Eur J Secur Res (2016) 1:77–95
DOI 10.1007/s41125-016-0005-1

ORIGINAL ARTICLE

Security Through Technology? Logic, Ambivalence and Paradoxes of Technologised Security

Stefan Kaufmann[1]

Received: 18 February 2016 / Accepted: 22 February 2016

Abstract The article presents key concepts, issues and empirical results from a social scientific examination of preliminary technologisation trends in the security sector. This examination largely takes the form of a critique which deals with the ambivalence, unintended effects and paradoxes of such processes. The causes and dynamics behind the preliminary technologisation of security arise not least from a reflection on the intrinsic vulnerability of liberal societies. Globally networked structures are addressed as a security problem. This recursive loop, that technologisation itself evokes sui generis uncertainties, also applies to security technology. The article systematically explores how security and insecurity are interwoven. It combines different technosociological perspectives as well as empirically examining significant dimensions and typical patterns of technological ambivalence. (1) Its starting point is the view of normative theory that technology always involves the materialization of expectations which give rise to specific follow-up actions and effects. (2) In a praxeological view the interesting fact is that security technology, despite such normative effects, still remains more or less open to context-specific adaptation. Differences in use, unintended and counterproductive effects are to be expected. (3) The concept of hybrid actors is drawn upon in considering the potential for new technology to profoundly transform security bodies and practices. (4) Based on the premise that technology provides a constitutive framework which lends stability, durability and specific formats to social processes and social forms in the first place, individual lines of thought can be conflated with the question of what power political and sociopolitical significance is to be found in the technologisation of security.

✉ Stefan Kaufmann
stefan.kaufmann@soziologie.uni-freiburg.de

[1] Institute of Sociology, Albert-Ludwigs-Universität Freiburg, Rempartstr. 15, 79085 Freiburg, Germany

Keywords Security devices · Security practices · Sociological theory of technology · Surveillance

1 Introduction: The Technologisation of Security

Security technology and services are a dynamic growth industry. According to a study of the US security market that was published in 2012, turnover in the industry stood at approximately USD 40 billion in 2007, USD 48 billion in 2011 and USD 51 billion in 2012, and is estimated to reach USD 81 billion in 2020.[1] When expanded to the global security market, the value forecast for 2020 is USD 226 billion.[2] Similarly, a study drawn up by the European Commission in 2012 projected long-term growth of 5 % (European Commission 2012, 459). For the German security market, a study authored in 2008—and therefore before the financial crisis—also predicts substantial rates of growth: 10 % annually in the detection technology sector, and 5 % for technology used in screening individuals, luggage and goods (VDI/VDE 2009, 34). Current data from the German Zentralverband Elektrotechnik und Elektroindustrie (Electrical and Electronic Manufacturers' Association) shows steady growth rates in Germany's electronic security technology sector between 2010 and 2015, with total value rising from just under €2.6 billion in 2010 to almost €3.3 billion in 2014.[3]

The boom in the security technology sector is generally considered to be a consequence of the events of 9/11. The immediate response from the US government can be highlighted as a driving force first of all, followed by that of many other governments and international authorities. New security laws were enacted; security measures and checks at borders, airports and ports were dramatically tightened; a new dimension was reached in monitoring communications as well as the flow of goods, traffic and money (cf. Lyon 2003b). At the same time, security laws set benchmarks for policies in research and industry. A prime example of this is the law passed under George Bush in 2007 that required all containers entering the USA by air or maritime freight from 2010 or 2012 to be scanned at their point of departure for hazardous nuclear, biological and chemical materials—even though there was no relevant hardware or software developed to a point where it was ready for use, let alone appropriate facilities available (cf. VDI/VDE 2009, 33). Legislative and executive security initiatives were therefore expected to be specifically coupled with scientific and technological research as well as industrial policy initiatives. Thus the Homeland Security Acts of 2002 established the *Homeland Security Advanced Research Projects Agency*, with departments for border and maritime security, chemical and biological materials, explosives, cybersecurity, and resilient systems.[4] The nexus between the security sector, science

[1] These results from the study published in late 2012 by the *Homeland Security Research Corporation* are available via http://homelandsecurityresearch.com/2012/09/u-s-homeland-security-public-safety-market-2013-2020/ (last accessed 30 October 2015). It was not possible to view the study itself, which is 624 pages long and not available through public libraries; the price for individual users is USD 4450.

[2] http://homelandsecurityresearch.com/2015/06/Global-Safe-City-Industry-Technologies-Market-2015-2020#figures (last accessed 30 October 2015).

[3] See http://www.secupedia.info/wiki/Sicherheitsmarkt (accessed 30 October 2015).

[4] Cf. http://www.dhs.gov/science-and-technology/hsarpa (accessed 12 April 2015).

and industry in Europe takes a similar shape. In its “Security Industrial Policy”, the European Commission quite explicitly associates security policy with the accelerated development of a European security industry: “[…] no security concept is thinkable without the adequate technologies. A competitive EU security industry is the conditio sine qua non of any viable European security policy and for economic growth in general” (European Commission 2012, 4). Security threats are primarily redefined as market opportunities, although the market would need to be developed first, or its development would need to be supported politically (cf. Hoijtink 2014, 459 et seq.). As a consequence, well-endowed security research programmes were set up by the EU and individual European countries such as Germany. The EU invested some €1.3 billion in security research between 2007 and 2013,[5] with the German Federal Ministry of Education and Research spending around €400 million over the same period as part of its “High-Tech Strategy”.[6]

Moreover, it is characteristic for this market that research and development programmes address not only classic departmental questions regarding internal security, but rather also work to increase social resilience. Technological developments for disaster prevention, emergency services, infrastructure security, food security, or combating pandemics are integral components of concepts such as homeland security or civil security. What emerges in this context is a security technology market that is difficult to define using traditional institutional classifications such as civilian/military, public/private or safety/security (cf. VDI/VDE 2009, 24–26; Hoijtink 2014, 460). Quite a few of the stakeholders involved in developing the market have backgrounds in military research and industry (cf. Hayes 2009). However, even focusing only on the “hot spots” of technological research, there is an enormous range of developments in security technology:

- Detection technologies: biosensors, odour sensors, computer tomography and terahertz technology to detect biological, chemical or nuclear substances; or sensor technology such as infrared sensors, acoustic sensors or X-ray technology to detect items or individuals.
- Identification technologies: biometric technology such as fingerprint, facial or iris recognition; pattern recognition to identify movements or to match odours or genetic fingerprints.
- Surveillance and tracking: wiretapping and recording technology for monitoring rooms, individuals and telecommunications, encryption and decryption technology, drones, intelligent video systems, web 2.0 applications.
- Development of automated system functionalities: in the field of data transfer, storage technology, analysis technology; or robotics technology for use by the emergency services etc.

[5] Out of 15 research sectors funded during this period, security ranked 13th in terms of budget, not far below the €1.74 billion spent on environmental research, but well above the €583 million awarded to the humanities and social sciences (cf. http://ec.europa.eu/research/fp7/index_en.cfm?pg=budget, accessed 12 April 2015).

[6] http://www.bmbf.de/de/6293.php (accessed 12 April 2015).

- Protection technologies: new materials developed to increase the shock resistance of buildings and other structures, for example; or materials developed for protective clothing worn by emergency responders, fire fighters, etc.[7]

Is the world safer with all this security technology? This, of course, is the wrong question. Security is one of those “wicked problems”—according to disaster researcher Wolf Dombrowsky (2012, 28)—a problem for which we do not have a clear-cut and stable definition, and where we are unaware of any point at which something is known to be safe and can be assessed as such on the basis of clear criteria. This also makes it impossible to decide what strategies solve security issues, which is why security policy must be regarded as the “management of unsolvable problems” (ibid., 29). However, even with the more precise question of whether particular technologies increase security in a given context by preventing specific hazards and damage or reducing the impact thereof, ambivalence often remains: in the words of Rammert (2015, 155), “why is it that more security technology does not automatically lead to less insecurity?”[8]—despite its ability to increase the effectiveness, reliability and efficiency of security measures. The reason lies not only in breakdowns and malfunctions, but also in structural ambivalence and the unintended effects of security technology implementation.

This idea is by no means new. On the contrary, it has long been the subject of work in the humanities and social sciences—including under the label *surveillance studies*. With reference to the question of how security and insecurity are interwoven, the following section aims to present key concepts, issues and empirical findings from a social scientific examination of preliminary technologisation trends in security practices. What technologies are under discussion? Security activities encompass a broad spectrum: “observing, identifying, classifying, combining, checking, documenting, archiving, investigating, warning, alerting, accessing, defending, searching, confining and barring” (Rammert 2015, 171). This list is not exhaustive, but it is evident that the technological arsenal intended as a contribution to security extends far beyond current innovation. This wide scope is not the only reason why a comprehensive definition of security technologies cannot be used as a basis for analysis—another is that a screwdriver can be used as a weapon and biometric facial recognition can be used to catalogue holiday photos. Instead, the area of interest here is technology for observation or surveillance and control, which is the focus of security policy expectations and market opportunities as well as broad public concern—with the exception of the protection technology listed, all innovation “hot spots” can be counted in this category. Firstly, the

[7] This list is taken from an index drawn up by Bruno Gransche, Philine Warnke and Peter Zoche (Fraunhofer ISI, Karlsruhe) as part of the BaSiD (Barometer Sicherheit in Deutschland, or “German security barometer”) project sponsored by the German Federal Ministry of Science and Education. In terms of the security market overall, however, the high-tech sector is by no means the only home for security technology. Fire alarms, mechanical locks, burglar alarms, video systems and similar items also cover a large proportion of the market (cf. Gummer et al. 2014, 7–10).

[8] This article follows Rammert’s conceptual viewpoint, but proposes a different systematisation and makes greater use of empirical results from security research instead of more general technosociological findings. All quotes from German are translated by the author.

ambivalence of such technology is systematically explored with reference to a variety of technosociological perspectives, different conceptualisations of and methodological approaches to technology. Significant dimensions and typical patterns of technological ambivalence are then empirically examined. (2) Initially starting with viewpoints that understand technology as normative social hardening, (3) praxeological conceptualisations are then used to analyse how technology is handled and adopted as part of security practices, and (4) the hybrid actor concept is drawn upon in considering the potential for new technology to profoundly transform security bodies and practices. (5) Finally, based on the premise that technology provides a constitutive framework which lends stability, durability and specific formats to social processes and social forms in the first place, individual lines of thought are conflated with a focus on the question of what power political significance is to be found in the technologisation of security.

2 Technology as a Normative Hardening of Society

All technology involves the materialization of social designs, in each case constituting a project with inherent expectations—of a political, legal, social, cultural and symbolic nature. At the same time, it also provides normative configurations which require specific follow-up actions—technical, logical, cognitive, psychological—and always defines the skills and roles of users more or less openly. In terms of power theory, even Marx described in his *Machinery and Modern Industry* chapter how capitalist rule is inherent in machinery and objectifies itself with the factory rules prescribed by mechanical rhythms (Marx 1984/1867, 391–530). Actor-network theory refers to translation or delegation, when for example the construction of speed bumps on a road causes the norm of driving slowly out of consideration for others to be transformed into a driver's self-interest in not damaging their car (Latour 1994, 38–40). In the normative theory of action, almost anything—mineral water bottles, for example—can be used to exemplify the complexity of referential connections between technical standards and social norms. There are references to inherent health standards (various mineral contents), or barcodes for point-of-sale scanning, which require habitualised operation but whose data is also used to control work routines and can be tied to other functions such as automated payment as well as technology to record and analyse consumer behavior (Joerges 1996, 119–144). This perspective brings into focus the genealogy of security technology, the question of innovation contexts, particularly the legitimation of technology-based measures, but also actor networks and actor conflicts in which functionalities, standards and specifications are defined or established. The technologisation of security is thus to be understood as a process of regulating often highly dispersed micropolicies.

The momentum of developments in security technology cannot be understood solely as an effect of 9/11; rather, its genealogy refers to a specific transformation of security policy rationality. Current concern pertains to globally networked flows of goods, resources, money, travel, communications and information, which are considered to be vulnerable and dangerous. An intensification of efforts to monitor and control globalised flows, motivated by security policy, manifested itself as early as the 1980s in the transformation of border controls (Andreas 2003), in the increased surveillance of public spaces, and even more so in the monitoring of globalised data flows. Even before 9/11, references could be found to "societies of control" (Deleuze 1992) and the "surveillance society" (Lyon 2001): "information societies […] are, by the same token, surveillance societies" (ibid., 5). The expansion of (technologised) surveillance is the risk policy equivalent to globalised networking. In a study that has already become a virtual classic, Marx (2002) contrasted traditional forms of social control with new, highly technologised surveillance. Compared to sporadic, more informal control, he describes the new form of technologised surveillance as involving focused observation, sustained visibility and pursuit; this form of control is dedicated, continuous, designed to be systematic and permanent. Observation data is collected and analysed, linked to forecasting and strategic planning—and as a general rule, is based on increasingly concealed and covert monitoring of asymmetric social relationships. Marx is not the only one to regard technological surveillance—whether video surveillance, communications monitoring or biometric data capture—as the expression of a new security policy rationality. Surveillance technology involves a transition from reactive security practices to a more preventive and prospective form of risk management that is interested in strategic information and operates with a generalised suspicion detached from individual cases. The political valency of such forms and practices of collecting and analysing data—such as in the context of telecommunications data retention, airline passenger information, biometric identity documents, dragnet investigations, surveillance of public and semi-private spaces—is ambivalent: on one hand, this establishes surveillance potential and procedures which are traditionally attributable to authoritarian regimes; on the other, "control" for Deleuze (1992), as in the concept of "new surveillance" (Marx 2002), is a "soft" power that is socially widespread and far transcends security aspects. "Control", particularly in the consumer sector, operates less by force and depends more heavily on incentives to collect personal data. "Control" is geared less towards normative discipline than flexible self-adjustment to the expanded boundaries of normality.

Delegating surveillance and control to technology, translating it into technology, first entails reliance on the utility, reliability and functionality of security devices: detection technology can sniff out dangers that would not otherwise be detectable, biometric feature comparisons can deliver far more accurate identification than a border official looking at a passport, the algorithm-based search processes in data mining can plumb communications data for particular criteria far more economically and in some respects with greater validity than would be possible using other methods. And yet more surveillance does not mean more security. Instead, a "dodgy relationship" (Peissl 2003) exists between the two. From a normative theory perspective, this conundrum can be dealt with on multiple levels.

Utility, reliability and functionality first of all mean that technology has inherent functional standards that relate to performance. It is on these that user's trust in technology generally rests: they do not know how things work—they are usually closed to them, a black box—but they have a systematic trust that they will do so (cf. Wagner 1994). However, in terms of security performance, "functionality" is by no means self-evident. For a great deal of technology, when the black box of technical design is opened, security can be deciphered as a paradoxical requirement even at the level of establishing technological standards. Whether detection technology that uses signatures to identify hazardous materials (Ammicht Quinn et al. 2011), or biometric fingerprint, iris or facial recognition through pattern matching (Zureik and Hindle 2004), or even behavioral pattern recognition via data analysis (Aradau and Blanke 2015), the problem widely faced by technology is that of dealing with reliability at the technological standards level in terms of the tension between *false positives* and *false negatives*. Where it is impossible to unambiguously detect materials or identify body characteristics or suspect patterns of behavior, a security economics decision must be made: whether to risk high false negative rates through high specificity, i.e. to risk the possibility of hazardous materials remaining unidentified by detection technology—or to cause high false positives through low specificity, i.e. to cause numerous false alarms, in this case due to supposedly hazardous materials. Even the latter case is generally detrimental to security—leaving aside other costs, particularly economic ones—because a well known result of false alarms is that alarms in general are no longer taken seriously. Despite all the promises of technology, the reliability of a security operation remains uncertain. Moreover, in many contexts it is considered a security risk to declare either false negative or false positive error rates.

Security devices consequently bring with them their own security problems. Taking biometric identity documents as an example, this begins with document counterfeiting safeguards, leading to the problem of readers being outsmarted ("fake fingerprints"), and it could impact the security of databases that store biometric data. And as biometric technology spreads through society—from access controls for high risk facilities to cash payments via fingerprint and even access to our own PCs—identity theft evolves into a widespread security problem (Wichum and Kaufmann 2016). Expressed more generally: first, the variety of functional aspects involving security devices paradoxically creates new forms of insecurity; "the complexity of security" (Rammert 2015: 171) increases on embedding various functions which, in the case of biometric identification, are all oriented towards the norm of posing only as the person you are. Secondly, security is defined differently by various actors. When it comes to the storage of biometric data, for example, it makes a difference whether the data on a biometric identity card or passport is stored in a central database or merely on a chip in the document itself. Storage in a database would create a sort of generalised wanted list which would potentially record everyone and not only the wanted persons. With chip versions, control situations can be installed that leave no data trails. In this context, technical standards govern whether security is interpreted as a strengthening of official surveillance and control options, or—and this is where the concept of "privacy by design" comes in—as protection against it. And it is precisely this that is highly contested on a political level: EU directives, for example, provide for establishment of central databases for biometric passports, while the German judiciary prohibits this. Generally, however, "the social diversity of the actors involved [increases] paradoxical effects" (ibid. 171).

Third, neither the translation of a norm into behavioral regulations nor its usefulness or functionality can be as precisely determined as seems to be the case in the materialization of the standard of driving slowly, in the form of a speed bump. One could call X-ray machines, body scanners, or explosives detectors at airports an almost unmediated transformation of a norm into technology. This transformation functions via a simple algorithm: “Violation of the norm will trigger an alarm.” These security devices are intended to prevent a very specific behavior, namely bringing weapons, objects that could be used as weapons, or substances that could be used to manufacture explosives on board of an aircraft. However, whether they are actually useful for preventing attacks on airplanes or airplane hijackings—and, indeed, whether they are generally a suitable method for fighting terrorism—appears questionable to many critics. In general, these technologies are based on very specific behaviors, however, terrorist activities can change quickly and be highly inventive: it is possible to find ways to outsmart devices and checkpoints, and even if this is unsuccessful, alternative goals can be established. Bruce Schneier brought the concept “security theater” (Schneier 2003, 38 ff.) into the discussion specifically in reference to airport checkpoints that rely on technology. Because the security capabilities of these measures or technologies are tailored so precisely, they serve only to hinder very unlikely incidents, and hardly ever address actual security. Instead, they assuage a feeling of security.

The relationship between surveillance and technology is different in the case of CCTV, which has become almost ubiquitous in semi-public and—in Great Britain, especially—in public areas as well since the 1990s (Hempel and Töpfer 2009). In this case, technical surveillance can only have a preventative function if the camera is noticed by potential perpetrators, causing them to change their behavior because they are being monitored (cf. Norris 2009 on the following). The expected preventative effect is also much less specific than with detection technologies, since they address all types of street-level offences. The overall arrangement of the monitoring system is more heterogeneous, localised, and distributed across social classes than in fairly standardised airport settings—and, moreover, this arrangement cannot be observed by those individuals being monitored by the camera. The arrangement can range from a simple screen to which one or perhaps multiple cameras with fixed directions are connected and provide direct transmission, to a digitized system that may have integrated facial, vehicle, or behavioral pattern recognition systems, may work with zooming or movable cameras, or may be controlled from an operational centre with multiple screens and operators in direct contact with police or first responders. Empirical findings on the preventative effect of CCTV are as diverse as the technical, local, spatial, and organizational settings in which they are used.[9] On a very general level, we can say that they are most successful in parking garages, appear to have essentially no effect on serious offences, especially violent offences, and also have no effect on public disorder offences (Norris 2009, 9–11). A common shift in justifications for such technologies

[9] On the principle difficulties in evaluating the effectiveness of technically-supported security measures to fight criminality and terrorism, see Kreissl et al. (2015), 151–154. This essay also offers an excellent overview of the diversity of surveillance technologies and methods of employing them.

is that, if they do not have a preventative effect, they can be relevant for legal prosecution. Here too, however, we also observe no clear statistical effect indicating that CCTV increases the success rate in solving crimes—not even in street theft (Norris 2009, 11 f.). As significant a reputation as CCTV has across large sections of the European public sphere, there is also data indicating that installing cameras does not increase the feeling of security (ibid. 12 f.).

Another relationship between surveillance and technology is unfolding currently in the area of data analytics processes, as implemented in the passenger pre-screening programmes in the USA and UK.[10] These processes add a new type of engineered prevention—as identified, for instance, by Louise Amoore (2011)—to the security calculus. The goal of these programs is not to enforce norm complying behavior through technical means, as with the other security technologies, nor is it to increase the costs for deviations. Instead, the focus is on eliminating a potential risk—they do not search for terrorists, but rather for individuals who could later prove to be terrorists. These programs are not based around the suspicion aroused by carrying a dangerous object, nor is the purpose to prevent or trace legal violations through observation. Instead, the focus is on predicting who could turn out to be dangerous to public safety in the future. This prediction occurs through associations and through compiling behavioral data gleaned from diverse contexts. This data is irrelevant in and of itself, asserting nothing about normality and deviations, but can trigger alarms through correlations: flying from Islamabad to London, buying a one-way ticket shortly before departure, refusing pork on the plane, etc. The algorithms according to which the calculus operates do not move within the field of the normative, but rather within the field of the possible. And—perhaps their most important feature—they are always subject to change. Calculations differ depending on place, time, and conditions; the programme is continuously modified. Latour's dictum "Technology is society made durable" (Latour 1991) could, in this case, be refined to state "Technology is society made adaptable." At least, this is the technically implemented expectation whose "counterterrorism effectiveness" measures itself based on the impossible statistical evidence of a "symbolic importance of claims and prevailing standards of modern rationality" (Hegemann and Kahl 2015, 199).

The implementation of security technologies for monitoring and other associated practices is—at least tendentially—registered as a violation of norms. The public/private balance is evidently shifting (Solove 2006). In 2007, the then German Federal Commissioner for Data Protection wrote—as had many before and as have many after him—of the "end of the private sphere" (Schaar 2007). There is fear of adjustments to social behavior resulting from the so-called "chilling effect," which would lead to normalization, conformity, avoidance, and dispensing with political freedoms. The capacities resulting from information technology are associated with wholly new forms of categorization. Social sorting, and categorical suspicion in the security field, lead to an increase in marginalization and exclusion (Lyon 2003a). Both categorizations also affect fundamental values of the democratic state

[10] The findings could apply in a similar manner to the prevention exercised by "predictive policing," which is focused more on spatial considerations than personal ones.

(Haggerty and Samatas 2010). Depending on the technology, these interventions can be focused on a variety of different levels: body scanners that react to body implants represent an entirely different type of injury than pre-screening behaviors, whose false positives land on no-flight lists or find themselves unable to open a bank account. In the fight against crime and terrorism, both the usefulness of security devices and their costs are contentious—and the effectiveness of both is proven only through anecdotal evidence.[11] “Whereas”—as Kreissl et al. (2015, 150) put it—“the critics taking a rights perspective point to the dangers that go along with new surveillance practices […], the supporters take a threat-based position, pointing to the damage caused by criminal or terrorist activities and the need to do whatever is technologically possible to prevent, detect or deter such activities.” However, this stance seems to mask a second contradiction: the purpose of technology is to achieve control over a situation. It is not possible to use them to enact prevention in the sense of a way to deal with the causes of behavior. In consequence of this, another key question is where one can best concentrate investments to fight terrorism and criminality.

3 On the Praxeology of Civil Security: Heterogeneous Methods of Utilisation and the Pitfalls of Technologisation

Technologies—and this is true for security devices as well—are only partially defined by the expectations and norms inscribed on them. Theories of technology, in particular those influenced by a cognitive-sociological or “cultural studies” perspective, that consider the genealogy, diffusion, and embeddedness in everyday life of bicycles, telecommunication technologies, automobiles, washing machines, and other objects (Hörning 1989; Bijker and Law 1992) emphasise this. They remind us that the technical potential for action possessed by an object is only realized through its use. During use, it becomes clear that technologies are always more or less open to context-specific adaptations. Frequently, they require more specific contextual embedding and variations in design. Moreover, technologies are appropriated by users, and in some cases by those whom they are used to monitor. The handling of technologies is frequently shaped by stubbornly heterogeneous appropriations, whereat appropriation can also refer to an explicit rejection. Even security devices hardly provide a full definition of the process of a security practice, not even in situations where they are embedded in very narrowly defined procedures, such as in baggage screening at the airport. Security devices are frequently utilised in heterogeneous ways on different hierarchical levels. One should expect not only resistance from affected parties, and counter-strategic ways of handling and using the technologies from monitored individuals, but also willful and deviant uses of technologies by officers themselves. If we do not reflect on the technology, but rather observe technologised practices for ensuring security, we observe more than just the creative ways users handle these objects. Instead, we also

[11] For more on these conflicting constellations, also see the article by Ralf Poscher in this edition.

observe unexpected and unintended, often entirely counterproductive effects (on the following, also cf. Amicelle et al. 2015).

Resistances and counterstrategies against state or other forms of organized surveillance are not rare. Besides legal and institutional prohibitions and restrictions of use, we often find organized protests by interest groups, social movements, or NGOs against the use of specific technologies or procedures. Such protests succeeded, for instance, in making the original version of the "full body scanner" appear scandalous, thereby gaining influence on the technological design of such terahertz detectors (cf. Bennett 2012). Even everyday counter practices against surveillance and monitoring are highly diverse: hidden surveillance practices may be uncovered, for instance in businesses or public spaces, or—certainly less an everyday practice—when Edward Snowden revealed the practices of the NSA; monitored areas may be avoided, which may be the result of a common chilling effect, but is also a counterstrategy of criminals that leads to a shift in areas where criminality takes place; one can blind technologies; for instance blocking facial recognition technology through specific trendy styling; one may hide identities f.e. by hiding of IP addresses; one may encrypt communications; one may prevent GPS locating by turning off a cell phone; one may destroy security devices, such as CCTV-cameras; or one may move into counter-surveillance, f.e. when demonstrators monitor police movements using drones (Gilliom and Monahan 2012).

This type of technologisation often says little about what kind of threat is being observed, who counts as a threatening individual, and whose security is in focus. F.e., constellations, actors' understanding of their tasks, and operating methods can be completely different when using CCTV (cf. Kammerer 2008, 143–226; Smith 2009): it is possible to use CCTV to pursue every violation of public order, no matter how small, but it is also possible to use it to accompany young people on their way home in the evening, with a protective intention. Ways these technologies are used may be determined through high-level regulation and supervision. However, even actors in security positions frequently display a surprisingly large amount of leeway in how they handle technology while completing their daily work. Only rarely are processes and procedures strictly determined by technologisation. The power of the individuals behind those screens to define their meaning should not be underestimated in many cases. To a great extent, this results from the fact that CCTV creates anonymous and entirely asymmetrical surveillance conditions, which is associated with a relative lack of responsibility for observers. Operators determine how suspicion is constructed by selectively directing their attention, which often follows stereotypical definitions; they make decisions on which suspicious moments to pass on, and their observations, recordings, and statements frequently lead to the arrests of individuals and are relevant to court proceedings. At least in a rudimentary manner, even operators can control threat estimations at the airport during automated physical checks for weapons or explosives. The detecting machines themselves don't check persons, but rather only whether persons may be carrying something that is not allowed and—at least this is what the technology is designed for—trigger an alarm only if the findings are positive. They thus spread suspicion equally over everybody refraining from the individuality of a person. In a certain way, they operate as "democratic machines" (Linhardt 2000). Nevertheless, operators also follow their own intuition in creating suspicion when they purposefully trigger false alarms (Lucchesi 2011, 10 f.). This behavior reverses the logic of the suspicion created by the machine. The legitimacy of any potential categorical suspicion is increased by being linked to the machine alarm. Another type of reversal takes place with CCTV operators when, out of a sense of class solidarity, they do not watch workers to stop them from stealing, but rather ignore a worker's violation and choose to turn the cameras on the executives instead. Especially with CCTV, there are multiple ways to adapt the security devices to one's own purposes: landscapes may be observed, voyeuristic purposes pursued, entertaining happenings investigated, etc.

Currently, technologisation almost always means digitalization. No matter what kind of devices are developed and used, at the end of the day these almost always produce digitized data that can be collected, saved, and evaluated in a databank. Operations that convey data produce their own effects, that can often modify organizational, contractual, or role-specific manners of operating in unforeseeable ways. One effect of data-based operations is that even the operations of security actors are increasingly registered through data and through technological means, potentially making them transparent. One example of this is body cameras, which are being tested and used by police units in the USA and UK, and which are already soon to be introduced by a variety of German state police forces. These cameras make clear how such transparency can change police work. In an opinion by US agencies (Miller et al. 2014), the first listed "benefit" of such cameras is "accountability and transparency," understood specifically in relation to complaints and as a way to solve "officer-involved incidents." The entire tone is focused primarily on protecting citizens from police despotism. One significant moment is in the monitoring of police officers by their supervisors. Officers do actually report that camera recordings lead to an increase in self-control (cf. Tanner and Meyer 2015, 394f). At the same time, they see the body cam as a tool to counteract recordings of police actions by citizens with mobile phone cameras by recording their own perspectives. Self-discipline is another effect that overlaps with the behavior of citizens—aggressive behavior is said to decrease while the camera is running.[12] Formalization, compliance with regulations, and objectification of police work are effects of mobile information technology, of which mobile digital terminals and associated decision support systems are increasingly a part.[13] Besides numerous other non-intended effects resulting from a movement to mobile networks—such as conflicts of authority when digital skills and service experiences contradict one another; a lack of back-up competence, when the systems fail—one central problem is that the boundaries between formal and informal communication are shifting.

[12] In Germany, the introduction is justified by saying that there are many cases of resistance to state authority and many cases of crimes against police officers.

[13] Cf. Tanner and Meyer (2015) on the following observations. They also refer to my own research project in the EU Security Research Program (Besecure, GA 285222), under which a decision management tool for urban criminal prevention was supposed to be developed. Structurally similar problems and concerns from actors were evident in another research project in the area of civil security, which was focused on the introduction of digital recording and decision support systems for emergencies in search and rescue (cf. Ellebrecht and Kaufmann 2014).

Informal communication is indispensable for police work in many situations. Confidential information, simple small talk as a part of community policing, and victim statements in sensitive cases are not compatible with automated camera recording. Internal information is also dependent on informal communication: information on suspects, for instance, such as who was recently released from prison, is given an entirely different significance depending on if it is transferred orally to a colleague or entered in writing in a databank. Often, relevant informational chains and channels may cease to exist during these kinds of shifts because they do not show up in process diagrams. Increasingly data-based communication also endangers the transmission of knowledge and experience. Ultimately, some police officers see the new technologies as ushering in a radical break: "Not only has technology thus destabilized the authority of elder officers, some of them also see it as being at the root of dehumanization. In their opinion, portable devices 'distract' younger officers and make them forget that most police work takes place under the eyes of both other professionals and the public" (Tanner and Meyer 2015, 391).

Amicelle et al. (2015, 301) derives consequences related to the politics of power from such observations, by pointing out that (security) devices only sometimes serve to prop up asymmetrical power relations in the long term; instead, their role is also always contested and dependent upon interpretation: "… socio-technical devices do not just contribute to (re)organizing relations between the 'state' and the ultimate 'targets' […] Their introduction also impacts power relationships within a hierarchically organized body […], as well as between political authorities and the myriad actors in charge of implementing those policies".

4 On the Praxeology of Civil Security: Hybrid Actors

We can understand security practices as associations between heterogeneous elements which are both technical and non-technical in nature. However, we can also understand elements associated in active practice as a new kind of hybrid actor. This is the dual meaning of the term actor network: "An actor-network is simultaneously an actor whose activity is networking heterogeneous elements and a network that is able to redefine and transform what it is made of" (Callon 1987, 93).[14] Bruno Latour expressed this in several significant examples, for instance when he says that neither people nor airplanes fly; instead, the attribute of a whole association of elements is what flies, including airports, aviation law, air traffic controllers, ticket windows, etc.: "B52s do not fly, the U.S. Air Force flies" (Latour 1994, 35). This applies not only to the level of actors in a corporation, but also to the discussion on weapons bans—do weapons kill, as critics of US weapons legislation maintain, or does the responsibility lie solely with the citizens who use them, as the weapons lobby suggests?—it may not be possible to come down on one side or the other, since the citizen with a weapon is a new actor (ibid. 30–36). The trick in this type of reflection is that one cannot assume that equipping, for instance, the secret

[14] Here, cf. also the lucid discussion in Schulz-Schaeffer (2008).

service or the border police with a new surveillance arsenal does nothing but give them new tools to work with. This is also how internal police criticism responded to the digitalization of their work: just as the association of unarmed police with those armed with machine guns constitute totally different kinds of police and police work, with new technologies not only the forms of reconnaissance, but also the external and internal self-perception of actors changes, as well as the framework conditions for their activities and the strategies and tactics by which they operate.

The example of border control in the EU shows how heterogeneous arrangements of groups working on border security and the handling of new technologies can be associated with a changed understanding of border security. We can differentiate between three different "hybrid actors" in border control: military, police, and data-analytic actors.[15] The military dimension of security management is associated with the practice of patrolling, of directly monitoring the border area. Border security is understood primarily as the task of discovering and preventing a potential penetration into one's own territory. Even if official EU papers still frequently speak of a "fight against illegal migration" or "a fight against organized crime" that takes place on the border (Carrera 2007), within EU border policing institutions—according to Bigo (2014)—talk of a "fight," a war, or even a clash of civilizations in the sense of Huntington is rare. Overall, a military understanding of border security plays only a subordinate role. However, practices based on military border security play an important role within the framework of EUROSUR (European border surveillance system) and its Spanish predecessor project SIVE (Sistema Integrado de Vigilancia Exterior). The mode of military surveillance that comes into play with these systems is displayed first in an understanding of space. Surveillance is no longer focused on the line of the border itself, but is rather shifted far beyond the border. The goal is to seal off "green" and "blue" borders, monitor border traffic far in advance of the border, and intervene as early as possible when necessary; in the case of the Mediterranean Sea, even close to the coasts of northern African states. EUROSUR and SIVE are, then, based to a great extent on technical components that could be ranked among high-end military technology: Reconnaissance units with high-power radar, infrared and video cameras with residual light amplifiers, mobile and stationary communication units with real time imagery, satellite and drone reconnaissance. The technology and operating methods of EUROSUR or SIVE correspond to those of military reconnaissance units associated with mobile forces. SIVE is—and this may be paradigmatic for its type of operations—managed by the Guardia Civil, an organization with a paramilitary character that was designed not for passport checks but for special operations in small units targeted at fighting infiltration, militant resistance, and domestic unrest—and that was not entrusted with protecting the border until the 1990s. The border police today doesn't wait at the border to catch potential border crossers; instead, it is moving towards more flexible border security tactics. However, in interview statements by European border officials, the military option is rarely

[15] I am basing my remarks primarily on the analysis of Bigo (2014), but shifting the conceptual direction slightly by employing my own work (Kaufmann 2006, 2008). Bigo works conceptually with the primacy of practical sense, which also controls the selection of technology. The concept of the "hybrid actor," on the other hand, leaves open the question of the primary forces that combine in the practices.

associated with coercive action. Not war, but rather the necessity of maintaining international order, stopping a chaotic river of people, justifies their actions. Border control is focused on containment and action of deterrence, which may indeed mean long-term confinement to border camps.

The core of border police practice, as described in the concept of open and secure borders by the Integrated Border Management, is the screening of legal and illegal. Border management works based on a kind of legal decision that, ultimately, boils down to a consideration of individual cases: who entered in a forbidden manner, who is carrying forbidden or dangerous objects. In this case, reconnaissance operates using entirely different technologies focused not on territory surveillance, but on determining the identities of persons and transported goods. These technologies are grouped on the one hand around the hermeneutics of creating suspicion and of identification. This includes the experience of the officer, who attempts to make an assessment of the truth of claimed identities based on categorical attributions, an interpretation of facial expressions, body language, health, clothing, behavioral patterns, and involuntary physical expressions, or attempts to ferret out prohibited goods individuals are carrying (Salter 2006). The ability to discover illegal actions is attributed to many years of experience, and is described by officers themselves as an art. On the other hand, this procedure is surrounded by an apparatus to detect dangerous items and goods, as well as a broad and branching apparatus to collect, save, and process biometric data: EURODAC (European Dactyloscopy), to save fingerprints of migrants or refugees and compare them with existing data, VIS (Visa Information System), to determine potential falsified visas, SISII (Schengen Information System II), to make comparisons with the directory of wanted persons. The spatial configuration associated with such practices of surveillance is encoded entirely differently than thinking of clearly marked borders. Instead, space and borders are thought of in networked constellations: surveillance follows the paths of migrants, links itself to streams of people and goods, attempts to block or regulate paths of origin by encouraging source countries to engage in exit checks; however, it also operates at hub points—such as train stations, highways, airports—inside the EU and in individual countries. Border controls are almost ubiquitous. The border is becoming liquid. Border management takes its justification from a liberal economy, which wants borders to be both held open and kept secure. Security is associated with a risk assessment that knows how to assess and react to a shift in directions, threat dimensions, and the quantities of incoming streams of goods, people, and money.

"Military" and "police" border security is based on entirely different routines and self-conceptions; it has a different understanding of what border security means and privileges different methodologies. On the one hand, it stems streams of people and goods and seals off areas, and on the other hand keeps streams of goods and people open, ensuring they are properly channeled and regulated. Maintaining order on the one hand, regulating streams, and adapting to changing risks on the other represent contrary foundations for legitimation. Bigo also sees a third dimension for managing border security: it comes from the practice of data analysis, as described, for instance, in the case of the passenger pre-screening programme. This data analysis, to name just one moment, radicalises the risk calculus. It can function even without seeing the person itself: "They [the data analysts] regulate the control of mobility according to these profiles and independently of an examination of the body of the person" (Bigo 2014, 218). Their individually tailored profiling, which decides who may pass without a check and who may not pass, as a potential (future) threat, makes a shift away from confirmative and towards explorative knowledge generation (Leese 2014). This is only successful, however, because the basis for the decisions of border officials, namely their "prejudices, their intuitions, sensibilities and dispositions, are concealed in the glossy technoscientific gleam of the risk-based solution" (Amoore 2011, 38).

5 Conclusion: Technology as a Societal Framework

Security devices function as a normative way to harden societies. At the same time, their use triggers the potential for action, bringing about opportunities to adjust, bend, and deactivate rules, and may have unintended consequences. Furthermore, we must consider that security devices can also be an essential component of group-specific self-understanding and external understanding and of radically changed practices. Bernward Joerges captured another manner in which technology functions with the metaphor of "Technology as the body of the society" (Joerges 1996); Bruno Latour speaks of "interobjectivity" (Latour 1996). Material technology functions as a constitutive framework that lends social processes and forms what stability, permanence, and specific formats they do have. On the level of social theory, this is currently reflected in concepts such as the "information age" and "network society" (Castells 1998) in view of the entire complex of technologies; applied to security theory, it is found in the concern over the vulnerability of "critical infrastructures" and "vital systems," as well as in the fact that the expansion of technologised, especially digitized forms of surveillance and monitoring into all areas of our lives means that the diagnosis of ours as a "surveillance society" (Lyon 2001) finds wide resonance.

The dominant social form of this surveillance is generally described using the term assemblage (Haggerty and Ericson 2000). This term refers to the fact that this is in no way a controlled, centralized flow of activities. An assemblage does not stand for a sovereign power and monitoring, but rather for a framework of scattered, discrete forms of monitoring and surveillance. An assemblage describes the parallel and combined functioning of numerous practices to monitor and observe streams of goods, resources, finances, travel, communication, and information. This type of surveillance framework is motivated by numerous forces: as the desire for profit, entertainment, control and—although this is only one element— a desire for security. Therefore, surveillance spreads in a rhizomatic fashion; it proliferates through the society in a fragmented manner. Security practices constitute just one—more or less—discrete moment of monitoring and surveillance. Currently—and this marks what is technical about these practices—monitoring and surveillance primarily functions based on digital technologies; it works based on the fact that nearly all flows are reflected in data, and that the individual is transformed into a "dividuum" split into a physical being and a "data double," as Haggerty/Ericson write with reference to Gilles Deleuze.

Under these conditions, constellations of power are increasingly configured using asymmetrical regulations surrounding the data double, asymmetries in the compilation of data, and in knowledge of which data exists on individuals, in which contexts this data is used (or may or can be used) or not used. The analysis of such constellations of power—and ultimately the societal discussion surrounding these as well—is focused on the level of basic "technical" standards that can make the power political content of technical configurations visible on the micro-level as the conceptual translation of social norms into technical norms. As we have seen, translating "security" into technology is a dodgy endeavor: At the micro level risks between producing too many false positives or to many false negatives have to be balanced; there is the question whose security is enhanced through specific technologies or through their specific design—and who in consequence might become more vulnerable; evidence that security measures work is hard to obtain and sometimes doubtful; and—last but not least—security devices do not address root causes for deviant behavior. Assemblage also means that surveillance and control can be observed in more contexts than just a top-down mode. Instead, we observe diverse practices, strategies, and battles surrounding monitoring and surveillance, and surrounding security devices and their deployment. Power relations translate into diverse twists and turns. Ultimately, one effect of the dominant technical framing is that control and surveillance are currently increasingly occurring under the primacy of "dataveillance" as surveillance and control of the data double. If assemblage is understood as the framework of discrete forms of monitoring, then configurations that compile data collected and processed intermittently in multiple fields stand out. Control, more in the form of authoritarian force, emanates from a centralized, opaque "apparatus" (Lyon 2003b), which acquires data from scattered collections. Its calculus would follow a logic of pre-emption, which operates *only* in the name of stopping a potential catastrophic future—and that could reject responsibility for decisions by specifying that decisions were to be made based on "technologically" generated knowledge. Uncertainty would become a general foundation for governance (Aradau and van Munster 2007). However, current governance in the name of security seems to be characterized more by the concept of the assemblage. Assemblage means that, as in the case of border security, various modes of governing occur in parallel, sometimes in complementary and sometimes in conflicting forms: security practices are undertaken in the mode of military and disciplinary access, in the mode of legally oriented police work, and in the mode of preventing and pre-empting political risks. In any case, under the conditions of dataveillance, under which surveillance—at least in Western societies—tends to become ubiquitous, and which is also oriented around an unknown yet potential catastrophic future, "the central point is that technologies of security produces ontologies of insecurity" (Smith 2009, 145).

References

Amicelle A, Aradau C, Jeandesboz J (2015) Questioning security devices: performativity, resistance, politics. Secur Dialogue 46(4):293–306

Ammicht Quinn R, Rampp B, Wolkenstein A (2011) An ethics of body scanners: requirements and future challenges from an ethical point of view. In: Wikner D, Luukanen AR (eds) Passive millimeter wave imagining technology XIV. SPIE Proceedings, vol 8022

Amoore L (2011) Data derivatives. On the emergence of a security risk calculus for our times. Theory, Cult Soc 28(6):24–43

Andreas P (2003) Redrawing the line. Borders and security in the twenty-first-century. Int Secur 28(2):78–111

Aradau C, Blanke T (2015) The (Big) data-security assemblage: knowledge and critique. Big Data Soc 1(2):1–12

Aradau C, van Munster R (2007) Governing terrorism through risk. Taking precaution, (un)knowing the future. Eur J Int Relat 13(1):89–115

Bennett CJ (2012) Privacy advocates, privacy advocacy and the surveillance society. In: Ball K, Haggerty K, Lyon D (eds) Routledge handbook of surveillance studies. Routledge, New York, pp 412–419

Bigo D (2014) The (In)securitization practices of the three universes of EU border control: military/Navy-border guards/police—data analysts. Secur Dialogue 45(3):209–225

Bijker WE, Law, J (eds) (1992) Shaping technology, building society. Studies in Sociotechnical Change. MIT Press, Cambridge

Callon M (1987) Society in the making: the study of technology as a tool for sociological analysis. In: Bijker W, Hughes T, Pinch T (eds) The social construction of technological systems. MIT Press, Cambridge, pp 82–103

Carrera S (2007) The EU border management strategy: frontex and the challenges of irregular immigration in the Canary Islands. CEPS Working Document 261

Castells M (1998) The rise of the network society. The information age: economy, society, and culture, vol I. Blackwell, Malden

Deleuze J (1992) Postscript on the societies of control. In: October 59, pp 3–7

Dombrowsky WR (2012) Sicherheit zwischen Dysplasie und Unentscheidbarkeit. In: Gerhold L, Schiller J (eds) Perspektiven der Sicherheitsforschung: Beiträge aus dem Forschungsforum Öffentliche Sicherheit. Peter Lang, Frankfurt am Main, pp 27–40

EU-Commission (2012) Security Industrial Policy. Commission Staff Working Paper. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012SC0233. Accessed 15 Nov 2015

Ellebrecht N, Kaufmann S (2014) Boosting efficiency through the use of IT? Reconfiguring the management of mass casualty incidents in Germany. Int J Inf Syst Crisis Response Manag 6(4):1–18

Gilliom J, Monahan T (2012) Everyday resistance. In: Ball K, Haggerty K, Lyon D (eds) Routledge handbook of surveillance studies. Routledge, New York, pp 405–411

Gummer CS, Skrzypietz T, Stuchtey TH (2014) Die Sicherheitswirtschaft in Deutschland—Marktstrukturerhebung von Unternehmen in einem Wachstumsmarkt, Potsdam. http://www.bigs-potsdam.org/images/Studien/Studie%20WISIND%202.%20Ergebnisbericht%20Druckversion.pdf. Accessed 15 Nov 2015

Haggerty KD, Ericson RV (2000) The surveillant assemblage. Br J Sociol 51(4):605–622

Haggerty KD, Samatas M (eds) (2010) Surveillance and democracy. Routledge, Oxon

Hayes B (2009) NeoConOpticon. The EU-Industrial-Complex. Statewatch. http://www.statewatch.org/analyses/neoconopticon-report.pdf. Accessed 15 Nov 2015

Hegemann H, Kahl M (2015) Constructions of effectiveness and the rationalization of counterterrorism policy: the case of biometric passports. Stud Confl Terror 38(3):199–218

Hempel L, Töpfer E (2009) The Surveillance Consensus: reviewing the politics of CCTV in three European countries. Eur J Criminol 6(2):157–177

Hoijtink M (2014) Capitalizing on emergence: the 'new' civil security market in Europe. Secur Dialogue 45(5):458–475

Hörning KH (1989) Vom Umgang mit den Dingen. Eine techniksoziologische Zuspitzung. In: Weingart P (ed) Technik als sozialer Prozeß. Suhrkamp, Frankfurt/M, pp 90–127

Joerges B (1996) Technik—Körper der Gesellschaft. Suhrkamp, Frankfurt am Main

Kammerer D (2008) Bilder der Überwachung. Suhrkamp, Frankfurt am Main

Kaufmann S (2006) Grenzregimes im Zeitalter globaler Netzwerke. In: Berking H (ed) Die Macht des Lokalen in einer Welt ohne Grenzen. Campus, Frankfurt, New York, pp 32–65

Kaufmann S (2008) Technik als Politik. Zur Transformation gegenwärtiger Grenzregimes der EU. Comparativ. Zeitschrift für Globalgeschichte und vergleichende Gesellschaftsforschung 18(1):42–57

Kreissl R et al (2015) Surveillance: preventing and detecting crime and terrorism. In: Wright D, Kreissl R (eds) Surveillance in Europe. Routledge, London, pp 150–210

Latour B (1994) On technical mediation—philosophy, sociology, genealogy. Common Knowl 3(2):29–64

Latour B (1991) Technology is society made durable. In: Law J (ed) A sociology of monsters essays on power, technology and domination, sociological review monograph No 38, pp 103–132

Latour B (1996) On interobjectivity. Mind Cult Act 3(4):228–245

Leese M (2014) The new profiling: algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. Secur Dialogue 45(5):494–511

Linhardt D (2000) Demokratische Maschinen? Die Vorrichtung zur Terrorismusbekämpfung in einem französischen Großflughafen (Paris-Orly). Kriminologisches J 32(2):82–107

Lucchesi A (2011) Die Bombe is eh im Koffer. Geschichten aus dem Handgepäck. Heyne, München

Lyon D (2003b) Surveillance after September 11. University Press, Cambridge

Lyon D (2001) Surveillance Society. Monitoring everyday life. Open University Press, Buckingham (Philadelphia)

Lyon D (2003a) (ed) Surveillance as social sorting. Privacy, risk, and digital discrimination. Routledge, London, New York

Marx GT (2002) What's new about the "new surveillance"? Classifying for change and continuity. Surveill Soc 1(1):9–29

Marx K (1984/1867) Das Kapital. Kritik der politischen Ökonomie (MEW Vol. 23). Dietz Verlag, Berlin

Miller L, Toliver J, Police Executive Research Forum (2014) Implementing a body-worn camera program: recommendations and lessons learned. Office of Community Oriented Policing Services, Washington DC

Norris C (2009) A Review of the increase use of CCTV and video-surveillance for crime prevention purposes. EU Citizens' Rights and Constitutional Affairs. PE 419.588

Peissl W (2003) Surveillance and security. A dodgy relationship. J Conting Crisis Manag 11(1):19–24

Rammert W (2015) Unsicherheit trotz Sicherheitstechnik? Das Kreuz mit komplexen Konstellationen. In: Zoche P, Kaufmann S, Arnold H (eds) Sichere Zeiten? Gesellschaftliche Dimensionen der Sicherheitsforschung. LIT-verlag, Berlin, pp 155–182

Salter MB (2006) The global visa regime and the political technologies of the international self: borders, bodies, biopolitics. Altern Glob Local Polit 31(2):167–189

Schaar P (2007) Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft. Bertelsmann, München

Schneier B (2003) Beyond fear: thinking sensibly about security in an uncertain world. Springer, New York

Schulz-Schaeffer I (2008) Technik in heterogener Assoziation. Vier Konzeptionen der gesellschaftlichen Wirksamkeit von Technik in Latours Werk. In: Kneer G, Schroer M, Schüttpelz E (eds) Bruno Latours Kollektive. Kontroversen zur Entgrenzung des Sozialen. Suhrkamp, Frankfurt am Main, pp 108–152

Smith GJD (2009) Empowered watchers or disempowered workers? The ambiguities of power within technologies of security. In: Aas KF, Gundhus H, Oppen Mork, Lomell H (eds) Technologies of (In)security. The surveillance of everyday life. Routledge, New York, pp 125–146

Solove DJ (2006) A taxonomy of privacy. Univ Pa Law Rev 154(3):477–564

Tanner S, Meyer M (2015) Police work and new 'security devices': a tale from the beat. Secur Dialogue 46(4):384–400

VDI/VDE Innovation und Technik, Arbeitsgemeinschaft für Sicherheit der Wirtschaft (2009) Marktpotenzial von Sicherheitstechnologien und Sicherheitsdienstleistungen. Der Markt für Sicherheitstechnologien in Deutschland und Europa—Wachstumsperspektiven und Marktchancen für deutsche Unternehmen. Schlussbericht. Berlin http://www.vdivde-it.de/publikationen/studien/marktpotenzial-von-sicherheitstechnologien-und-sicherheitsdienstleistungen. Accessed 12 Apr 2015

Wagner G (1994) Vertrauen in Technik. Zeitschrift für Soziologie 32(2):145–157

Wichum R, Kaufmann S (2016) Die Technisierung der Sicherheitsproduktion und ihre Ambivalenzen—das Beispiel biometrischer Identifikation. In: Haverkamp R, Arnold H (eds) Sicherheitsempfinden in Deutschland **(in print)**

Zureik E, Hindle K (2004) Governance, security and technology. The case of biometics. Stud Polit Econ 73:113–137