless there is a set of data to compare it to, a framework to give it some meaning. In the age of statistical systems, the collection of data sets is what makes it possible to make inferences on populations and to evolve undesirable categorizations. This is also what Phillips defines as surveillance:

”Surveillance is the creation and managing of social knowledge about population groups. This kind of privacy can easily be violated if individual observations are collated and used for statistical classification, which applied to individuals makes statements about their (non)compliance with norms, their belonging to groups with given properties and valuations, etc.”

In that sense any data, by its potential to be aggregated, has many data subjects, or better said always carries the potential of pointing to a data population. Individual decision making on personal data always effects all correlated subjects [40]. Individualized concealment of data or unlinking of identities from traces provides little or no protection against breaches based on statistical inferences or discriminatory categorization for all correlated data subjects. Any individual can be categorized, as long as enough information has been revealed by others and aggregated in databases. The other way around, it is impossible to guarantee semantic security in statistical databases. Meaning it cannot be guaranteed that access to a statistical database would not enable one to learn anything about an individual that could not be learned without access [13]. Hence, not only is categorization a problem, but also analysis of statistical databases could reveal information about individuals.

Further, much information is revealed about individuals by virtue of their associations with others. By now, we all carry digital devices that accumulate data about our environments, as well as providing information about us to those environments. We disseminate this information on the social web or simply among our little ecology of devices. We talk loudly on our cell phones about ourselves and others, reveal pictures of family, friends or visited locations, archive years worth of emails on multiple backup devices from hundreds of persons, map out our social networks which reveals information about all those in the network. In each of these cases it is evident that it is not only individuals that reveal information about themselves, but we all participate in multiple kinds of horizontal and vertical information broadcasts and surveillances. We collectively produce data: we produce collaborative documents on wikis, take part in online discussions and mailing lists, comment each others pictures etc. All of this data is relational and makes sense in its collectivity. It also works the other way, in the networked world that Stalder describes, much information is collected about us and is linked in order to give us access to systems.

Hence, looking at data as snippets of individual contributions to digital systems actually misses the actual value of that data in its collectivity and relation-

ality. It does not recognize the publics we create and share, one of the greatest promises of the Internet. Individualizing participation in the surveillance society makes it difficult to develop collective counter-surveillance strategies, and limits our engagements with surveillance systems to individual protections of our actions.

The depiction of information privacy and data protection analogous to individual property rights actually exacerbates the problem of a contested public sphere. Although the rise of the social web can be celebrated as a long expected gift or cooking pot economy, not only its privatization through large companies, but also the privacy debates contribute to articulations against seeing information on the web as a public good¹⁵ The logic of privacy and private ownership has created the false perception that data in its singularity is of outmost value and is controllable. Privacy through confidentiality and anonymity can follow this logic and can be detrimental to collective critical engagement in surveillance systems.

4 Returning to the assumptions of PETs

Personal data is an undefined category that is widening ever since PPDM has introduced the concept of quasi identifiers. This means that practically all data are always potentially linkable to an individual and hence are personal data. And in the logic of privacy as confidentiality, any data may reveal something about the individual, and hence needs to be kept private. In the different surveillance perspectives, the authors discuss how this is inconvenient, undesirable, and sometimes impossible. Let us return to the assumptions of PETs using the prior critiques:

1. *There is no trust on the Internet:* This is a technical fact. Especially the underlying design of the Internet makes it very difficult to give guarantees of the security of communication. The problem here is that the absence of technical measures to make certain guarantees gets conflated with social definitions of trust. Exactly what social definitions of trust may be and how these categories get conflated is beyond the scope of this paper. In the rest of the paper we would like to take a closer look at the rest of the assumptions listed. In order to do that, we first review a set of critiques from a surveillance perspective in the next section.
2. *Users are individually responsible for minimizing the collection and dissemination of their personal data:* As we argued in the information perspective to surveillance, the protection offered through the confidentiality of personal data is limited. Anonymously collected data does not protect against surveillance systems and the reflexes of their controllers to manage and sort

¹⁵ It is therefore no surprise that in the latest uproar against the new Terms of Use of Facebook users have argued for a radical deletion of their profile to include the deletion of all their contributions to other profiles and all their correspondences to other people. The protection of individual privacy in such instances is valued over the integrity of the discussions forums, mailboxes of friends, posted photographs etc.

populations. Categories created through the databases using de-identified data can easily be used to classify individuals by virtue of mapping some of their attributes to categorical descriptions. The effectivity of these categories depends on the power of those holding this data and their success in making constitutive claims. Therefore, assuming keeping personally identifiable data confidential or unlinking individuals identities from their data traces may protect individuals from social sorting and marketing systems that are based on inferring categories from attributes does not hold as long as the power of those data controllers are not questioned.

3. *If they know your data, then they know you:* Surveillance data is often a place holder. It points to something that has happened or that has been, it often loses a sense of sender and receiver. Data loses the intentions behind its creation and starts to float in digital systems as data bodies. We need to dismantle the power of such data to stand for some "reality" or "truth". We need to scrutinize the uses of this data and deconstruct attempts to monopolize its meaning. When accountability is of concern, other technical mechanisms should be put into place that guarantee the necessary proofs that a certain data validly stands for something. But we should be careful to claim truth to data in order to argue for confidentiality as privacy protection.
4. *Collection and processing of personal data, if used against individuals, will have a chilling effect:* It is true that collection and processing of data, if used against individuals can have a chilling effect. McGrath shows in most of his examples that there could also be other effects. By now, there are multiple occurrences in which people have publicized data in order to protect themselves against the breach of their privacy ¹⁶. In a surveillance world confidentiality and anonymity can actually make somebody suspect or devoid of protection.
5. *Technical solutions should be used to protect privacy instead of relying solely on legal measures:* Given the amount of surveillance measures that have been installed and the amount of information collected about each person by their friends and organizations they are affiliated with, it is unrealistic to expect that technical measures can be applied realistically to actually keep many of daily interactions confidential. Hence, we must search for a combination of all three, technological solutions, legal protections and social practices to respect those activities that we would like protected. A solely techno-centric approach is unrealistic, is bound to overwhelm any individual, and often too quick to dismiss many social contracts that we enjoy in everyday life.

¹⁶ Anne Roth started a blog in which she documented their everyday activities after her partner was declared the number one terrorist in Germany in 2007 and they found out that their family had been subject to police surveillance for over a year (<http://annalist.noblogs.org/>). Similarly, New Jersey artist Hasan Elahi started documenting every minute of his life on the Internet after he was detained by the FBI at an airport (<http://trackingtransience.net/>). Both of these persons made the assumption that keeping their lives public protects their freedoms when their data is used against them.

5 Revisiting PETs:

Although we have shown that many of the assumptions underlying PETs is problematic, we still see an important value in the opportunities they have at offer. Especially given their vulnerable position as a result of politics of hypersecurity – based on another assumption, that only criminals and people who have something to hide use PETs– it is necessary to be precise with our critique. The human-centricity in the surveillance perspectives sketched above is that they tend to dismiss the ability of PETs to have alternatives and multiple (unexpected) affects. The solutions suggested by the different perspectives also delegates the problems often to the social: in the form of accountability, performativity and liability. We would like to explore the potential constitutive role that PETs play or can play in the surveillance society. Hence, we revisit PETs from each of the surveillance perspectives that we have summarized above in order to explore both, their potentials as well as their limitations.

We agree that putting the responsibility of re-establishing privacy should not solely lie on individuals. It is paradoxical to suggest that the solution to potential undesirable instances of control should lie in users having to control their actions and data all the time. Therefore visions of large scale anonymous or pseudonymous systems where users constantly hide their attributes and connections [7] and have to re-establish other forms of relatedness through digital reputation [11] are inconvenient and undesirable in a networked world.

Nevertheless, disabling the users' options to exercise some control over revealing their personal data if they want to is just as undesirable. We would hence argue that the accountability that Stalder demands of data processing systems should also include services for anonymous and/or pseudonymous users. The networked society should continue to offer access to those who do not want to be so engrained in the existing networks i.e., not being very well networked should not lead to individuals being excluded from services. Therefore, PETs that enhance privacy through anonymity and confidentiality –or where better suitable unlinkable pseudonyms– should be integrated where possible. Nevertheless, their mere existence should not be enough to relieve data controllers and processors of their responsibilities and accountabilities. This should also have a legal effect: we should reconsider if it is desirable, and, if so, how anonymized data can also be legally protected?

We very much agree with the critique of Zwick and Dholakia with respect to the constitutive force of these marketing databases. PETs, and more specifically anonymizers, as long as they do not hide user behavior, do not protect against the categorization discriminations based on marketing databases. Further, if we accept that categories of desirable and undesirable customers are constituted by the owners of those databases, then even hiding behavioral data may not protect against such constitutive forces. Hence, suggesting PETs can protect the privacy of individuals against aggressive marketing databases goes beyond burdening individuals, but actually produces a false perception of autonomy, and maybe even an illusion of control: if my data is important to me, then I can

protect it, if I want to give away my data for a utility, I can do so. Such utility arguments are not an option in existing databases with categorization powers.

Further, Zwicks and Dholakia's proposal for customer agency is limited to the engagement of the "customer" with the database. Their suggestions are to allow individuals to correct their profiles, which may go as far as deleting oneself from the marketing databases. But in a networked world, as Stalder argues, deletion will often not be an option. Never mind the technical problem of guaranteeing that all traces of data are deleted. In that sense, although their critique of PETs is substantial, by resurrecting a notion that they call "sense of autonomy" based on access and control of individual database entries, the authors re-install a false sense of autonomy.

Instead, agency with respect to databases maybe found in making visible the established relationality of data. Phillips states that the only thing that remains private in current surveillance systems are the methods through which these discriminatory classifications are created and used. By that he refers to the databases and algorithms used for data mining in those databases. It is through engagement with surveillance methods that it is possible to actually determine possible discriminations as well as desirable effects. It is also then possible to understand what through the aggregation of individual revelations of information becomes known to a specific public e.g. government, marketers. Such transparency practices could also demystify the effects of data collection and processing. Ideally, we can then actually collectively as societies or communities discuss if and how desirable the newly created private or public spaces are.

Significant is also the role PETs can play in the negotiation of the public and private. Tools such as anonymizers and anonymous publication services may allow users to challenge boundaries between the private and public. Anonymous speech has always been an important tool in democracies and an extremely helpful tool in repressive regimes. Nevertheless, the ultimate goal is not to limit the articulation of such opinions to anonymized spaces, but to make it possible to state such opinions in public and to safely hold public discourse on issues that are repressed. In that sense, PETs are not normative tools for how we should ultimately communicate if we want to have privacy, but can play an indispensable role in negotiating the public and private divide.

For McGrath engagement with surveillance is key rather than re-establishing privacy and public assembly absolutes within a relativistic culture. Instead, he suggests that: ownership of imagery and data selves; freedom of image and data circulation; the multiplicity and discontinuities of data experience; and, the emotional instability of security systems should be the center of our focus. Therefore, in a first impression we can conclude that PETs can rather be categorized as anti-surveillance strategies. But, given their recent popularity to circumvent repressive governments i.e. as a way to reach Internet sites that have been blocked by governments, there may be more value in those tools than visible at first sight.

6 Conclusion:

We have argued in the last section that despite the problems with the assumptions underlying PETs, and despite the legitimate critiques articulated in the surveillance perspectives, PETs can and should be part of privacy research. The more we engage in surveillance space, the more we will find diverse uses for PETs. But, it was one of our objectives in writing this paper to give legitimacy to multiple approaches to "privacy design" in computer science. We are especially interested in those approaches that do not work solely with the privacy as confidentiality paradigm, and are able to mesh techno-centric and human-centric perspectives as constitutive others. We believe that a broader vision of privacy and a deeper understanding of surveillance could help both users and computer scientists to develop systems that support multiple kinds of privacies and data protection practices. For all of this, it is clear that an interdisciplinary approach is imminent.

In the past years, other approaches to privacy in computer science have started flourishing. Two of these can be shortly listed as follows:

- *privacy as control*: A wider notion of privacy, appearing in many legal codifications, defines the term not only as a matter of concealment of personal information, but also as the ability to control what happens with it. This idea is expressed in Westins [50] definition of (data) privacy: the right of the individual to decide what information about himself should be communicated to others and under what circumstances and in the term "informational self-determination" first used in a German constitutional ruling relating to personal information collected during the 1983 census [6]. Some examples of research in this area are accounted for under the title of identity management systems and trust based systems with (sticky) privacy policies. These approaches often rely on and make use of data protection legislation as well as technical mechanisms. This approach is hence valuable for improving accountability of information systems, a point emphasized in the different surveillance studies perspectives. These mechanisms also are based on the building stones offered by the techniques developed in the privacy as confidentiality paradigm, but are not limited to it.
- *privacy as practice*: It can help users immensely to know what data exists about them, to understand how it travels, and to comprehend ways of improving privacy practices in the future. The users can then either request for changes to be made to existing data, which is the idea of information self-determination, or reconfigure their settings and change their interactions to strategically reveal or conceal data in the future. There is little but valuable research done on systems that support users strategic revelation and concealment based on what is already known. Palen and Dourish argue that "privacy management in everyday life involves combinations of social and technical arrangements that reflect, reproduce and engender social expectations, guide the interpretability of action, and evolve as both technologies and social practices change" [33]. Following the same lines of

thought, Lederer et al.[23] suggest improving privacy sensitivity in systems through feedback that improves users' understanding of the privacy implications of their system use. They add that this can then be coupled with control mechanisms that allow users to conduct socially meaningful actions through them. Concretely the authors suggest the use of mechanisms like the identityMirror [26]. A similar approach is suggested in the concept of privacy mirrors [29]. Hansen [21] suggests combining such features with identity management mechanisms that implement privacy as control.

In order to make any privacy related guarantees, regardless of the approaches taken, the system developers will have to secure the underlying systems. Hence, the three approaches: privacy as confidentiality, control, and practice are not only complimentary to each other, but also depend on the security of the underlying infrastructures.

Last but not least, there is a need to consider other approaches to data then just personal data. We have explained in Section 3.5 the importance of the relationality of information. If we accept that data are relational, then we have to reconsider what it means to think about data protection. For legal frameworks this is the challenge of dealing with data that is co-created by many, that has multiple data subjects, or that is controlled by many. For computer scientists, it requires thinking of collaborative tools, anywhere from new forms of access control to methods for negotiating the visibility, availability and integrity of data owned and shared by many.

In this paper, we have shown some of the problems that arise with the privacy as confidentiality approach in a surveillance society. We have done this by studying how PETs based on data confidentiality and anonymity function, what techno-centric assumptions they rely on, and how these assumptions can be shaken by our surveillance realities. We have used surveillance perspectives to review the assumptions underlying PETs. We then returned to the surveillance perspectives to step out of some of their human-centric assumptions. In doing that we explored the potentials and limitations of PETs in a surveillance society. Last, we sketched two other approaches to privacy in computer science and pointed out the importance of understanding the relationality of data in statistical systems and our networked world. We believe it is through the combination of all three approaches: privacy as confidentiality, privacy as control and privacy as practice, that we can both: recognize users abilities, witt and frustrations in navigating in the surveillance world; and, develop critical and creative designs with respect to privacy.

7 Acknowledgements

This work was supported in part by the Concerted Research Action (GOA) Ambiorics 2005/11 of the Flemish Government, by the IAP Programme P6/26 BCRYPT of the Belgian State (Belgian Science Policy), and by the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n 216287 (TAS³ -

Trusted Architecture for Securely Shared Services).¹⁷ The authors also wish to thank Carmela Troncoso, Claudia Diaz, Nathalie Trussart, Andreas Pfitzmann, Brendan van Alsenoy, Sarah Bracke, Manu Luksch and Aaron K. Martin for their valuable and critical comments.

References

1. J. D. Babcock. A brief description of privacy measures in the rush time-sharing system. In *AFIPS '67 (Spring): Proceedings of the April 18-20, 1967, spring joint computer conference*, pages 301–302, 1967.
2. Matthias Bauer, Benjamin Fabian, Matthias Fischmann, and Seda Gürses. Emerging markets for RFID traces. <http://arxiv.org/abs/cs.CY/0606018>, 2006.
3. BBC. Flashback: Rodney king and the LA riots. Online, 10. July 2002.
4. Bettina Berendt, Oliver Günther, and Sarah Spiekermann. Privacy in e-commerce: stated preferences vs. actual behavior. *Communications of the ACM*, 2005.
5. Sandra Braman. Tactical memory: The politics of openness in the construction of memory. *First Monday*, 11(7), 2006.
6. Bundesverfassungsgericht. BVerfGE 65, 1 – Volkszählung. Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden, 1983.
7. David Chaum. Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, 1985.
8. Michael R. Curry and David Phillips. Surveillance as social sorting: Privacy, risk, and automated discrimination. In David Lyon, editor, *Privacy and the phenetic urge: geodemographics and the changing spatiality of local practice*. London: Routledge, 2003.
9. George Cybenko. A critical need, an ambitious mission, a new magazine. *IEEE Security and Privacy*, 1(1), 2003.
10. Claudia Diaz. *Anonymity and Privacy in Electronic Services*. Katholieke Universiteit Leuven, 2005.
11. Roger Dingledine, Nick Mathewson, and Paul Syverson. Reputation in privacy enhancing technologies. In *CFP '02: Proceedings of the 12th annual conference on Computers, freedom and privacy*, 2002.
12. J. Domingo-Ferrer and V. Torra. A critique of k-anonymity and some of its enhancements. In *Third International Conference on Availability, Reliability and Security, 2008. ARES 08.*, 2008.
13. Cynthia Dwork:. Differential privacy. In *ICALP (2)*, pages 1–12, 2006.
14. EU. Directive 95/46/ec of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities*, page 31, November 1995.

¹⁷ The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

15. Cornelius E. Gallagher. The computer and the invasion of privacy. In *SIGCPR '67: Proceedings of the fifth SIGCPR conference on Computer personnel research*, pages 108–114, 1967.
16. Edward L. Glaser. A brief description of privacy measures in the multics operating system. In *AFIPS '67 (Spring): Proceedings of the April 18-20, 1967, spring joint computer conference*, pages 303 – 304, 1967.
17. Stephen Graham. Software-sorted geographies. *Progress in Human Geography*, 29(5), 2005.
18. Ralph Gross and Alessandro Acquisti. Information revelation and privacy in online social networks. In *WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pages 71–80, 2005.
19. Paolo Guarda and Nicola Zannone. Towards the development of privacy-aware systems. *Information and Software Technology*, 51(2):337 – 350, 2009.
20. Serge Gutwirth. *Privacy and the Information Age*. Rowman and Littlefield Publishers, 2002.
21. Marit Hansen. Linkage control - integrating the essence of privacy protection into identity management. In *eChallenges*, 2008.
22. Daniel Kifer and Johannes Gehrke. l-diversity: Privacy beyond k-anonymity. In *IEEE 22nd International Conference on Data Engineering (ICDE'07)*, 2006.
23. Scott Lederer, Jason I. Hong, Anind K. Dey, and James A. Landay. Personal privacy through understanding and personal privacy through understanding and action: Five pitfalls for designers. In *Personal Ubiquitous Computing*, volume 8, pages 440–454, 2004.
24. Paul Lewis. Video reveals G20 police assault on man who died. *The Guardian*, 7. April 2009.
25. Ninghui Li and Tiancheng Li. t-closeness: Privacy beyond k-anonymity and -diversity. In *IEEE 23rd International Conference on Data Engineering (ICDE'07)*, 2007.
26. Hugo Liu, Pattie Maes, and Glorianna Davenport. Unraveling the taste fabric of social networks. *International Journal on Semantic Web and Information Systems*, 2(1):42 – 71, 2006.
27. David Lyon. Editorial. Surveillance Studies: Understanding visibility, mobility and the phenetic fix. *Surveillance and Society*, 1(1), 2002.
28. John McGrath. *Loving Big Brother: Performance, Privacy and Surveillance Space*. Routledge: London, 2004.
29. David H. Nguyen. Privacy mirrors: Understanding and shaping socio-technical ubiquitous computing. Technical Report, 2002.
30. Helen Nissenbaum. Privacy as contextual integrity. *Washington Law Review*, 79(1), 2004.
31. Department of Justice. 28 cfr part 75 revised regulations for records relating to visual depictions of sexually explicit conduct; inspection of records relating to depiction of simulated sexually explicit performance; final rule. *Federal Register*, 73(244), 2008.
32. Wanda J. Orlikowski. Sociomaterial practices: Exploring technology at work. *Organization Studies*, 28, 2007.
33. Leysia Palen and Paul Dourish. Unpacking "privacy" for a networked world. In *CHI '03: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 129 – 136, 2003.
34. Ryan Paul. Security expert used tor to collect government e-mail passwords. *Ars Technica*, September 2007.

35. H. E. Petersen and R. Turn. System implications of information privacy. In *AFIPS '67 (Spring): Proceedings of the April 18-20, 1967, spring joint computer conference*, pages 291–300, 1967.
36. Andreas Pfitzmann and Marit Hansen. Anonymity, unobservability, and pseudonymity: A consolidated proposal for terminology. Technical report, Technical University, Dresden, 2008.
37. David J. Phillips. Privacy policy and PETs. *New Media and Society*, 6(6):691–706, 2004.
38. David Rebollo-Monedero, Jordi Forné, and Josep Domingo-Ferrer. From t-closeness to pram and noise addition via information theory. In *PSD '08: Proceedings of the UNESCO Chair in data privacy international conference on Privacy in Statistical Databases*, 2008.
39. IEEE Computer Society Press Room. Computer society history committee names top 60 events (1946-2006). IEEE Website, 2007.
40. Antoinette Rouvroy. Technology, virtuality and utopia. In *Reading Panel on Autonomic Computing, Human Identity and Legal Subjectivity – Legal Philosophers meet Philosophers of Technology, CPDP 2009*, 2009.
41. Daniel J. Solove. A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), January 2006.
42. Felix Stalder. The voiding of privacy. *Sociological Research Online*, 7(2), 2002.
43. Latanya Sweeney. k-anonymity: a model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10(5):557–570, 2002.
44. Herman T. Tavani and James H. Moor. Privacy protection, control of information, and privacy-enhancing technologies. *SIGCAS Comput. Soc.*, 31(1):6–11, 2001.
45. James P. Titus. Security and privacy. *Communications of the ACM*, 10(6), 1967.
46. Evan Wagstaff. Court case decision reveals dangers of networking sites. Daily Nexus News, February 2007.
47. Yang Wang and Alfred Kobsa. Privacy Enhancing Technologies. In M. Gupta and R. Sharman, editors, *Handbook of Research on Social and Organizational Liabilities in Information Security*. Hershey, PA: IGI Global, 2006.
48. Willis H. Ware. Security and privacy in computer systems. In *AFIPS '67 (Spring): Proceedings of the April 18-20, 1967, spring joint computer conference*, pages 279–282, 1967.
49. Willis H. Ware. Security and privacy: similarities and differences. In *AFIPS '67 (Spring): Proceedings of the April 18-20, 1967, spring joint computer conference*, pages 287–290, 1967.
50. A. F. Westin. *Privacy and freedom*. Atheneum, 1970.
51. Alma Whitten and J.D. Tygar. Why johnny can't encrypt: a usability evaluation of pgp 5.0. In *SSYM'99: Proceedings of the 8th conference on USENIX Security Symposium*, 1999.
52. David Wills and Stuart Reeves. Facebook as a political weapon: Information in social networks. *British Politics*, 4(2):265 – 281, 2009.
53. Detlev Zwick and Nikhilesh Dholakia. Whose identity is it anyway? consumer representation in the age of database marketing. *Journal of MacroMarketing*, 2003.