Noname manuscript No.
(will be inserted by the editor)

PETs and their users.

Retelling a story in the surveillance society.

Received: date / Accepted: date

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 anonymity of data traces have resulted from such research. The objective of this paper is to show that PETs are indispensable but are short of being the privacy solutions they claim to be. Further, we will argue that the computer scientists conception of privacy through data confidentiality is data centric and displaces end-user perspectives and needs in a surveillance society. Last, we discuss alternative paradigms for privacy design.

Keywords privacy as confidentiality · privacy enhancing technologies · surveillance society

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.[Gallagher(1967)]

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 for introducing 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 he was a keynote speaker at the American Federation of Information Processing Societies' 1967 Spring Joint Computer Conference in New Jersey, USA [1] and consequently his words were echoed in the Communications of the ACM [Titus(1967)].

[1] The series of conferences commenced in 1961 and were dissolved in 1990 [Room(2007)]

Given that special historical constellation we can state that 1967 was the year in which privacy as a research topic was introduced to the field of computer science. [2] At the conference a session on privacy problems was introduced and a total of 5 papers were presented on the topic of privacy. [3]. Privacy was never defined in these papers but assumed to be confidentiality of data, the breach of privacy then meaning the leaking 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 [Gallagher(1967)], the transposition of the concept to research in computer science was limited to data confidentiality.

Research on privacy enhancing technologies that guarantee data confidentiality and hence user privacy have been an important research topic ever since [4]. This research has resulted in the development of various systems that have important functions for guaranteeing anonymous speech, secure communication and unlinkable electronic activities in a networked world.

The objective of this paper is to show that data confidentiality and anonymity, two important properties of privacy enhancing technologies, are indispensable but are short of being the privacy solutions they claim to be. Further, we will argue that the computer scientists conception of privacy through data confidentiality is data centric and displaces end-user perspectives and needs in a surveillance society. Last, we argue that we need to include approaches to privacy design that are also dependent on understanding user needs and information practices, legal approaches and changing conceptions of privacy.

Similar critique of PETs have been written in the past [Phillips(2004), Stalder(2002), Tavani and Moor(2001)]. This paper is valuable nevertheless for a number of reasons. First, confidentiality as the way to preserve privacy is a recurring theme in privacy debates generally and in computer science specifically. Second, although the authors of those papers make some important claims, we have some additional arguments which can be seen as new challenges to privacy research. Further, our argument is not that anonymity and confidentiality tools should be done away with but that its potentials and limitations for protecting privacy have to be explored again and again in a world of rapidly developing technology, ubiquitous surveillance, as well as changing perceptions, legislation and practices of privacy.

The paper is organized as follows. In Section 2 we give an overview of computer science research on privacy as confidentiality and anonymity. Here we also list some of the assumptions that go along with this kind of research. Next, in Section 3 we give accounts of different perspectives on surveillance society and their implications for thinking of privacy as confidentiality and for the use of PETs. We then return to the assumptions in Section 4. In the conclusion we then review PETs from a surveillance perspective and identify new challenges for privacy research.

---

[2] It is true that cryptography has a longer history and one could argue hence that privacy of messages pre-dates computer science. We in this paper start our account of privacy research, stated as such, with its first introduction at the Spring Joint Computer Conference.

[3] Three of the authors were from the RAND Corporation [Ware(1967a)][Petersen and Turn(1967)], one from M.I.T [Glaser(1967)] and one from a company named Allen-Babcock Computing [Babcock(1967)].

[4] 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 [Cybenko(2003)].

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 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 [Ware(1967a)]. 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 data and if this was unrealistic when a central authority and the necessary discipline was lacking in non-governmental/private computer networks [Ware(1967b)]. They 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. Hence, confidentiality, a concept that played an important role in military think was chosen as the main paradigm for privacy research.

Ever since there has been much progress in "non-military" contexts defining what should count as informational privacy [Gutwirth(2002), Solove(2006), Nissenbaum(2004)] 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 [EU(1995)], Art. 2 (a)).

Important for our purposes is the emphasis on identity, which is assumed to be unique for one natural person. 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 such. The standard types of personal data are profile data describing individuals, including name, address, health status, etc.

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. Much of the personal data collected using current day technologies represent activities of individuals in spheres assumed to be private prior to their digitization. Not digitizing these activities and avoiding the exchange of such digitized data would not change the state of the "private sphere" but this can limit the potentials of technology and are often not desirable 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 other 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 concerned with how public the traces consequently become. Anonymity is achieved by unlinking the identity of the person from the traces of his/her activities left in information systems.

In technical terms, this translates to a set of users with a certain size k, or shortly k-anonymity. With k-anonymity the traces k individuals leave behind when using information systems cannot be distinguished by an observing party – the observing party may be the service provider or some other party with observation capabilities. If k is small, it could cause a threat to those in the set thinking that they are anonymous. Given a significantly large set and the absence of an all-seeing observer, an acceptable degree of anonymity is achievable.

The capabilities of anonymizers are not only limited by the size of k 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 Egerstad [5].

The end of the 90s also saw the development of a new research field called privacy preserving data mining (PPDM). Initially focusing on databases of anonymized personal data, early results showed that simple de-identification is not enough for anonymization. In her seminal work Sweeney [Sweeney(2002)] 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. Later work in the field proved k-anonymity itself is not enough to anonymize data sets [Kifer and Gehrke(2006), Li and Li(2007), Rebollo-Monedero et al(2008)Rebollo-Monedero, Forné, and Domingo-Ferrer, Domingo-Ferrer and Torra(2008)].

The results of PPDM research have shown that what counts as personal data can be quite tricky. 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 these issues later. For now, let us look at some of the assumptions that PETs make when defining privacy as confidentiality and anonymity.

2.3 Anonymity and Confidentiality in the Internet: Assumptions of PETs

There are some basic assumptions of the privacy as confidentiality or anonymity paradigm that inform the logic of PETs. These assumptions are often not made explicit. 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

[5] 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 [Paul(2007)]

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 (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 [6].
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 that (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 undesirable ways may have a chilling effect. Hence keeping personally identifiable 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 data or techno-centric but not user centric. In order to argue that this is the case, we will look at some of the finding of surveillance studies authors with respect to life in the surveillance society. When appropriate, we will list critiques of PETs. Later 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 studies [7] perspectives. Each of the perspectives investigate

[6] 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 [Wagstaff(2007)]

[7] 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

surveillance spaces and their effects 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. The different perspectives can be summed up as follows:

- the daily perspective
- the marketing perspective
- the political perspective
- the performative perspective
- the information perspective

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 [Berendt et al(2005)Berendt, Günther, and Spiekermann]. 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 [Whitten and Tygar(1999)]. 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 [Gross et al(2005)Gross, Acquisti, and H. John Heinz].

In a short article Felix Stalder argues otherwise [Stalder(2002)]. 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 we need when 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 instituions.

Therewith, Stalder problematizes PETs that make use of anonymity or even unlinkable pseudonyms for daily encounters [8]. Wide spread use of anonymity and unlinkable pseudonymity tools burdens the individuals, more so then 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.

---

of influencing and managing people and populations [Lyon(2002)]. 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.

[8] Unlinkable pseudonyms refer to systems in which users identify themselves with different pseudonyms for different transactions. For an observer it should not be possible to identify if two pseudonyms are coming from the same user. The pseudonyms can be revoked ideally only under certain (legally defined) conditions.

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 numerous studies [Curry and Phillips(2003), Graham(2005)]. 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 [Bauer et al(2006)Bauer, Fabian, Fischmann, and Gürses].

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 based on the 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, 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 [Zwick and Dholakia(2003)]. Zwick states that the control of the consumer to determine his digital identity is minimal. Because, Zwick claims,

> "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."

Instead, by suggesting that knowledge is a function of linguistic power and linguistic power in the mode of information resides with database technologies, 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 [McGrath(2004)].

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, we need to conceive systems that allow users to negotiate when and if they want to keep their information private and public. We need 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 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 [McGrath(2004)]. 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."

As a strategy, McGrath demands a shift form 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[Lewis(2009)], or even the case of Rodney King in the U.S.A. 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.

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 un/desirable 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 [Rouvroy(2009)]. 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.

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. 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 relationality. 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, but also the privacy debates contribute to articulations against seeing information on the web as a public good [9] The logic of privacy and private ownership has created the false perception that data in its singularity is of 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 almost data are

[9] 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.

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. Using the different surveillance perspectives we have shown how this is inconvenient, undesirable, and 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 their reflexes to manage and control populations. Categories created through the databases using de-identified data can easily be linked to 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 such inferences and the systems that are based on these inferences is not correct.
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 looses a sense of sender and receiver. Data looses 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 [10]. In a surveillance world confidentiality and anonymity can actually make somebody suspect or devoid of protection.

[10] 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. *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 affilliated with, it is unrealistic to expect that technical measures can be applied realistically to actually keep many of daily interactions confidential. Hence, we must depend on legal protections and social practices to respect those activities that we would like protected. A technocentric approach is unrealistic, is bound to overwhelm any individual, and too quick to dismiss many social contracts that we enjoy in everyday life.

5 Revisiting PETs:

Although we have shown that much of the assumptions underlying PETs are 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 hyper-security – based on another assumption, that only criminals have the incentives to use such technologies– it is necessary to be precise with our critique. Hence, we need to revisit PETs for each of the surveillance perspectives that we have summarized above exploring 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 [Chaum(1985)] and have to re-establish other forms of relatedness through digital reputation [Dingledine et al(2002)Dingledine, Mathewson, and Syverson] 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 desirable. We would hence argue that the accountability that Stalder demands of data processing systems should also include services for anonymous 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.

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. There 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 the traces of data. In that sense, although their critique of PETs is substantial, the authors' solutions also do not move beyond a false perception 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 then 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 then 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. 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. These can be shortly listed as follows:

- *privacy as data protection:* 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 [Westin(1970)] denition 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 [Bundesverfassungsgericht(1983)]. 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. Let us call these legal-centric privacy design approaches. Such approaches are especially valuable for improving accountability of information systems.
- *privacy as practice:* It would help users immensely to know what data exists about them, to make clear how it travels, and 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" [Palen and Dourish(2003)]. Following the same lines of thought, Lederer et al.[Lederer et al(2004)Lederer, Hong, Dey, and Landay] 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 [Liu et al(2006)Liu, Maes, and Davenport]. A similar approach is suggested in the concept of privacy mirrors [Nguyen(2002)]. Hansen [Hansen(2008)] suggests combining such features with identity management mechanisms that implement privacy as data protection. It is interesting that for such tools we will need the expertise of data miners themselves, those most accused of contributing the privacy nightmare. Nevertheless, in this kind of research we think that it will be possible to develop user-centric privacy designs.

Last but not least, there is a need to consider other approaches to 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 belongs to many, gives information about many, and that is controlled by many. For computer scientists, it requires thinking of collaborative tools, anywhere from new forms of access control to methods of negotiating the visibility, availability and integrity of data owned and shared by many.

In this paper, we have shown the problems that arise with the privacy as confidentiality approach in a surveillance society. We have done this by understanding how PETs based on data confidentiality and anonymity function, what technical and socio-technical assumptions they rely on, and how these assumptions are shaken by our surveillance realities. We have then reviewed the assumptions underlying PETs and revisited their potentials and limitations. Last, we have 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, legal-centric privacy design 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 privacy designs.

References

[Babcock(1967)] Babcock JD (1967) A brief description of privacy measures in the rush timesharing system. In: AFIPS '67 (Spring): Proceedings of the April 18-20, 1967, spring joint computer conference, pp 301–302

[Bauer et al(2006)Bauer, Fabian, Fischmann, and Gürses] Bauer M, Fabian B, Fischmann M, Gürses S (2006) Emerging markets for RFID traces. http://arxiv.org/abs/cs.CY/0606018

[Berendt et al(2005)Berendt, Günther, and Spiekermann] Berendt B, Günther O, Spiekermann S (2005) Privacy in e-commerce: stated preferences vs. actual behavior. Communications of the ACM

[Bundesverfassungsgericht(1983)] Bundesverfassungsgericht (1983) 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. URL http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm

[Chaum(1985)] Chaum D (1985) Security without identification: transaction systems to make big brother obsolete. Communications of the ACM

[Curry and Phillips(2003)] Curry MR, Phillips D (2003) Surveillance as Social Sorting: Privacy, Risk, and Automated Discrimination, London: Routledge, chap Privacy and the phenetic urge: geodemographics and the changing spatiality of local practice

[Cybenko(2003)] Cybenko G (2003) A critical need, an ambitious mission, a new magazine. IEEE Security and Privacy 1(1)

[Dingledine et al(2002)Dingledine, Mathewson, and Syverson] Dingledine R, Mathewson N, Syverson P (2002) Reputation in privacy enhancing technologies. In: CFP '02: Proceedings of the 12th annual conference on Computers, freedom and privacy

[Domingo-Ferrer and Torra(2008)] Domingo-Ferrer J, Torra V (2008) A critique of k-anonymity and some of its enhancements. In: Third International Conference on Availability, Reliability and Security, 2008. ARES 08.

[EU(1995)] EU (1995) 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 p 31, URL http://europa.eu.int/eur-lex/en/consleg/main/1995/en$_1995L0046_index.html$

[Gallagher(1967)] Gallagher CE (1967) The computer and the invasion of privacy. In: SIGCPR '67: Proceedings of the fifth SIGCPR conference on Computer personnel research, pp 108–114

[Glaser(1967)] Glaser EL (1967) 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, pp 303 – 304

[Graham(2005)] Graham S (2005) Software-sorted geographies. Progress in Human Geography 29(5)

[Gross et al(2005)Gross, Acquisti, and H. John Heinz] Gross R, Acquisti A, H John Heinz I (2005) Information revelation and privacy in online social networks. In: WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pp 71–80

[Gutwirth(2002)] Gutwirth S (2002) Privacy and the Information Age. Rowman and Littlefield Publishers

[Hansen(2008)] Hansen M (2008) Linkage control - integrating the essence of privacy protection into identity management. In: eChallenges

[Kifer and Gehrke(2006)] Kifer D, Gehrke J (2006) l-diversity: Privacy beyond k-anonymity. In: IEEE 22nd International Conference on Data Engineering (ICDE'07

[Lederer et al(2004)Lederer, Hong, Dey, and Landay] Lederer S, Hong JI, Dey AK, Landay JA (2004) Personal privacy through understanding and personal privacy through understanding and action: Five pitfalls for designers. In: Personal Ubiquitous Computing, vol 8, pp 440–454

[Lewis(2009)] Lewis P (2009) Video reveals g20 police assault on man who died. The Guardian, URL http://www.guardian.co.uk/uk/2009/apr/07/video-g20-police-assault

[Li and Li(2007)] Li N, Li T (2007) t-closeness: Privacy beyond k-anonymity and -diversity. In: IEEE 23rd International Conference on Data Engineering (ICDE'07

[Liu et al(2006)Liu, Maes, and Davenport] Liu H, Maes P, Davenport G (2006) Unraveling the taste fabric of social networks. International Journal on Semantic Web and Information Systems 2(1):42 – 71

[Lyon(2002)] Lyon D (2002) Editorial. surveillance studies: Understanding surveillance studies: Understanding visibility, mobility and the phenetic fix. Surveillance and Society 1(1)

[McGrath(2004)] McGrath J (2004) Loving Big Brother: Performance, Privacy and Surveillance Space. Routledge: London

[Nguyen(2002)] Nguyen DH (2002) Privacy mirrors: Understanding and shaping socio-technical ubiquitous computing. Technical Report, URL http://citeseer.ist.psu.edu/old/641969.html

[Nissenbaum(2004)] Nissenbaum H (2004) Privacy as contextual integrity. Washington Law Review 79(1)

[Palen and Dourish(2003)] Palen L, Dourish P (2003) Unpacking "privacy" for a networked world. In: CHI '03: Proceedings of the SIGCHI conference on Human factors in computing systems, pp 129 – 136

[Paul(2007)] Paul R (2007) Security expert used tor to collect government e-mail passwords. Ars Technica, URL http://arstechnica.com/security/news/2007/09/security-expert-used-tor-to-collect-government-e-mail-passwords.ars

[Petersen and Turn(1967)] Petersen HE, Turn R (1967) System implications of information privacy. In: AFIPS '67 (Spring): Proceedings of the April 18-20, 1967, spring joint computer conference, pp 291–300

[Phillips(2004)] Phillips DJ (2004) Privacy policy and pets. New Media and Society 6(6):691–706

[Rebollo-Monedero et al(2008)Rebollo-Monedero, Forné, and Domingo-Ferrer] Rebollo-Monedero D, Forné J, Domingo-Ferrer J (2008) 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

[Room(2007)] Room ICSP (2007) Computer society history committee names top 60 events (1946-2006). IEEE Website, URL http://www.computer.org/portal/cms$_docs_annals/annals/images/top60.pdf$

[Rouvroy(2009)] Rouvroy A (2009) Technology, virtuality and utopia. In: Reading Panel on Autonomic Computing, Human Identity and Legal Subjectivity – Legal Philosophers meet Philosophers of Technology, CPDP 2009

[Solove(2006)] Solove DJ (2006) A taxonomy of privacy. University of Pennsylvania Law Review 154(3)

[Stalder(2002)] Stalder F (2002) The voiding of privacy. Sociological Research Online 7(2), URL http://www.socresonline.org.uk/

[Sweeney(2002)] Sweeney L (2002) k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems 10(5):557–570

[Tavani and Moor(2001)] Tavani HT, Moor JH (2001) Privacy protection, control of information, and privacy-enhancing technologies. SIGCAS Comput Soc 31(1):6–11

[Titus(1967)] Titus JP (1967) Security and privacy. Communications of the ACM 10(6)

[Wagstaff(2007)] Wagstaff E (2007) Court case decision reveals dangers of networking sites. Daily Nexus News, URL http://www.dailynexus.com/article.php?a=13440

[Ware(1967a)] Ware WH (1967a) Security and privacy in computer systems. In: AFIPS '67 (Spring): Proceedings of the April 18-20, 1967, spring joint computer conference, pp 279–282

[Ware(1967b)] Ware WH (1967b) Security and privacy: similarities and differences. In: AFIPS '67 (Spring): Proceedings of the April 18-20, 1967, spring joint computer conference, pp 287–290

[Westin(1970)] Westin AF (1970) Privacy and freedom. Atheneum

[Whitten and Tygar(1999)] Whitten A, Tygar J (1999) Why johnny can't encrypt: a usability evaluation of pgp 5.0. In: SSYM'99: Proceedings of the 8th conference on USENIX Security Symposium

[Zwick and Dholakia(2003)] Zwick D, Dholakia N (2003) Whose identity is it anyway? consumer representation in the age of database marketing. Journal of MacroMarketing