Privacy self-regulation through awareness?

A critical investigation into the market structure of the security field.

Carla Ilten, Daniel Guagnin, Leon Hempel

Technische Universität Berlin / Zentrum Technik und Gesellschaft (ZTG)

Document for final submission

1 Introduction.

This paper aims to provide a critical contribution to the ongoing discourse on self-regulation with regard to privacy and data protection.[1] This discourse encompasses the amendment of the EU Data Protection Directive and the related discussion about a principle of accountability.[2] Underlying these conceptualisations is the assumption that data protection law is generally observed, but could be simplified and even reduced in favour of more self-regulatory approaches which are deemed more efficient.
We would like to raise critical questions about the institutional conditions and frameworks that greatly influence data controllers' potential and motivation for enacting privacy awareness and self-regulation; in other words, the market structures that these organisations operate within. An investigation into organisations' practices is indispensable in order to evaluate these current claims for self-regulation and to lay out the conditions that need to be met if market forces are to be harnessed for privacy and data protection.
The results and conclusions presented were gained in the course of the EU FP7 project "Privacy Awareness through Security Organisation Branding" (PATS). The project inquires into the possibilities of organisational self-regulation in the field of security technology and services by means of branding – understood as a complex, two-sided communication process between companies and stakeholders.[3] Specifically, research from the first three work packages is used. We started out with an analysis of current security regimes and actors, then interviewed representatives of security organisations in detail about their privacy awareness and practice, as well as conducting a qualitative analysis of security organisations' communications and self-presentations.
The security field can be used as a burning lens to focus particular problems when it comes to the self-regulation of privacy and data protection: while the industry certainly represents a particular case when it comes to actor relationships, our analysis shows which questions need to be asked in order to understand existing structures of, and obstacles to, privacy protection. We argue that powerful obstacles lie in market structures that are obscure rather than a provider of incentives for self-regulation. These findings facilitate

---

1 cf. e.g. European Commission, "Communication from the Commission to the European Parliament, the Council, the Economic and Social committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union," (Brussels: European Commission, 2010). Accessed: 20.7.2011, http://ec.europa.eu/health/data_collection/docs/com_2010_0609_en.pdf

2 cf. Article 29 Working Party, „Opinion 3/2010 on the principle of accountability," (Brussels: Article 29 Working Party, 2010). Accessed 28.7.2011, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf

3 The PATS project is funded from 2009 to 2012 and involves partners from Germany, the UK, the US, Poland, Israel and Finland. The findings presented here are mainly based on the outcomes of the German team. The project website can be found at www.pats-project.eu

further thought about a principle of accountability with regard to the governance of privacy in different industries dealing with (personal) data. It is not enough to look at legal provisions and privacy statements when we want to assess the state of "health" of privacy and data protection in the EU – we need a thorough examination of the patient.

1.1 Security regimes

The first work package was a research journey of all involved project partners into their respective national empirical fields: mapping the security regimes along the concepts of actors, technology and discourses. For this, we gathered on the one hand quantitative data about the security industry market and developed different qualitative types of security organisations; on the other hand we made a literature review of documents and articles about the development of the security field between 1989 and 2009. This section gives an account of the more general trends we have observed and which focus on the current debate surrounding the regulation of privacy in this sector.

1.2 Securitisation

Several discourses on security were identified during our research of current security regimes. A powerful, but creeping discourse concerns the broadening of security both as a term and as a political task. This development has been labelled "securitisation" in the academic discourse and has at the political realm enabled shifts in competences and power.[4] Security is seen as a cross-cutting political issue that needs to be ensured in virtually every social sphere. The notion of a "right to security" propels the pursuit of security to a number one responsibility for the state.[5] In Germany, this discourse was first associated with criminal theory but has been utilised by political interests of power extension and centralisation.[6] Under the title of "security vs. freedom", the shift of the political norm towards measures of securitisation has been discussed and the considerably weakened position of privacy values and other liberties observed[7].
The most unquestioned discourse about "new threats" originated in the political realm and is tightly coupled to processes of globalisation and allegedly new forms of war after the end of the Cold War. This discourse has global scope and is taken up by both political and economic actors, especially after 9/11. It is a powerful narrative and justification for securitisation processes in the US, but in most other countries analysed as well.[8]
Another manifestation of the extension of the security notion can be identified in what we called the "network paradigm". Originally coined and used by social scientists in response to socio-technical developments, the "network" term has seen a career beyond compare. It has been appropriated by many scientific communities dealing with organisational structures, politics and economic developments. Management literature has happily taken up the term, and it has become most common in describing social relations. Rooted in the fascination about the Internet and networking technologies in general, the term "network" could be translated with "up to date" or even "futurist". The discourse is used by many, if not all of the actors dealt with here. Yet, it proves most useful to those already most competent when it comes to networking: the companies we have identified as *Systems Integrators* in a security actors typology.

---

4 cf. Barry Buzan, Ole Waever, and Jaap de Wilde, *Security: a new framework for analysis (*Boulder, CO.: Lynne Rienner Pub., 1998). For the German security regime, see also Hans-Jürgen Lange, H. Peter Ohly, and Jo Reichertz, *Auf der Suche nach neuer Sicherheit: Fakten, Theorien und Folgen* (2nd ed. Vs Verlag, 2009) and Tobias Singelnstein and Peer Stolle, *Die Sicherheitsgesellschaft. Soziale Kontrolle im 21. Jahrhundert* (VS Verlag fuer Sozialwissenschaften, 2006)

5 Josef Isensee, Das Grundrecht auf Sicherheit. Zu den Schutzpflichten des freiheitlichen Verfassungsstaates (Berlin: Walter de Gruyter, 1983)

6 cf. Heiner Busch, "Kein Mangel an Sicherheitsgesetzen." *FriedensForum*, 2008. Accessed: 30.7.2011 http://www.friedenskooperative.de/ff/ff08/6-61.htm;
Hans-Jürgen Lange and H. Peter Frevel. "Innere Sicherheit im Bund, in den Ländern und in den Kommunen," in *Auf der Suche nach neuer Sicherheit: Fakten, Theorien und Folgen* (VS Verlag, 2009)

7 Stephan Heinrich and Hans-Jürgen Lange,"Erweiterung des Sicherheitsbegriffs," in *Auf der Suche nach neuer Sicherheit: Fakten, Theorien und Folgen* (Vs Verlag, 2009)

8 cf. e.g. David Lyon, "9/11, Synopticon, and Scopophilia: Watching and Being Watched," in *The New Politics of Surveillance and Visibility.* Haggerty, Kevin. D. and Ricard V. Ericson, eds. (Toronto: University of Toronto Press, 2006) and Sebastian Bukow, "Deutschland: Mit Sicherheit weniger Freiheit über den Umweg Europa," in *Europäisierung der inneren Sicherheit*, edited by Gert-Joachim Glaeßner and Astrid Lorenz (Wiesbaden: VS Verlag, 2005), 43-62.

The network paradigm and the rhetoric of "new threats" are tightly coupled: The dissolution of borders, globalisation, new types of conflict or war have been bundled into one image by the 9/11 terrorist attacks in the USA. This focus event, singularly witnessed by millions through extensive media coverage, is probably present before everyone's eyes when "new threats" are mentioned, also in Germany. The invention of the term "Homeland Security" by the US government in the aftermath of the attacks and the instalment of a powerful institution of the same name is the consequence of the "new threat" discourse as well as a medium for safety and security convergence. The Homeland Security department is not only responsible for "Counterterrorism", "Preparedness, Response, Recovery", but also for "Border Security" and "Immigration". It thus includes safety from natural disasters in its security mission and subsumes immigration under the security aspect.
A similar development can be shown for Germany long before the attacks took place. The understanding of security had undergone a process of broadening for some two decades. The roots of this shift lie in the military and security political discussion that has seen a merge in internal and foreign security. As an early focus event, the Schengen Agreement (1985) and Convention (1990) brought the borders into focus for Germany. First, the 1985 Agreement regulated a now "borderless" massive area, with the Convention shoring up Germany's new position in the centre of the EU. The suspension of internal borders was seen as an experiment, also in terms of criminal behaviour. Fear of an increase in organised crime and massive trans-border criminal movement arose. One of the conclusions drawn was that outer borders now needed to be even more secure[9].

1.3 Privatisation

While most telecommunications and internet service providers have unintentionally become part of the security regime, many private actors – companies – benefit from the extension of security in general. A first major trend concerns the rising use of risk management and security measures on the part of companies and industries. Traditional security service companies offered services of locking, guarding and patrolling. With the continued increase in space occupied by industries, more protection has been engaged. Security services have also often been linked with building-related services such as cleaning and other forms of maintenance.
Concerning the notion of security, a qualitative shift has occurred with the introduction of IT in most industrial and service organisations: it has become a security issue and a sector of its own, extending the "security market" vastly. With growing networks and more complex supply chains through outsourcing and lean production, security of business, data, finance, etc. has come to be seen as one issue termed "business continuity". The rescue comes as a comprehensive systems solution from one hand, e.g. the large security service company or the systems integrating company, including risk management, services, and technologies. This development finds its expression in the emergence of a market for security consulting as a stand-alone product. Consultancies take on an intermediary role in the unregulated, diverse and thus confusing security market.
A second development concerns the shift in public and private spaces. Many places have – often unnoticed by the public – become private spaces. Whole infrastructures such as public transport are private, shopping precincts, banks and even streets are in the responsibility of their owners, yet used as, and perceived as, public spaces. The employment of private security services can thus be seen as the "natural" responsibility that comes with property (of space), a kind of "self-help" on the part of those who create these spaces.[10] To the people who frequent these spaces, and often to the security actors themselves, it is far from clear where the responsibilities lie. At the same time, since security is not the prime function of the organisations using private spaces, it is always in competition with commercial interests. Highly symbolic and visible security measures such as video surveillance thus meet with more approval from the companies than the

---

[9] cf. Jef Huysmans, *The politics of insecurity: fear, migration and asylum in the EU* (London, New York: Routledge,2006); Wyn Rees, "Organised Crime, Security and the European Union," in *Organised Crime and the Challenge to Democracy*, edited by Felia Allum and Renate Siebert (Routledge Chapman & Hall, 2003)

[10] cf. Hans-Jürgen Feltes, "Akteure der Inneren Sicherheit: Vom Öffentlichen zum Privaten," in *Auf der Suche nach neuer Sicherheit: Fakten, Theorien und Folgen*, 2nd ed., edited by Hans-Jürgen Lange, H. Peter Ohly, and Jo Reichertz (Wiesbaden: VS Verlag für Sozialwissenschaften, 2009) 109.; Tim Newburn, "The Commodification of Policing: Security Networks in the Late Modern City," *Urban Studies* 38 *(*2001):829-848.

more expensive security staff. This problem of accountability and legitimacy becomes crucial when privacy and data protection come into view – if security is of secondary importance, privacy is considered to be even less relevant.
The type of outsourcing of security functions commonly perceived as privatisation is the fulfilment of core security functions through private companies in Public Private Partnerships[11]. Here, it is not private but public space that is handed over to be secured through private actors. The requirements set by the public agencies are not much higher than otherwise – a point criticised by some actors within the market, because professionalisation processes stay slow. Still, the security service market leaders are prepared for Public Private Partnerships as they themselves are setting higher standards and approaching police quality in terms of education and appearance.[12]
With the blurring of safety and security concepts and functions, actors formerly concentrating on defence (and aviation) step into the civil security market more powerfully. Making intense use of the network paradigm and their experience in real-life missions, these companies now offer comprehensive solutions for the protection of critical infrastructures and crisis management and present themselves as the prime partner for the state when it comes to cooperation with private actors. In this regard, a capacity imbalance of public and private security providers is articulated. While public agencies now use private information infrastructures, they cannot keep pace with the original technological novelties. Large-scale sensitive projects such as the digital telecommunications network for security organisations are implemented by private companies.
To sum up, what is commonly termed "privatisation" is not a mere outsourcing of public functions, but a complex and multi-faceted development. An increase in private space (space privatisation) – industry and business representing an important share – also accounts for the involvement of private actors in security. At the same time, the state encroaches on private assets when security agencies make use of companies' infrastructures. Thirdly, an entirely new sector within security has emerged, adding to the capacity of private actors as compared to state capacities – the field of IT security, a major cross-cutting security issue. Considering these developments, it makes sense to speak first of an extension of the security regime in general – including both public and private actors –, and second of the qualitative extension and quantitative growth of a security market undergoing structural changes. Indeed, the "security market", as heterogeneous as it is, has attracted much attention from economically interested actors, especially in the field of technology.

1.4 Networked security

The institutional vision of "networked security" which connects agencies and includes safety and security is complemented by the security technology oriented use of the term. Perceived changing threats are faced with converging solutions: "Many measures which were initially aimed against organised crime are by now used against international terrorism."[13] What is more, measures are now aimed at terrorists, burglars and fire at the same time. Security technologies have undergone a process of convergence through digitisation, making new functionalities possible in interconnected systems[14].
Great hopes are set in the security technology market – mostly from an economic perspective, but from a rhetoric viewpoint and closely coupled to the new understanding of security. The security technology market is booming – at least according to the market overviews available and the self-description of the participants. Still, the market remains completely obscure and mostly arbitrarily defined. All kinds of technologies can be subsumed under "security" if the application indicates it, which is best shown with classic dual-use technologies. Biometric sensors, for example, are quite common in industrial quality

---

[11] cf. Martin Morlok, and Julian Krüper."Sicherheitsgewährleistung im kooperativen Verfassungsstaat." in *Auf der Suche nach neuer Sicherheit: Fakten, Theorien und Folgen* (VS Verlag, 2009)

[12] Andreas von Arnim, "Private Security Companies and Internal Security in Europe," in *Recht und Organisation privater Sicherheitsdienste in Europa*, edited by Reinhard Ottens, Harald Olschok, and Stephan Landrock (Stuttgart: R. Boorberg, 1999)

[13] Sebastian Bukow, "Internal security and the fight against terrorism in Germany" (Philosophische Fakultät III Institut für Sozialwissenschaften, Humboldt Universität Berlin, 2005). Accessed: 30.7.2011, http://edoc.hu-berlin.de/oa/conferences/reZgVweZSLueU/PDF/27QEOto3iuZCs.pdf

[14] cf. Paul Edwards, *The closed world: computers and the politics of discourse in Cold War America* (Cambridge Mass.: MIT Press, 1996); and Michele Zanini, and Sean J.A. Edwards, "The Networking of Terror in the Information Age," in *Networks and netwars: the future of terror, crime, and militancy*, edited by John Arquilla and David Ronfeldt (Santa Monica CA: Rand, 2001)

management, but have been re-appropriated as a security technology. Security technology development is also generally supported well in terms of funding.
In such a dynamic market, as could be expected, actors try to get their share of the cake. Large economic players play the game – they make the most of existing discourses such as the network paradigm or extended security programmes. Our analysis has shown that many corporate players utilise security extension rhetoric in order to expand their business[15]. Market potential studies and an uncritical use of "new threat" rhetoric become self-feeding mechanisms. Since all technology can be appropriated for security uses, there is a wide field especially through convergence of digital technologies such as IP video and biometrics. Systems integrators benefit from this development.

1.5 An expanding security market

Against the backdrop of this general process of securitisation of political, legal and economic regimes and an expanding security market, notions of regulation shift when it comes to the problematic effects of security services and technologies on the people and the public under surveillance. Responsibility for the protection of privacy and data is being transferred to companies with clear for-profit goals and little intrinsic motivation to question the supremacy of security over privacy protection. The underlying assumption of most actors is that legal provisions are clear and sufficient to safeguard the data subjects' privacy and liberties.
There is clearly a contradiction between the goal of "networked" and "total" intelligence pursued and advertised by security companies – the general idea of feasibility and omnipotence – and the public and individual interest to preserve privacy and personal data protection, as well as just having "unobserved" spaces. Yet, when it comes to surveillance, attention focuses mostly on the state as the central actor and potential invader. Decentralised surveillance, delivered by private actors in private spaces such as public transport systems, is harder to discern and grasp in its entirety, or assess with regard to its effects. This is true both for the data subjects and regulating bodies, and the organisations themselves.
The transformation of the security field towards increasingly market-based relations leads to new questions about the governance of privacy and the efficacy of legal provisions[16]. A closer look at the actual, day-to-day practices of security actors is, to this end, necessary. Discussions about new forms of more market-based regulation – "self-regulation" - cannot be led without a clear picture of the context and mechanisms – the market – that these organisations operate within.
While privacy is largely perceived as a "problem", and not an opportunity within the security industry, some developments suggest that there is room for privacy awareness raising within organisations: the targeted professionalisation of the security service market, a trend towards systems solutions including consulting and auditing (risk management), and the branding efforts of globally operating companies. Based on these potential opportunities attached to the hugely enhanced role of the private sector, the PATS project inquired into current levels of privacy awareness among security actors as part of the next research step.

2 Security actors

In this section, we will take a closer look at the actors' practices, attitudes and awareness of privacy. The results presented here are based on 12 in-depth qualitative interviews with stakeholders from security organisations of the different types we discerned in the previous work package: technology producers, service providers, consultancies, research institutions and associations.[17] The main question during this research phase was how privacy is perceived by security actors, and how, in contrast with abstract legal norms, privacy and data protection are actually *practised in organisational routines and operations. In other words: how does privacy figure in security actors' daily business lives and decisions?*

---

[15] This is what we also found in the analysis of security communication, see section 3.

[16] A comprehensive review is provided by Colin J. Bennett and Charles D. Raab in *The governance of privacy: policy instruments in global perspective*" (2nd and updated ed. Cambridge Mass.: MIT Press, 2006).

[17] The interviews were semi-structured, qualitative interviews which lasted from 1 hour up to 3 hours. All but one interview were conducted face to face and recorded. They were then transcribed or paraphrased closely. The analysis was done using the qualitative analysis tool Atlas.ti with a Grounded Theory approach.

In this section we argue that in practice there is a limited understanding of privacy and often very low awareness. This state of affairs is strongly related to actor constellations and their relationships within markets. These findings lead us to articulate criticism of the current market relationships which represent a less than "perfect" market – in particular, we face substantial problems with regard to the information about security needs and technologies as pointed out in the preceding section.

2.1 Organisational practices.

In general, we found a very limited understanding of privacy in security organisations. Privacy is mainly understood as data security – a rather technical understanding of privacy that neglects the democratic value of privacy and the basic principles of data parsimony and sensitivity. Privacy is thus reduced to organisational-technical issues of data processing and storage and is not dealt with on the level of business processes or decisions in general.

Another important practice is the reference to the existence of ISO standards and legal frameworks with the objective of shifting responsibility to those entities. These standards and legal frameworks are used as black boxes when used as an argument for not giving more thought to the related issues: "Why, but there is a data protection law!" The practices and routines regarding privacy and data protection are opaque even to the members of the organisations we interviewed. This becomes problematic when the unquestioning trust in the almost magical workings of legal provisions is accompanied by a reluctance to even discuss the topic – as privacy, so our interview partners argued, had surely been taken care of in some shape or form.

Another dimension of opacity lies in the fact that the organisational structures – which should enhance privacy compliance – depend on the actual practices of each company. For example, it makes a big difference as to whether data protection officers are employed full time or not, how well trained they are in data protection issues and how independently and proactively they can act within their company. As stated in interviews, the qualification of employees is indeed an issue; some actors are still trying to achieve basic legal compliance, which renders active engagement for data protection impossible and sheds a very critical light on ideas of self-regulation.

In conversations, most of the representatives express their willingness to enhance privacy protection, but they feel that they face the described organisational problems and are limited in their sphere of action, because they have to act according to the needs, more specifically: the demand of the markets. This will be elucidated further in the following.

2.2 Privacy awareness.

While there are indeed individuals who wish to enhance the privacy practices within their organisations and who are aware of privacy problems and problematic structures, there is nevertheless a general lack of communication with the public about privacy issues – even when there is a real interest in providing and enhancing privacy within the business model. We found examples of security actors with a strong willingness to improve the privacy situation in relation to services or technologies offered. These interviewees stressed that trust is more important in the long run than instant economic profit, and that they offer data protection education in addition to their security products and services. Yet, according to a technology producer who offered specific Privacy Enhancing Technology (PET) options in combination with an IP camera product, there is little or no demand for these technologies and clients will not buy them as long as it is perceived as a costly "add on". This lack of client interest, along with what one interviewee called a "cat-and-mouse-atmosphere" when talking about data protection issues, seems to lead to a situation where companies do not feel like communicating about privacy in the public domain. It seems like putting oneself in danger for no reason.

This difficult relationship between privacy practice and privacy communication becomes evident when we look at companies that went through privacy scandals. From our interviews, it emerged that data leakage or misuse scandals hit the clients of security (technology) providers, not necessarily the security companies themselves. When misuse becomes publicly known, these organisations mostly show two reactions: either they begin to talk publicly about their privacy efforts or they avoid any (further) publicity about data protection. For the former however – intense communication on privacy efforts – it was reported that

organisations try to achieve formal law abidance to “safeguard the management board from claims”.[18] This is illustrated by companies that set up entire compliance departments to purify their reputation, notwithstanding the efficacy of these measures. Reputation is an important asset especially in regard to investors' trust, but engagement spurred by this motivation does not surpass a pragmatic attitude towards data protection and privacy. The communication aims to present a good image regardless of the real effectiveness of data protection measures and related practices.
The second common reaction to scandals is the avoidance of further image damage through the avoidance of any communication about privacy related issues, which against the backdrop of the “accountability” discourse seems to be a questionable strategy. Companies that stay silent about their surveillance projects clearly impact their security technology providers' behaviour. Not only are suppliers less than encouraged to enhance their privacy performance, but they are also asked to keep a low profile. This is in stark contrast to ideas of self-regulation or even building a positive image by stressing one's outstanding privacy performance.

2.3 The actors and the market.

To revisit the findings so far: There are intransparent structures which lead to a certain degree of opacity. Responsibility is shifted to institutions such as data protection law or data protection officers, quality standards or – as we will point out in the next section – even technology (e.g. PET). We want to argue here that the market, which is invocated as a source for regulation by the “invisible hand”, reflects this opacity and is far from constituting a regulative framework. The current market structures do not relay market pressure or incentives towards more privacy protection to the companies in charge. On the contrary, it seems that the regulating power of the security market weakens privacy as a consequence of the actual relationships.
According to our outcomes we face (1) conflicting interests of different actors, (2) a tendency to hold citizens accountable notwithstanding their constrained possibilities to influence or participate security organisations and their clients' business behaviour, and, maybe most problematic, (3) a total lack of representation of citizens/ data subjects and of any information directed towards this group.
The low demand for privacy tools is rooted in the market setup: the clients are interested in (cheap) surveillance technologies, not in citizen rights. It is important to understand the supplier-client relationship here: if we think of clients as those paying for security products and deploying them in their facilities, they provide the demand for security technologies – and are legally held responsible as “data controllers”. The suppliers are security technology producers or security service providers offering their products to this market of clients, e.g. public transport companies, airports, other companies or institutions.
Which role does the citizen, public transport passenger, or employee take on in this constellation? The data subject is a client of the security organisations' clients – or even a dependant, e.g. in an employment relationship. The relationship is thus not always a voluntary one based on market forces. Even if we concede consumers some market power in respect of their choice of e.g. surveilled or non-surveilled supermarkets, their power is very low. Sheer selection forces do not go far here; for example, in order to avoid public transport due to the use of CCTV, one has to opt out of the system and use alternative transportation means. It becomes difficult to walk the streets without being captured by any camera, or even realise in whose space – public, private? – one is moving about and whose camera is watching – so in this case, how can consumers possibly exert market influence by pure selection? Accordingly, the actor we expect to demand privacy – the data subject – is utterly uninformed and cannot easily exert influence within the market of security technologies and services. In a sort of pre-emptive move, many interviewees from the security field hold citizens accountable for infringements of their privacy with reference to the fact that they use Google and Facebook – the great icons of voluntary data deluge – and take part in rebate marketing. This attitude suggests that “the horse has already bolted” and is combined with an affirmation of consumers' choice. The assumption that ICT users themselves generally lack privacy awareness is both implicitly and explicitly mentioned, often alleging a generational difference and genuinely new culture of “digital natives” that knows no privacy concept. At the same time the public's and citizens' demand for security is taken for granted and articulated over and over e.g. when it comes to security on public

[18] See interview 2, line 46.

transport where violent events receive a lot of media attention.
In the current communication of the European Commission, the problem of the citizen's burden of being held accountable is addressed with the claim of enhancing the transparency of e.g. privacy notices, replacing opt-outs with opt-ins, and strengthening the power of the users.[19]
However it is questionable as to how internal market regulations can be enhanced to strengthen privacy efficacy when we are facing an utter non-representation of the citizen within the markets. Our findings pertain to the specific case of the security market, but we hold it to be indicative of the general lack of information and transparency when it comes to the much heralded market-based regulation of privacy in other industries (Social Network Sites).

3 Security communication

To round off the perspective we will now give an insight into the security communication of security organisations, based on the analysis of material from security fair, brochures, websites and several issues of a security journal.[20] Notably we find a special mode of communication: the self-representations are strictly oriented to the clients of the specific market. Accordingly the analysis shows which values are communicated and how security is constituted in the security branch.

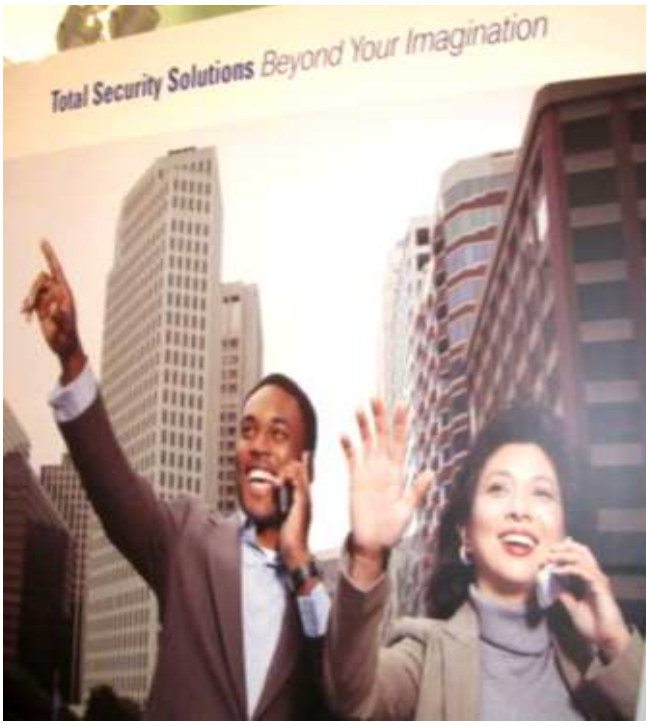

Fig. 1. Samsung: Total Security Solutions – Happiness and prosperity

3.1 Economic value and invisibility.

The most obvious kind of narratives we find is the presentation of economic values and a general feeling of happiness. The latter is mainly communicated with images of happy people, which are obviously happy because they are secured and protected by technologies and services. Organisations try to communicate that economic value is actually secured through security services and technologies. Economic value is shown both as private home property and in a business context. Remarkably, economic value is sometimes encased with the notion of ethical values such as in the slogan "protecting values"[21]. Obviously in the material the threats are hardly shown; yet the economic value and people take centre stage.

For example on this poster from Samsung, smiling well dressed people walk through a stylised financial district. They are happy and busy; they use their cell phones. There is no visible threat; security technology does not even feature in the picture. The threat is completely absent while the slogan is "Total Security Solutions. Beyond your imagination." Only in this slogan is the issue of security made explicit. Yet, no-one appears to take notice of threats or the security technologies. The picture also implies that security is, rather ironically, a precondition for the *freedom to move*. The message is *"freedom through security"*, meaning that those who are allowed to move have to be "secured" whereas the fact that most people in the world are not allowed to move as they want, and security technologies enhance their exclusion, is not worth mentioning in this poster. Being secured means in this context being scanned and categorised as either a trusted

---

[19] cf. European Commission. *"Communication from the Commission to the European Parliament, the Council, the Economic and Social committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union"*, loc. cit.

[20] We collected pictures from stands and brochures at the fair "Security Essen 2010", material from website presentations and ten issues of a security related stakeholder journal between 2009 and 2010. For the analysis, we used Atlas.ti to find common narratives in the self-representations of the organisations, and coded the material using a Grounded Theory approach.

[21] Quote from a poster of a company named Orfix.

or mistrusted person. Beyond that, this co-constructs the idea that people who are not allowed to move freely are dangerous and have to be excluded.

3.2 Total security and convergence**.**

At the same time, the "Total Security Solutions" term symbolises another evident narrative; Samsung is offering integrated system solutions, and this sort of product is focusing on the technological promises we find connected with "*networks*" and interoperating systems. We find these lines of argumentation linked to a modern belief in technological possibilities which is not at all aware of critical reflections and the limitations of technologies. It is rather the co-constructing of black boxes that leads to social causes and implications being neglected.

Continuously we found the theme of the "blessing" technologies, mainly computer analysis tools, which were presented and touted in various ways. We called this theme also *cybernetic*, because it refers to the discourse in the second half of the 20th century, and it seems like a very uncritical dream of almighty computer systems giving *men the power and the control* over the world. Total security is often presented in a *game-like* manner at the security fair, when companies want to illustrate the great possibilities provided by technologies in their stands.

The common argumentation line of *cybernetics* is that artificial intelligence promises to regain control over the flood of data. Beyond that we also find a reference to science which strengthens the connection to the modern age and cybernetics: "imageology – the science of surveillance"[22]. It is here that technology is constructed both as a data emerging tool and at the same time it gives humans the power to keep an overview through its own intelligence. Consequently it is a double solution (seek and control), while humans are neither able to gain all the information nor to keep track over it without technology. In other words, data control supports the vision of crowd control.

Summarizing this narrative suggests empowering humans to deploy a ubiquitous surveillance setting which focuses on prevention instead of reaction.

3.3 Naturalisation

Imagery of natural settings and natural metaphors is frequently used by the security organisations. In some cases we find a direct comparison with nature such as the "organic" functioning of technologies, systems and organisations. Often, nature is taken as a model for technologies. Many pictures show nature to describe security situations and to construct a certain feeling. For example, on a Honeywell poster there is a picture of a nearly closed shell combined with the slogan "closing the security gaps." Again there is no explicit reference to threats, but a focus on the solution. At the same time it is clearly connoted that threats

[22] Quote from a Bosch poster

are a natural problem. The social character of security as a societal concept is completely neglected. Communication of this quality supports an irrationalisation of the discourses. Security is presented as a natural need – and natural facts cannot be discussed.

More subtle than the described nature imagery is the naturalisation of social hierarchies. We find images of mothers protecting their child and of families in their safe home; a clear reference to the "natural" hierarchies of protection.

In all, this stands in line with the argumentation that first, threats are a natural phenomenon and second that security is a natural need which has to be taken care of. Naturalisation is here an argument of determinism, which consolidates the actual relations and neglects social reasons and causes that underlie the challenges facing security.

Security Buyer: Sheltered

4 Conclusion

We have argued that the market structures in the security field are obscure to the extent that no incentives for self-regulation are perceived by the actors involved. Security actors are clearly interested in making a profit and do not have sufficient intrinsic motivation to kick-start self-regulation. Demand for more attention to privacy would have to be forced upon these actors, but no one currently articulates this demand within the market.
Not only are market relationships indirect, but citizens and the public are rarely even represented in the market at all. Privacy cannot translate into a means of monetary regulation in the marketplace in this set-up. What is more, security companies actively support obscuring discourses about threats and security through their communication strategies of naturalisation and invisibility. Security and privacy are rendered "unspeakable" through these opaque imageries, and public discourse about privacy is further hindered.
This investigation into organisations' practices has shown that current claims for self-regulation need to be backed up by research into the conditions that have to be met if market forces are to be harnessed for privacy and data protection. Institutional conditions and frameworks greatly influence data controllers' potential and motivation for enacting privacy awareness and self-regulation. These structures need to be known in detail in order to make statements about self-regulation prospects and goals in specific sectors. In particular, internal market regulations cannot be enhanced to strengthen privacy efficacy when we are facing a total non-representation of the citizen or the data subjects within the markets. An important issue to raise within the current self-regulation discourse is thus how, hitherto, under-represented actors can be shifted into a more powerful position within "self-regulating" markets, and which mechanisms need to be implemented in order to make market forces "work" towards privacy protection.

5 Bibliography

1. von Arnim, Andreas. "Private Security Companies and Internal Security in Europe." In *Recht und Organisation privater Sicherheitsdienste in Europa*, edited by Reinhard Ottens, Harald Olschok, and Stephan Landrock. Stuttgart: R. Boorberg, 1999.
2. Article 29 Working Party. "Opinion 3/2010 on the principle of accountability." 2010. Accessed 28.7.2011, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf
3. Bennett, Colin J., and Charles D. Raab. *The governance of privacy: policy instruments in global perspective*. 2nd and updated ed. Cambridge Mass.: MIT Press, 2006.
4. Bukow, Sebastian. "Deutschland: Mit Sicherheit weniger Freiheit über den Umweg Europa." *In Europäisierung der inneren Sicherheit*, 43-62. edited by Gert-Joachim Glaeßner and Astrid Lorenz. Wiesbaden: VS Verlag, 2005.
5. Bukow, Sebastian. "Internal security and the fight against terrorism in Germany." Philosophische Fakultät III Institut für Sozialwissenschaften, Humboldt Universität Berlin, 2005. Accessed: 30.7.2011, http://edoc.hu-berlin.de/oa/conferences/reZgVweZSLueU/PDF/27QEOto3iuZCs.pdf
6. Busch, Heiner. "Kein Mangel an Sicherheitsgesetzen." *FriedensForum*, 2008. Accessed: 30.7.2011, http://www.friedenskooperative.de/ff/ff08/6-61.htm
7. Buzan, Barry, Ole Waever, and Jaap de Wilde. *Security: a new framework for analysis.* Boulder Colo.: Lynne Rienner Pub., 1998.
8. European Commission. "Communication from the Commission to the European Parliament, the Council, the Economic and Social committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European

Union." Brussels: European Commission, 2010. Accessed: 20.7.2011, http://ec.europa.eu/health/data_collection/docs/com_2010_0609_en.pdf
9. Feltes, Hans-Jürgen. "Akteure der Inneren Sicherheit: Vom Öffentlichen zum Privaten." *In Auf der Suche nach neuer Sicherheit: Fakten, Theorien und Folgen*, 2nd ed., edited by Hans-Jürgen Lange, H. Peter Ohly, and Jo Reichertz. Wiesbaden: VS Verlag, 2009.
10. Heinrich, Stephan, and Hans-Jürgen Lange. 2009. "Erweiterung des Sicherheitsbegriffs." In *Auf der Suche nach neuer Sicherheit: Fakten, Theorien und Folgen*. VS Verlag.
11. Huysmans, Jef. *The politics of insecurity: fear, migration and asylum in the EU*. London, New York: Routledge, 2006.
12. Isensee, Josef. *Das Grundrecht auf Sicherheit. Zu den Schutzpflichten des freiheitlichen Verfassungsstaates*. Berlin: Walter de Gruyter, 1983.
13. Lange, Hans-Jürgen, H. Peter Ohly, and Jo Reichertz. *Auf der Suche nach neuer Sicherheit: Fakten, Theorien und Folgen*. 2nd ed. VS Verlag, 2009.
14. Lange, Hans-Jürgen, and H. Peter Frevel. "Innere Sicherheit im Bund, in den Ländern und in den Kommunen." In *Auf der Suche nach neuer Sicherheit: Fakten, Theorien und Folgen.* VS Verlag, 2009.
15. Lyon, David. "9/11, Synopticon, and Scopophilia: Watching and Being Watched." In *The New Politics of Surveillance and Visibility*. Haggerty, Kevin. D. and Ricard V. Ericson, eds. Toronto: University of Toronto Press, 2006.
16. Morlok, Martin, and Julian Krüper. "Sicherheitsgewährleistung im kooperativen Verfassungsstaat." In *Auf der Suche nach neuer Sicherheit: Fakten, Theorien und Folgen.* VS Verlag, 2009.
17. Newburn, Tim. "The Commodification of Policing: Security Networks in the Late Modern City." In *Urban Studies*, 38 (2001): 829-848.
18. Rees, Wyn. "Organised Crime, Security and the European Union." In Organised *Crime and the Challenge to Democracy*, edited by Felia Allum and Renate Siebert. Routledge Chapman & Hall, 2003.
19. Singelnstein, Tobias, and Peer Stolle. *Die Sicherheitsgesellschaft. Soziale Kontrolle im 21. Jahrhundert*. VS Verlag, 2006.
20. Zanini, Michele, and Sean J.A. Edwards. "The Networking of Terror in the Information Age." In *Networks and netwars: the future of terror, crime, and militancy*, edited by John Arquilla and David Ronfeldt. Santa Monica CA: Rand, 2001.