Sci Eng Ethics (2014) 20:659–673
DOI 10.1007/s11948-014-9529-9

ORIGINAL PAPER

Assessing Security Technology's Impact: Old Tools for New Problems

Reinhard Kreissl

Received: 14 July 2013 / Accepted: 21 February 2014 / Published online: 2 March 2014

Abstract The general idea developed in this paper from a sociological perspective is that some of the foundational categories on which the debate about privacy, security and technology rests are blurring. This process is a consequence of a blurring of physical and digital worlds. In order to define limits for legitimate use of intrusive digital technologies, one has to refer to binary distinctions such as private versus public, human versus technical, security versus insecurity to draw differences determining limits for the use of surveillance technologies. These distinctions developed in the physical world and are rooted in a cultural understanding of pre-digital culture. Attempts to capture the problems emerging with the implementation of security technologies using legal reasoning encounter a number of problems since law is by definition oriented backwards, adapting new developments to existing traditions, whereas the intrusion of new technologies in the physical world produces changes and creates fundamentally new problems.

Keywords Security technology · Privacy · Risk · Social theory

Security Technology and Technological Security

Trying to define security amounts to nailing the proverbial pudding to the wall. As Luhmann (1993) has pointed out, from the point of view of social theory, security is an empty signifier. Like the idea of health as binary opposition to disease, security is perceived as the conceptual counterpart or contrasting concept to risk or danger.

This paper grew out of a European research project IRISS (Increasing Resilience in Surveillance Societies) funded under the 7th Framework Program Socioeconomic Sciences and Humanities (Grant Agreement No 290492).

R. Kreissl (✉)
Institut für Rechts- und Kriminalsoziologie, Museumsstr. 5/12, 1070 Vienna, Austria
e-mail: reinhard.kreissl@univie.ac.at

While it may be futile to define security, as a vague idea, it provides the basis for screening the world with regard to risks and threats, hazards and dangers. Luhmann conceptualizes the problem of risk not from the individual's point. He rather perceives risk as a culturally and socially structured way of looking at the world. The emergence of risk as a prominent social category according to Luhmann is triggered by a shift in the temporal and social logic of action: applying a risk perspective, we evaluate every decision or action with regard to any future damages it may cause. While an action may be evaluated with regard to the binary scheme of right or wrong, through reference to traditions or criteria of legal and illegal, risk logic focussing on future effects is superseding these criteria. And since the future is difficult to predict, every decision becomes risky. With the increasing interconnectedness of modern societies, the potential number of future effects increases and thus the risks grow. Taking a risk perspective also changes the causality of attribution. While *danger* may be attributed to external forces, *risks* are deliberately taken, i.e. the losses or damages that may occur as a consequence of taking a decision are attributed to the risk taker.[1]

Whether a situation is perceived from a perspective of risk (self-attribution) or danger (external attribution) depends on the societal context and is not dependent on the objective state of the external world. Having your house destroyed by an earthquake can be seen as a loss caused by an external force. On the other hand, it may be attributed to your (risky) decision to build it in an area where earthquakes can happen. Insurance companies play on this distinction when excluding compensation for specific risks.

Assessing present individual or institutional action or decisions with regard to any future damages they may cause fuels an encompassing security discourse without any built-in stop-rules. The crucial point here is that risks loom on either side of a decision: choosing option A in a given situation or refraining from A entails a risk.

The ensuing type of policy discourse emerging under these conditions has been analysed as "securitization" (Buzan et al. 1998). Each and every policy issue in a securitized domain is perceived and negotiated in anticipation of future damages or hazards that might flow from it. This fosters a mind-set of continuous insecurity (or in extreme cases, of latent paranoia) and fuels a Culture of Fear (Glassner 1999).

While under these conditions security as a finite state can never be achieved, nonetheless the problem of attribution can be temporarily solved by public authorities in political discourse. A security "problem" (e.g. Islamic terrorism) is defined and a "solution" (e.g. massive pre-emptive surveillance of potential suspects) is presented and implemented (see De Goede 2008). This process could be called the security-cycle.[2] Such cycles can be reiterated creating ever-thicker layers

[1] As Luhmann states with regard to the difference between risk and danger: "The distinction presupposes … that uncertainty exists in relation to future loss. There are then two possibilities. The potential loss is either regarded as a consequence of the decision, that is to say, attributed to the decision. We then speak of risk – to be more exact of the risk of decision. Or the possible loss is considered to have been caused externally, that is to say, it is attributed to the environment. In this case we speak of danger." (Luhmann 1993: 21)

[2] This concept is common coinage among law enforcement agencies and it precisely mirrors the recursive logic of assessment-evaluation-management-measurement like an endless Moebius band.

of security measures building upon one another while at the same time eroding what could be called pre-securitized trust and ontological security (Giddens 1991). Typically a security-cycle involves the implementation of some sort of security technology to control, track, monitor, or identify individuals, groups or systemic processes, a more or less explicit legal regulation for the use of this technology and a political narrative providing justification and evidence for the intrusive measures implemented to increase security and reduce risk. Securitization as a policy also entails the redefinition of social problems as security problems and public money is diverted from social policy programs to surveillance and control (see Bigo 2002). Investing in security and surveillance technologies can trigger a vicious cycle: the more information is gathered, the more security problems are identified leading to more information gathering.

In order for such technology-based security systems to work, they have to apply some standard of behaviour or normality, defining parameters of secure operation. If a threshold is reached or a deviation occurs, the security-technological system is supposed to produce an alert or react in some pre-determined way. While this logic may apply to some extent in the realm of safety for technical systems (e.g. when controlling the internal mechanical or chemical processes of a power plant; but see Perrow 1999), it is difficult to extend into the realm of the social. Defining a social situation as "normal" is typically an accomplishment of the actors involved, i.e. what is normal is negotiated locally among individuals involved in a social situation. The legal system provides an institutional setting to decide about such negotiations, when conflicting interpretations prevail. But establishing an objectified, algorithmic standard for normalcy is problematic.[3] Nonetheless, technological security regimes are based on such conceptions. We will return to this problem later.

The logic of risk as a cognitive frame to understand security problems is reinforced through what is seen as dominant features of modern societies: these societies are highly complex, interconnected, and mobile (see Urry 2000), and extend beyond the boundaries of nation states, the classical providers of security in political theory (see Beck 1999). They depend on vulnerable infrastructures of transport, logistic chains, communication and energy supply. Hence, these societies see themselves as risk prone, i.e. the dominant political and legal discourse focuses on the containment of risks, on the prevention of perceived future damages to be prevented through a dense network of preventive measures of control and surveillance (for an early candid account see Jungk 1977). The model citizen in these societies has been referred to as the prudent citizen (O'Malley 1996), taking preventive precautions to avoid future harm. Under the heading of security, state and citizen are tied into a regime of preventive risk avoidance, monitoring the present and predicting future events in many cases through the use of security (i.e. surveillance) technologies.

Such a technological approach to security issues, focussing on the preventive control of assumed future damages is difficult to reconcile with some of the entrenched ideas of legal and political theory. Modern law operates on the

[3] A frequent air-traveller might wonder how such standards are defined and implemented, when taken out from the waiting queue for special security checks at the gate (see Kirschenbaum et al. 2012).

assumption of a pre-existing social, normative and moral order. If there is reasonable suspicion that a norm protected under law has been violated, law steps in, i.e. law enforcement agencies are entitled to take executive action, *after* a norm-violating behaviour has happened: committing a murder is illegal, but being somehow under suspicion of killing a person in the future is not. Here a fundamental conflict with the logic of risk and security arises. One of the main achievements of modern law is to limit the intrusion of the state into the realm of civil society and citizens' private sphere without reasonable cause. As soon as the legal system starts to operate along the lines of prevention by identifying and sanctioning pre-criminal behaviours (Zedner 2007), this limitation begins to disappear. The intrusion into the private sphere of citizens, collecting data, expanding pre-emptive surveillance and control may appear problematic against the background of fundamental rights and constitutional safeguards in most modern legislatures, but such measures are presented as legitimate means to prevent future damages under a risk logic. A dominant discursive frame applied to process this problem is based on the metaphor of a balance between "liberty" and "security", both being perceived as dominant values with a weight, connected through a kind of symbolic exchange rate, where the one can be traded off against the other. Seductive as this metaphor may seem, it does not capture the problems evolving with the increasing securitization of society (Zedner 2005), but rather conceals these problems, while at the same time reinforcing securitizing policies.

At closer inspection, most national legal frameworks display a kind of double structure. While at the surface constitutional rights such as the right to privacy are maintained, there often are exceptions to the rule. Laid down in the small print of executive orders, one finds special clauses, opening the door for massive surveillance under certain conditions. It is often the national security agencies that decide whether such "conditions" prevail (Foschepoth 2013).[4]

To understand the emergence of this comprehensive and powerful preventive regime, where surveillance technologies gradually spread across all sectors of society and erode well-rehearsed legal safeguards, one has primarily to look at the economic and political drivers pushing the trend (see Ball and Snider 2013). But one has also to understand what could be termed the implicit anthropology, actor models or conceptions of the social from which different interpretations of security can be derived. While the spread of surveillance technologies may be accounted for primarily in economic terms, there are always shifts in the political semantic and the basic concept of political and public discourse involved. The following will focus on such shifts in what could be called the collective semantic infrastructure.[5] On the

[4] At the time of writing, the practices of different national security services were discussed in the media after NSA whistle-blower Edward Snowden had disclosed some of the practices employed by these agencies. Such disclosures nicely demonstrate the point. For most of the scandalous surveillance practices, the administration could produce some sort of quasi-legal justification.

[5] The term collective semantic infrastructure is used here for lack of a better alternative to refer to a set of foundational categories or contrast pairs underlying a given culture or society. As Bauman (2000) points out, the categories of time and space are undergoing a fundamental change in "liquid" modernity. The same could be shown for categories of gender, where transgender discourses are eroding the binary distinction between the male and the female (see Ekins and King 2006). Other examples to be discussed later are the distinction between the natural and the artificial or life and death.

one hand, security may be understood as the default state of a social unit, depending on the even and autonomous operation of a social order. On the other hand, security can be theorized as a fragile state maintained through the imposition of continuous control of the members comprising a social unit. This difference can be seen when comparing different images of humans, human association and human behaviour.

Three Models of Humans

Tomasello (2008) in his book on the origins of human communication develops an argument that what makes humans human is their capability of developing what has been termed a theory of mind, i.e. the capability to perceive their conspecifics as beings similar to themselves, endowed with the capacity to develop intentions and design their actions on the basis of plans and goals. In Great Apes, who can be seen from an evolutionary perspective as our closest relatives, this capacity has not developed. Having a brain capable of performing such complex social calculation was the basis for the cultural take-off known as the Neolithic revolution. Being able to read another person's mind amounts to understanding her actions as meaningful and directed and so builds up complex structures of symbolically mediated interaction. Tomasello nicely demonstrates the primacy of the dyad over the monad, or the group over the individual (Kreissl and Steinert 2008). This holds not only from a phylogenetic evolutionary perspective, when reconstructing the evolution of the human species, but also at the personal, ontogenetic level: before we become individuals, we are tied into the mother–child dyad or the group caring for the infant. This is where we learn what it means to be an autonomous individual. Our neurophysiological hardware, evolved over millions of years, has equipped us for this task.

In contrast, there is the philosophical tradition running from Hobbes and Locke to present-day political and legal theory rehearsing variations of a master theme of the human being as the self-contained owner of himself, propelled by self-interest, fuelled by biological drives (Macpherson 2011). Being human and civilized amounts to having possession of oneself and being able to obey the rules imposed by the inner (Kant) and outer (Hobbes) ruler of natural drives and desires. The divide between nature and culture here is perceived as the distinction between an unrestrained biology and an externally imposed social, political, legal order, reinforced by sanctions against the rule breaker.[6] In order to maintain such order, an adequate regime of control and rule has to be implemented whereas, following the line of reasoning as developed by Tomasello and advanced research and theory in the neurobiological sciences, it is nature enabling the emergence of the complex social formation.

From the Hobbes-Locke tradition flows the idea of order being the product of good governance and comprehensive control and, taking a bird's eye perspective, it

[6] This requires a heterodox reading of classical texts of political philosophy, an exercise taking place mostly outside the mainstream debate (see Böhme and Böhme 1985).

is here where we find the origins of the idea of security being secured by surveillance and control.

Looking at the historical trajectory of modern societies, one sees that these societies developed primarily along the lines of the Hobbesian model. The interesting point from a theoretical perspective of political semantic is the gradual change in the concept of the human that goes along with this development and which is often overlooked when discussing the problematic of modern societies. According to Foucault, the concept of the human being as an object of knowledge surfaces in the seventeenth century and—so Foucault's diagnosis in the famous final sentences of his book *The Order of Things* (1970)—man as an object of knowledge may soon be erased, like a face drawn in sand at the edge of the sea. Following this idea, one might think of a post-human regime, keeping the outer form of the human but changing in its inner workings. The mechanism resembles what Crouch (2004) diagnosed as "post-democracy", where the institutional set-up remains formally intact, while the inner workings erode.

From this perspective, one could sketch a third model of man or actor model: the techno-social hybrid. Man no longer is the possessive individualist or self-propelled organism, but is about to become a node in an assemblage comprising technologies and artefacts, constitutively dependent on abstract systems for survival (Giddens 1990). The term "techno-social hybrid" has been applied to account for the amalgamation between biological and technical components in an organism. As a cultural theme, the idea of a hybrid organism or even an artificial individual runs through the history of political thought from La Mettrie's *L'homme machine* (1747, 1996) to William Gibson's *Neuromancer* (1984). Similar ideas of hybridization are ventured in science and technology studies where the concept of the "actant" has been introduced (Latour 1988; Brown 2006). From the perspective of critical security and surveillance studies, one would emphasize what could be called the machine-readability of an individual as a dominant feature of such hybridization (Lyon 1994). From the perspective of cultural sociology, one could point to the increasing "mediatisation" of social interaction, fostering a trend described as "dangerisation" (Lianos and Douglas 2000).

What is at stake here is a kind of new ontology with impact on a myriad of social, cultural, political and legal issues. What should be reconstructed are the gradual, glacial shifts in the human condition, the fabric of society and the structure of social interaction. Taking these shifts into focus, we can see the erosion of basic foundational concepts in legal and social theory. These shifts are rarely considered, since many of the concepts applied here are seen as self-evident. While it is acknowledged that certain concepts, such as privacy, have to be re-conceptualized in present-day societies, the very idea of an autonomous human actor, endowed with fundamental rights, forming the underlying basis of the idea of privacy is still maintained.

When defining this model of an autonomous human actor, a number of binary differences are introduced: the human writ large is contrasted to the technical, the natural is contrasted to the artificial, etc. A brief look at contemporary debates on technology and human nature in social theory reveals the limits of such a narrow conception of the human (see e.g. Rose and Novas 2005). What can be observed there is the gradual erosion of the difference between nature and technology, used to define a distinctive realm of human agency. This difference can be linked to the

above-mentioned difference between risks and dangers as two different framings for the understanding of security. While events and states deemed *natural* are beyond human reach and decision, they become objects of human decision as soon as they are within the reach of technology. Natural events are attributed to external forces; events, perceived as a consequence of individual decisions, are attributed to the individual who takes the decision. This can be demonstrated when briefly looking at the human life span and the effects technological developments have at either end of the human life. With the spread of technologies for prenatal genetic screening to the level of consumer medicine, women (and prospective parents) are confronted with risky decisions regarding their future offspring: should they use prenatal testing to determine genetic risks facing the embryo and if a certain risk such as trisomy 21 is detected, should they opt for abortion (Tremin 2006)? A similar situation can be found at the other end of the human life span, where new technologies allow for life-extending measures beyond what used to be called a "natural" death. Risky decisions have to be taken here as well: should the equipment for keeping an organism alive be turned off or not? When a person decides in advance whether s/he wants life-extending measures to be taken, there are severe risks involved as well. And, as mentioned above, both sides of the decision bear a risk.

The existential situations of birth, life and death, beyond the reach of informed decisions for most of human history are becoming the object of multiple and complex risky decisions due to technologies shaping and manipulating what used to be "natural" processes—they become securitized. Without going into detail here, one can emphasize the effect of technology on the conception of fundamental categories applied in making informed decisions in risk-prone, i.e. future-oriented situations. It is difficult if not impossible to go back to what could be termed a state of innocence (or to use a kind Rawlsian veil of ignorance) under these conditions. Being human in these scenarios amounts to being an organism merged with technologically generated information (e.g. about certain genetic or other physiological states). What can be known about an individual can be known only due to the application of complex technologies. This affects also the first-person perspective: to understand who I am, I have to draw on aspects of my machine-readability. Scholars in surveillance studies have coined the term "data double" (Lyon 2007) to analyse the emergence of person-related profiles in remote databases, but as the term double denotes, this idea is still rooted in the ontological human versus technical divide. The question though is: can this divide still be maintained? Can notions of what it means to be human in a more traditional ontological sense still be meaningfully applied? Being machine readable has become a core element of the human condition in modern societies and at the same time unavoidably creates a myriad of data traces, probably collected somewhere by someone for some purpose.[7]

[7] The recent hype over the so-called "quantified self" is a pop-cultural offspring of what scholars like Nikolas Rose called the "biological Self" (Rose and Novas 2005). The idea to constantly monitor vital signs such as heart rate or blood pressure and then to adapt one's daily life to an optimized path is a reflexive use of new technologies and an adaptation of the self concept. Insurance companies may want to analyse such bio-data, calculating their clients' health risks (which are financial risks for the companies). In any case, the idea of what it means to be human—reflexively, economically and politically—is changing with the injection of such monitoring technologies into the human organism.

This situation of a human being constitutively *informatized* or *datafied* can create challenges with unexplored cultural and social implications, as will be shown in a brief discussion of the concept of privacy. The binary distinction between public and private dates back to the ancient Greek debates about democracy and political life in the polis. The private sphere (or the Greek *oikos*) was opposed to the interaction among equals in public space (the *agora*). It was in the public space, in face-to-face encounters with others at eye-level, where the social existence of the citizen materialised through reciprocity (Arendt 1993). This reciprocity could never be achieved in the *oikos*, where the (male) Athenian citizen acted in an a-symmetrical position as the *oikosdespot*, the master of his servants (including his wife and children). Hence the public was normatively privileged over the private life. This has changed over time, but what has remained is the intuitively plausible idea of the private as a sphere under the exclusive control of the individual. This change or reversal may also account for a certain ambiguity in the present-day debate about privacy, which is also seen as a pre-condition for civic engagement (an obviously public activity).[8] Taking a critical look at contemporary Western democratic societies, one finds a paradoxical mirroring of private and public spheres: whereas many political activities are kept secret, and freedom of information with regard to what public authorities do is very limited (Katz 1970), there is at the same time in many respects a publication of hitherto classical private information, either as a consequence of surveillance or of deliberate exposure of individuals in cyber space. While in social and political theory, the mutual dependence, balance or dialectic of public and private as distinct spheres, forms of social relation or practices have been discussed extensively (e.g. Habermas 1991), the emergence and spread of new technologies and surveillance practices affects this subtle balance in a substantial way. This begs the question of whether categories of political thought and legal instruments developed in and for a pre-digital society are still capable of capturing present-day problems of privacy and autonomy. The challenge is to reconstruct these ideas while taking into account the socio-technical changes shaping the human condition.

Technology and the Devolution of Privacy

On 21 April 1865, the coffin with the body of Abraham Lincoln, assassinated president of the United States, was put on a train in Washington DC and sent on a journey to Springfield Illinois where the train arrived 3 May 1865 and Lincoln's remains were buried. On the way from DC to Springfield, the train stopped several times for private and public viewing. About 130 years later, Diana Princess of Wales died in a car crash in Paris. The public funeral in Westminster Abbey on 6 Sept 1997 was attended by an estimated 3 millions and over 2 billion watched live coverage of the funeral on TV. These are two indicative events for the study of

[8] The link between the private and public sphere here is made through what is termed the "chilling effect". Speaking out in public, knowing that any such public statement can be recorded or documented by the police or any other agent, is supposed to have a chilling effect on potential civic activists. Such effects may also emerge as side-effects of governing cyber space (see Cohen 2003).

privacy and technology. In both cases, public figures are centre-stage but due to different technologies their public appearance was completely different, creating a different set of problems. Controlling the public exposure of Lincoln's corpse was much easier than for that of Princess Diana. Lawsuits on the publication of pictures taken by paparazzi of the late princess went on for years after her death and caused fierce debates about privacy, freedom of information and the self-restraint of the media.

What today is seen as the modern debate about privacy was triggered by the emergence of new technologies. With the spread of photography, Warren and Brandeis (1890) in the US called for the right to be let alone as a fundamental human right. Perceiving privacy as a concept (a social practice as well as an individual state) to be addressed within the realm of law, as Warren and Brandeis did, points towards a cultural change. The availability of photography, particularly of taking pictures at a distance without the consent of the person being pictured, combined with the spread of newspapers, circulating such images to a nationwide public was the basis for a new cultural practice, challenging or problematizing the categorical divide between private and public. Whereas in "pre-photographic", "pre-mass-media" times, being in public meant to expose oneself or being exposed physically to others (like Lincoln's corpse on the train), modern photography dissolved the physical bodily appearance from the public visibility of the person.[9]

This created a new problem that, from a legal perspective, could be termed the (intellectual) property right of representation—or for that matter of "data"—and so the issue had to be addressed in law to create collectively binding definitions and regulations (see Westin 1967 for an early account). The right to privacy today is considered as an abstract individual right, connected to an abstract person, who has, or should have, the power to determine what others can see, hear, and know about him or her—independent of any immediate detrimental effects. In Germany, this was codified as a constitutional right of "informational self-determination" in 1983.[10]

This right (as most other subsequent privacy legislation) was modelled after the concept of a legal subject, being the owner of person-related information and data.

Establishing such a right in legal discourse requires reference to entrenched traditions, looking at former cases applicable to this presumably new constellation. Such cases typically involve person-to-person problems of privacy, which are concerned with the public disclosure of private facts. *Alter* reveals a fact, considered to be private, about *Ego*, thereby constituting a breach of privacy. The problem though is that privacy in present-day societies can hardly be comprehensively conceptualized following this pattern, since individuals have become leaking containers, leaving continuous data traces when pursuing their daily course of life and the idea of "owning" these data is like owning the footprints left from a walk on a soft surface.

[9] With the emergence of new techno-gadgets such as Google Glass, we may see a new turn of the screw with regard to privacy intrusive technologies (see Boyd 2008).

[10] The same court in 2008 decided that data processors have to take adequate measures to protect person-related data from misuse.

When looking at legal constructs such as the right to informational self-determination, one of the key questions is: what or who could be the referent of such "selves" in this constitutionally defined right? Can such a self be meaningfully construed? Is there a meaningful way to talk about a self-contained person, as the owner of data being produced in, and relating exclusively to, the private sphere? Or have "data" not become a defining element of the individual and so being a person amounts to being a machine-readable, datafied techno-social hybrid? Can the difference between the "self" as the bearer of rights and the "data" referring to this self still be applied under these conditions or are data and self collapsing into one?

Alternative accounts to privacy have attempted to take the social context or social function as a starting point (e.g. Nissenbaum 2010; Baghai 2012) and to understand privacy not as an absolute concept but in terms of "contextual integrity", as Nissenbaum calls it. Privacy from this perspective is probably better understood as a form of contextualized social practice. The important difference here is the refocusing on the social situation as opposed to the individual right, or the refocusing from an isolated (Hobbesian) individual to a dyadic constellation, as analysed for example by Mead (1934). If we take the social situation as a starting point, privacy can be understood in a different way. It is no longer the isolated individual having a right, but social actors in context, acting in a mundane situation, creating or maintaining privacy among them.

Taking the contextual view, privacy becomes an issue, a topic of debate, controversy, law, and research, only when it seems to be jeopardized as a formerly taken-for-granted element of the physical world. Privacy as a mode of social practice, as a state occurring quasi naturally in society, historically remained in the background unless a disturbance took place. Privacy was practised but went unnoticed as long as it was not disturbed. Introducing photography in Warren and Brandeis' times constituted such a disturbance. Injecting a technology that can freeze images and make them portable into the flow of public daily life creates a problem for the normative order and the regulation of privacy.

Bringing privacy to the foreground, making it a topic of debate involves defining explicit (legal) standards for a social practice or norm hitherto performed or followed without explicit guidance. Respecting another person's privacy was—in pre-photographic times—a matter of politeness, of courtesy, and a problem of primarily local relevance, involving interpersonal relationship. To maintain privacy, the only requirement was to have at least two competent social actors following a cultural norm, implicitly agreed upon. Jane Austen's novels nicely describe this complex and subtle grammar of privacy and public space. Honouring privacy was strictly a matter of reciprocal co-ordination among culturally competent actors of higher status (privacy never was a topic for the lower classes; see Braudel 1993). Privacy also was mainly defined through private space. Whatever happened or was uttered in a realm conceived as private was not supposed to be communicated outside this sphere. But which spaces qualify as private in a society of pervasive electronically and institutionally mediated communication?

Of course, there has always been the social practice of gossip, circumventing the cultural rules of privacy protection. Information obtained from a person and considered as private could be communicated to a third party behind her back and

circulated without her knowledge and consent. But this was a breach of privacy remaining in the domain of the physical world. Gossip as a breach of privacy is different from the systematic large-scale collection of all kinds of data about a person outside an immediate social and local context and gossip can take on a quite different dynamic once it is turbo-charged by new social media (Solove 2007). The prototypical scenario informing Brandeis and Warren's legal reasoning could be seen as an extension of the gossip model, made possible by photography and mass media, and focussing on the individual person's reputation. The contemporary problematic though is different. It is no longer about disclosing facts considered private to a third person but about not knowing what person-related facts, data and information are "out there" in the first place. The dynamics of privacy violations in a society composed of individuals continuously leaking data and being defined by their machine-readability is difficult to capture with the gossip model. A frequently applied image to capture this new situation is the metaphor of Big Brother. This Leviathan-like figure represents a panoptical centre of control and surveillance, where all information is digested and turned into repressive governmental action. Big Brother fuels the fantasy of some actor knowing everything and being capable of governing the life of the ordinary citizen in more or less subtle ways.[11]

Solove (2001) critically examines this key metaphor developed by George Orwell in his novel *Nineteen-Eighty-Four*. He suggests as an alternative and complementary metaphor Franz Kafka's vision as developed in his novel *The Trial*. In the story, the main character Joseph K. is accused of having committed a crime, though he never finds out what charges exactly are brought against him. The key point is, Joseph K. never finds out, no matter how hard he tries, what is going on in the impenetrable bureaucracy handling the charges against him. The novel ends with the execution of the protagonist without his having found out what the whole process was all about. Joseph K. is losing his ontological security, not finding a person, sharing his concerns, providing him with advice and information. He is forced to play to rules he does not know.

When Solove suggests replacing Big Brother with Kafka's vision as developed in his novel of *The Trial*, he assumes an existentialist idea of a human being, exposed to veiled and non-transparent powers: the unprotected, weak human being in front of closed doors and behind these doors an amorphous power. He is deprived of his right to informational self-determination, since he does not know what information to ask for and if he asks he is informed that all the inner workings of the bureaucracy are to remain secret.

Is Kafka's hero a valid metaphor for today's surveillance society? There is a crucial difference: whereas Joseph K. tries to find out what the bureaucracy knows about him, what charges are brought against him, today he would be in a situation where he has to continuously produce person-related information in order to interact with such a bureaucracy. It is no longer the naked, vulnerable human confronted with a powerful bureaucracy, keeping silent and not reacting to his pleas, but rather

[11] The Big Brother metaphor tends to focus on surveillance, leaving aside the economic dimension of a data-driven economy. Collecting, processing and trading personal data has become a profitable business model. With every click on the computer, users create valuable intelligence not only for state authorities but for private enterprises as well.

the digitalized, datafied, informatized citizen, who has to pass through control and check points, producing pin codes, ID-documents, passwords and being scrutinized by different scanning technologies in order to gain access and in doing this permanently exchanging (leaking) data with the other side. While Jospeh K. takes a random walk through the labyrinth of an opaque bureaucracy, waiting in front of closed office doors only to return without any new information, the movements and actions of his present-day counterpart would be friendly, welcomed at an information counter, precisely monitored and registered and he would be guided along a pre-determined path. This is not to say that the modern datafied individual is less vulnerable in the face of an opaque bureaucracy. The main difference is in the activation and "responsibilisation" of the subject, who is supposed to actively co-operate and interact, to produce ID-tokens and make choices when entering into an exchange with the powers of the virtual world.

With the comprehensive, technologically mediated "datafication" of society, it becomes increasingly difficult to set aside what could be called a non-digital realm of human existence, a relevant set of social processes going unnoticed and unrecorded. Such a realm is necessary to talk in a meaningful way about privacy. Human existence is comprehensively datafied including the most intimate relations.[12] But not all of the data collected and stored are the result of targeted surveillance regimes. Often data are produced as side effects of electronic communication or digital consumerism creating data about commercial transactions that are collected and stored automatically. And finally not all surveillance regimes are per se malevolent, satisfying problematic needs and desires of a Big Brother—but nonetheless they affect the ontological status of the human being.

Conclusion

When it comes to a critique of modern surveillance technology, privacy as a right linked to a person and privacy as a cultural practice, informing social interaction, both seem to miss the point. Conceiving of privacy as a right, to be enforced by law, falls short in the face of the sheer magnitude of data created in the technology-mediated daily walk of life in modern societies. Furthermore, this right is permanently hollowed out by new legislation justifying intrusive measures with security needs. Trying to understand privacy as a cultural practice, one encounters similar problems: even the most intimate of encounters are in one way or the other linked to electronic media, with platforms such as Facebook only the tip of the iceberg[13] and so in order to create a private situation it is necessary to take

[12] Although trust and reciprocity developing in face-to-face interactions still provides the basis for social relationships, the "virtual/digital" is superseding the "natural/local" in the social fabric of society. This provides the basis for a new form that could be termed "inter-veillance", as opposed to surveillance and sousveillance, creating new opportunities to follow up on the digital traces a person has left on the Internet (see Jansson 2011).

[13] By way of anecdotal evidence, one could quote an article from *The New York Times* of 25 Dec2012, written by Jessica Silver-Greenberg, ("Perfect 10? Never mind that. Ask for her credit score") reporting on the use of credit scoring as one parameter to choose partners for dates in online forums.

precautions. Having a private sphere amounts to cutting off most of the links defining an individual as a node in the network society since being exposed to data-gathering devices or data-generating processes has become the default state of everyday life in Western societies.

If neither Big Brother nor Kafka's Trial, what image would fit the present day constellation of security and surveillance? Maybe William Burroughs' *Soft Machine* or the movie *The Matrix* could provide a more adequate metaphor. What a new metaphor would have to capture is the self-referential nature of surveillance and security technologies implemented to monitor, track, guide, and control the multitude of flows of humans, information, energy, capital and symbols in the *Economies of Signs and Space* (Lash and Urry 1994). Human actors have been gradually transformed into an element of the environment of a giant system comprising a myriad of complex technologies—some of them explicitly implemented for surveillance and security purposes, others designed for different tasks—and the main objective or focus of surveillance has changed: what has to be maintained is the smooth working of the technological assemblage where human actors are reduced to a source of irritation. Looking at research on "safety culture" and "human factors", assessing "human reliability" as a risk for the operation of techno-social systems nicely demonstrates this point (Badke-Schaub et al. 2008). Probably there is no best solution to this problem, since neither is there a way back to a pre-technological culture, nor is there a dark centre of power inhabited by Big Brother who could be eliminated by some sort of magic bullet. What remains is to find an answer to the question of how to replace the old concepts built around the idea of an autonomous human actor to find a meaningful way to address these new problems. There is no easy way out here, but probably a feasible political strategy could be built around the idea of transparency. Reconstructing autonomy in the digital age of encompassing surveillance requires what could be termed "privacy labour". Empowering individuals as techno-social hybrids to manage and mould the "techno" part of their existence, to access, check, control and change the information creating their data doubles, could help to regain autonomy and privacy. This not only requires a reflexive awareness of what it means to be a person in the digital world, but at the same time a new technological literacy and the adequate legal-political framework to create a platform for the debate of what it means to be human in the triple sense of Homme, Bourgeois and Citoyen in the age of encompassing surveillance.

Acknowledgement I would like to thank my colleague David Wright for helpful advice and two anonymous reviewers for pointing out shortcomings in the draft.

References

Arendt, H. (1993). *Was ist Politik?*. München: Piper.

Badke-Schaub, P., Hofinger, G., & Lauche, K. (Eds.). (2008). *Human factors. Psychologie sicheren Handelns in Risikobranchen*. Heidelberg: Springer.

Baghai, K. (2012). Privacy as a human right: A sociological perspective. *Sociology, 46*(5), 951–965.

Ball, K., & Snider, L. (Eds.). (2013). *The surveillance industrial complex: Towards a political economy of surveillance*. London: Routledge.

Bauman, Z. (2000). *Liquid modernity*. Cambridge: Polity Press.
Beck, U. (1999). *World risk society*. London: Polity Press.
Bigo, D. (2002). Security and immigration: Toward a critique of the governmentality of unease. *Alternatives: Global, Local, Political, 27*(1), 63–92.
Böhme, G., & Böhme, H. (1985). *Das Andere der Vernunft – Zur Entwicklung von Rationalitätsstrukturen am Beispiel Kants*. Frankfurt/M: Suhrkamp.
Boyd, D. (2008). Facebook's privacy trainwreck: Exposure, invasion, and social convergence. *Convergence: The International Journal of Research into New Media Technologies, 14*(1), 13–20.
Braudel, F. (1993). *Civilization and capitalism, 15th–18th Century, Vol. I: The structure of everyday life*. New York: Penguin Books.
Brown, S. (2006). The criminology of Hybrids. Rethinking crime and law in technosocial networks. *Theoretical Criminology, 10*(2), 223–244.
Buzan, B., Waever, O., & Jaap de Wilde, J. (1998). *Security: A new framework for analysis*. Boulder: Lynne Rienner Publishers.
Cohen, J. E. (2003). DRM and privacy. *Berkeley Technology Law Journal, 18*, 575–617.
Crouch, C. (2004). *Post-democracy*. Cambridge: Polity Press.
De Goede, M. (2008). The politics of preemption and the war on terror in Europe. *European Journal of International Relations, 14*(1), 161–185.
Ekins, R., & King, D. (2006). *The transgender phenomenon*. London: Sage.
Foschepoth, J. (2013). *Überwachtes Deutschland. Post- und Telefonüberwachung in der alten Bundesrepublik*. Göttingen: Vandenhoeck & Ruprecht.
Foucault, M. (1970). *The order of things: An archeology of the human sciences*. New York: Vintage Books.
Gibson, W. (1984). *Neuromancer*. New York: Ace Books.
Giddens, A. (1990). *The consequences of modernity*. Stanford: Stanford University Press.
Giddens, A. (1991). *Modernity and self-identity: Self and society in the late modern age*. Stanford: Stanford University Press.
Glassner, B. (1999). *The culture of fear: Why Americans are afraid of the wrong things*. New York, NY: Basic Books.
Habermas, J. (1991). *The structural transformation of the public sphere*. Boston: MIT Press.
Jansson, A., (2011). Perceptions of surveillance: Reflexivity and trust in digital domains. In *Paper presented at the annual meeting of the International Communication Association, TBA, Boston, MA*, May 25, 2011 http://citation.allacademic.com/meta/p488315_index.html (last visited Jan 5, 2014).
Jungk, R. (1977). *Der Atomstaat*. München: Kindler.
Katz, J. M. (1970). The games bureaucrats play: Hide and seek under the freedom of information act. *Texas Law Review, 48*, 1261–1278.
Kirschenbaum, A., Mariani, M., Van Gulijk, C., Lubasz, S., Rapaport, C., & Andriessen, H. (2012). Airport security: An ethnographic study. *Journal of Air Transport Management, 18*, 68–73.
Kreissl, R., & Steinert, H. (2008). Für einen gesellschaftstheoretisch aufgeklärten Materialismus. *Kriminologisches Journal, 40*(4), 269–283.
La Mettrie, J. O. (1996). *Machine Man and Other Writings* (trans. by. Ann Thomson). Cambridge, UK: Cambridge University Press (first publ. 1747).
Lash, S., & Urry, J. (1994). *Economies of signs and space*. London: Sage Publishers.
Latour, B. (1988). *The pasteurization of France*. Cambridge, MA: Harvard University Press.
Lianos, M., & Douglas, M. (2000). Dangeriztion and the end of deviance. *British Journal of Criminology, 40*, 261–278.
Luhmann, N. (1993). *Risk: A sociological theory*. New York: De Gruyter.
Lyon, D. (1994). *The electronic eye: The rise of the surveillance society*. Minneapolis: Uniersity of Minnesota Press.
Lyon, D. (2007). *Surveillance studies*. Cambridge: Polity Press.
Macpherson, C. B. (2011). *The political theory of possessive individualism, from Hobbes to Locke*. Oxford: Oxford University Press.
Mead, G. H. (1934). *Mind, self and society*. Chicago: University of Chicago Press.
Nissenbaum, H. (2010). *Privacy in context technology, policy, and the integrity of social life*. Stanford: Stanford University Press.
O'Malley, P. (1996). Risk and Responsibility. In A. Barry, T. Osborne, & N. Rose (Eds.), *Foucault and political reason: Liberalism, neo-liberalism, and rationalities of government* (pp. 189–207). Chicago: University of Chicago Press.

Perrow, Ch. (1999). *Normal accidents. Living with high-risk technologies*. Princeton: Princeton Unviersity Press.

Rose, N., & Novas, C. (2005). Biological Citizenship. In S. J. Collier & A. Ong (Eds.), *Global assemblages: Technology, politics and ethics as anthropological problems* (pp. 439–463). Oxford: Blackwell Publishers.

Solove, D. J. (2001). Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review, 54*(6), 1393–1462.

Solove, D. J. (2007). *The future of reputation. Gossip, rumor and prvacy on the internet*. New Haven: Yale University Press.

Tomasello, M. (2008). *Origins of human communication*. Cambridge, MA: MIT Press.

Tremin, S. (2006). Reproductive freedom, self-regulation, and the government of impairment in utero. *Hypathia, 21*(1), 33–53.

Urry, J. (2000). *Sociology beyond societies: Mobilities for the twenty-first century*. London: Routledge.

Warren, S., & Brandeis, L. B. (1890). The right to privacy. *Harvard Law Review, IV*(5), 193–220.

Westin, A. (1967). *Privacy and freedom*. New York: Atheneum.

Zedner, L. (2005). Security and liberty in the face of terror: Reflections from criminal justice. *Journal of Law and Society, 32*(4), 507–533.

Zedner, L. (2007). Pre-crime and post-criminology? *Theoretical Criminology, 11*(2), 261–281.