PATS

Privacy Awareness Through Security Organisation Branding

Ethically Focused Brand Evaluation

WP 4 Synthesis Report

Deliverable D 4.3

Cross-national Report by WP leader
Philadelphia

US Team

Temple University

Philadelphia, PA

Project number
230473

Call (part) identifier
FP7-SCIENCE-IN-SOCIETY-2008-1

Funding scheme
Coordination and support action

Contents

A. Introduction

This report provides an overview and synthesis of the national reports provided by each PATS national team for WP4. As described in PATS Annex 1, the purpose of this work package is to "increase the knowledge of existing symbolic representations of security agencies and security functions of private industry" (pg. 28). Each national partner has collected and analyzed promotional material from security companies in their respective national contexts from industry publications, trade shows, corporate websites, and photographs of video surveillance operating in city centers. Theoretically, we see this data to constitute communicative discourses that convey meanings about security, risk, and privacy between and amongst privacy industry, to their public and private sector clients, and the general public. Our aim is to analyze this material for reflexive discourses, or ways in which the industry talks to itself about itself, and external discourses, or ways that the industry talks to users and the public. Or, as the UK team appropriately quotes in their report, our aim is to examine "who says what, to whom, why, to what extent and with what effect?" (Lasswell 1948).

This report is split into two broad sections. The first will review the main findings of each national partner. This section is organized thematically rather than on a country-by-country basis. The second section will draw on existing academic literature to outline what the ethical branding of privacy could be and incorporates examples from the national reports. In doing so, we hope to provide a bridge between previous work packages and future work.

B. Section One: Reviewing the Evidence

Perhaps the most common theme to emerge across all national reports is the degree to which the industry promotes technological advances as the most promising solution for all manner of security anxieties. This commitment is evident across a range of products the industry produces and is commented on by all national reports. In their analysis of promotional material of surveillance cameras, the UK team notes, "Large amounts of technical detail is included, describing 'hi-resolution', 'high quality', and 'optimal image quality' specifications. Often the detail included is so technical that only someone experienced in that field would be able to understand it" (pg. 6). The enumeration of technical capabilities was also touched on by the German and Finland reports; Finland for examples notes how Finnish firms rely on promoting "quality and technological content in the products and services" they offer (pg. 12).

In many respects, this communicative strategy is to be expected as it is the nature of advertising to promote any sort of product as the best in the field. As the Israeli report notes, this message is one of the most important to be conveyed to clients, and it would be rare to find a company that knowingly markets its products as second-rate. At the same time, and as the German, UK, and USA teams point out, the commitment to ever-more sophisticated technologies also reflects the wider embrace of technology as a 'fix' for all manner of security concerns after 9/11 (Lyon, 2003). In the last decade or more, new and more sophisticated surveillance cameras augmented with analytics capabilities, wide-area scanners for detecting CBRN material, and identity verification devices have all been promoted

as the solution for the apparently endemic nature of uncertainty today. Implicit in this is the view that humans are by nature fallible and that technology can overcome these limits. This 'fix' is also part of the modernist dream of technology as a way to exercise control over all aspects of life in order to reduce uncertainty and maximize wellbeing that Germany calls the "dream of cybernetic control." Indeed, there is a strong message from the industry that all risks can be brought within the realm of technological-enhance human control if the right tools can be developed. This dream is perhaps most apparent in the burgeoning field of GIS modeling for homeland security and emergency management where entire cities can be represented with 3D digital models and integrated surveillance cameras, lending a game-like dimension to security wherein all risks can be brought within the enclosures of this simulated environment. Actually doing so is a practical and ontological impossibility, but confronting these limits would not only undercut the foundation of the industry but require calling into question one of the basic ideas of modernity. Instead, this impossibility is harnessed as a driver for further innovations in the field.

Closely related to the promotion of technological advances, but existing in tension with the modernist embrace of technology, are representations of human labor as an important element to mitigating security risks today. This is most apparent in the respective analyses offered by each national team of G4S/Securitas. Common across all national contexts is the way that G4S/Securitas represents their security guards as capable, competent, and professional. Finland for example reports how Securitas emphasizes the expertise and professionalism of its national workforce. Similarly, the UK team reports how these companies emphasize their level of expertise in meeting the large or small scale security needs of clients in a customer service-focused way. Germany quotes promotional copy from Securitas that says how the firm's workforce meets their client's needs "in a professional way." Again, this message is not wholly unexpected, and it is probably rare to encounter cases where a security provider knowingly promotes its workforce as sub-par and unprofessional. Yet what also stands out in the various example images made available by G4S and Securitas is how their guards are portrayed performing security duties in malls, sporting events (particularly in the UK context as stewards for football matches and the upcoming 2012 Olympics[1]) and other leisure/tourism contexts, as well as in contexts such as transportation, energy and utilities, and infrastructure security. Even armed forces – one of the key functions of the modern nation-state – is a potential growth industry for these firms as they move into providing supports roles for military operations (see German report, pg. 7). In other words, what we see in these various representations is evidence of the strategic positioning of these firms in relation to (at least) two interrelated trends in security governance accruing in the last two decades: the growth of quasi-public space (privately owned facilities that are normally open to the public) and the trend towards downsizing and outsourcing routine public service functions in government, and these companies exploit these trends by maintaining stocks of flexible labor that can meet the needs to today's postindustrial and neoliberal economies.

All reports provide examples of the industry drawing upon representations of society, economy, and risk in order to demonstrate the utility of their products. The UK and German teams both comment

[1] During the preparation of this report G4S (UK) announced it has signed a £100 million contact to be the official security provider of the 2012 Olympic Games.

on the gendered nature of advertising in the security field. Germany, for example, describes how much of the promotional strategies on display at the security fair they attended are constructed with men as their primary audience, which comes across in how security is portrayed as a 'man's game' and women delegated to supporting roles. This gender dynamic was embodied in a female model of Lara Croft hired by a security company to provide "fun and attention" for visitors to the booth. This was mirrored at the trade show attended by the US team wherein visitors to a certain sales booth were given the opportunity to have their photos taken with two members the Dallas Cowboys cheerleaders. Other representation of gender are less explicit but no less significant to account for. The UK team highlights how promotional copy from the industry often reinforce the view that women are the 'weaker sex' in need of protection in their homes and routine activities by using phrases such as 'securing your life' and 'enhance security' alongside images of women in domestic contexts.

The implicit identification of risk and vulnerability touched on in this example from the UK in relation to gender is extended in relation to other ostensibly vulnerable populations as well. As the US and Israeli reports demonstrates, advertisements from the industry often depict at-risk populations or locations as well such as babies and children, the elderly, families, schools or hospitals. In these contexts security products are offered not only for their power of protection but as a means for enhancing *feelings* of safety and security. Israel provides the example of "Baby Match," a product designed for identifying and, if needed, tracking newborn babies in hospital wards. This product plays on fears of mismatch or abduction of babies in hospitals, and is marketed as a "precaution against abduction but also for the peace of mind that mother and baby are matched from birth to discharge" (Israel, pg. 9). In other cases the identification of risk is more explicit. This is most apparent in data presented by the US team, which identifies how the industry plays on fears of catastrophic terrorism after 9/11 as a way of demonstration the necessity of the industry's products and expertise within the homeland security market. These representations play on the discourse of 'the new terrorism,' characteristic of which is the idea that potentially catastrophic risk is pervasive, imminent, and in need of aggressive and preemptive measures (Aradau & van Munster, 2007). We see this precautionary rationality extended in many advertisements from the US context, such as one that shows the mushroom cloud from a nuclear detonation. This image is linked to a nuclear material detection unit that is promoted as an indispensible way of preventing such destruction. "The alternative," the ad states, "is unthinkable."

Another commonality to how the industry markets its products is representations of globalization and global mobility. As the German team reports, this includes images of personal and informational mobility as represented by images of business travel or symbols of capitalism such as business centers along with messages indicating how informational security is an integral element of today's business enterprise. Other representations of mobility are less about information security and business management as they are about securing the physical infrastructures that enable large-scale mobility such as airports, seaports, rail transportation networks, and energy facilities. Securing these infrastructural assets has become a key growth area for systems engineering and integration firms such as Siemmens, which promote their expertise in providing authorities with 'full situational awareness' and 'enhanced command and control' capabilities by tying together various individual

technologies into integrated systems, or 'total security solutions' as promotional material from Siemmens often puts it.

The exploration of public signage of video surveillance cameras revealed a wide variety of communicative strategies at work. The Polish team reports how there are no laws restricting the use of surveillance cameras by government agencies except in "intimate" settings such as washrooms or changing rooms. Government authorities are, however, required to post notices of who is responsible for control of particular facility, which may or may not include notice of the use of surveillance cameras. Neither are there requirements for privacy entities to inform the public of the use of surveillance cameras. Instead, notification of cameras is done in a strategic way to "frighten off thieves or persons who in any way intend to disrupt the security of people or their property" (pg. 21). The Finnish team reports how the public signage of surveillance cameras in the Helsinki-Vantaa airport is ubiquitous but subtle, reflecting an avoidance of overt impressions of security in favor of an atmosphere that is "free from control, while on the other hand control is strongly present" (pg. 14). They note that surveillance cameras in Finland are operated primarily by private agencies, though there is an increased interest on the part of government agencies to implement video surveillance system in the country. The German team also comments on the ubiquity of surveillance cameras operated by private actors to monitor private property. While there are no provisions restricting the capacity of private actors to do so, the German team notes the ambiguity that comes when these cameras have fields of vision that capture public space. Government agencies are permitted to use surveillance cameras to monitor state facilities and buildings which is covered by German data protection laws, but public notification of the operation of these cameras is rare even though required by law (pg. 16).

The UK, USA, and Israel reports provide examples where security, surveillance and policing initiatives are incorporated within wider efforts to rebrand cities as safe and secure environments. Israel's case study focuses on a national project called "City without Violence," which is the national government's flagship program for addressing with anti-social behavior, violence, delinquency, and crime in cities across the country. This program includes 5 main areas of intervention: enforcement, education, welfare, leisure, and partnerships with public stakeholders. Video surveillance cameras are an integral part of the enforcement component of this program, which involves locating cameras in high-crime 'hotspots' accompanied by signage notifying the public of the operation of the cameras. Similarly, the UK details how surveillance cameras and associated signage are part of local public-private partnerships to ensure safety in the cities of Oxford and High Wycombe.

In Oxford, surveillance cameras are one element in a complex of spatial tactics (such as strategically positioned street furniture and open sight lines) that aim to increase formal and informal surveillance in the town center. Though official material from the local public-private partnership suggests that surveillance cameras should be approached with caution due to the possibility of increasing fear of crime (a point also made by the Finnish team), cameras have been enthusiastically adopted throughout Oxford. Surveillance cameras are also common in High Wycombe as the town grapples with high rates of "petty crime and that various forms of anti-social behavior (such as urinating, defecating, drinking alcohol and fighting in the streets)" (UK report, pg. 33).

Though crime reduction is the direct aim of these initiatives, the UK report also explains how these initiatives are part of wider efforts to restore these town centers as shopping and leisure destinations. “The main impetus behind the CCTV system seemed to be to protect the town centre as a retail and leisure area. The CCTV system was used to encourage existing businesses to stay in the town and to encourage new retailers into the centre with the message that the cameras encouraged shoppers to spend time and money in an environment where they felt safe. The cameras were also thought necessary to match other nearby town centers which competed for business and customers and had CCTV systems” (UK report, pg. 33).

The UK Data Protection Act requires all video surveillance programs to be accompanied by signage that informs the public who is operating the system and how operators can be contacted. (This raises the interesting point that this means that the ‘signs of surveillance’ are more heavily regulated than the existence of the cameras themselves; UK report, pg. 27). The signs themselves can range from highly professional signs carrying lots of detail to amateurish signs lacking the required detail. Significant for our purposes is that the visual appearance of these signs reflects the orientation of local authorities towards crime and disorder. In Oxford, camera signage appears to be integrated into the prevailing streetscape, which reflects an attempt not to eclipse the city’s historical designation with overt signs of security. High Wycombe has “far larger and more conspicuous CCTV signs than Oxford” (pg. 38), which reflects a more overt process of signification and deterrence at work. Furthermore, these signs are part of a wider array of posted prohibitions or “official graffiti” (Hermer & Hunt, 1996) reminding individuals to refrain from a host of behaviors such as feeding pigeons, smoking, drinking of public, or defecating in the street.

The US team reports on the large-scale video surveillance networks being constructed in Chicago and New York City under the auspices of the Department of Homeland Security’s Urban Area Security Initiative. Both initiatives involve establishing high-capacity and city-wide digital backbones that physically and wirelessly centralize police-operated cameras and enable those operated by other state agencies or the private sector to be accessed under emergency conditions.

In Chicago this initiative is called ‘Operation Virtual Shield’ and in New York City the ‘Domain Awareness System.’ These surveillance networks exemplify the sort of developments that privacy advocates warn pose serious concerns for civil liberties and personal privacy. These concerns stem from the fact that such systems no longer involve small numbers of cameras with comparatively restricted fields of vision but highly integrated networks that can span entire metropolitan centers wherein it is hypothetically possible to track a single individual over large swaths of the city. The power of government scrutiny of public activities becomes qualitatively different given the potential for continuous monitoring in this way, leading many to argue that current regulatory frameworks for the use of video surveillance are inadequate. As indicated in the US D3.1 report, there are no federal laws pertaining to the use of video surveillance in public space due to the widely accepted doctrine that there is no reasonable expectation of privacy in public space, but the DHS has formulated a series of best practices for the use of video surveillance (DHS, 2007). Adherence to these guidelines is optional, however, resulting in a highly uneven regulatory landscape where some municipalities are transparent about their surveillance networks while others are not.

Chicago is an instance of the latter. Chicago does not have any public documents describing the purposes of the system, rules about who can access video images and under what conditions, or retrieval and disposal guidelines as suggested by the DHS best practices for video surveillance. The DHS also recommends, "to the extent practical, the agency should provide notice through appropriate signage in area where CCTV is employed" (DHS, 2007a: 25), but no such signage is posted in the city. In contrast, city authorities in New York have issued a document titled "Public Security Privacy Guidelines" (PSPG) that explains the purpose of the Domain Awareness System, the legal basis upon which this initiative is authorized, defined the types of information collected through the system, and how this information will be stored, used, and protected. Notifying the public of the operation of surveillance cameras is part of these guidelines. The PSPG states,

> All NYPD-owned CCTVs that are part of the Domain Awareness System will have accompanying signage, and the NYPD will recommend that signage accompany each Stakeholder-owned CCTV that is part of the Domain Awareness System (pg. 3).

This signage is apparent throughout Lower Manhattan where most of the cameras are located. Unlike the UK where specific information is required to be included on these signs (even if this is haphazard in practice), these signs simply indicate that individuals are entering an "area" where cameras are operating, and are generally located at major corridors or intersections are people move in and out of the Lower Manhattan Security Zone (Nemeth & Holander, 2010). One example of this is the Brooklyn Bridge where numerous notifications are visible for pedestrian and vehicle traffic moving in both directions. Surveillance cameras have proliferated in midtown Manhattan after the March 2010 attempt to detonate a car bomb in Times Square. As in lower Manhattan, camera signage are placed in highly visible locations rather than accompanying each individual camera. This is most apparent in Times Square where large numbers of public signage, and the cameras themselves, are visible throughout the area.

This review has touched on some of the key findings from the research undertaken by all national partners for WP4. To reiterate, the aim of this research is to "increase the knowledge of existing symbolic representation of security agencies and security functions of private industry" (pg. 28). We have advanced this aim in two ways: by analyzing advertising and promotional material gather from the security industry and through sites visits to document the public presentation of surveillance cameras. We can see this material as collectively constituting what Monahan calls *security cultures*, which describes "prevailing understandings of threats and appropriate responses to them" (Monahan, 2010: 147). A number of themes stand out in the security cultures analyzed in WP4, including how the industry promotes advances in technology as the most promising tool for mitigating risk today and reflects prevailing representations of society, economics and risk to demonstrate the utility of its products. These themes have important consequences to be registered. As the UK team points out, the faith in technology as a 'fix' that can address all manner of contemporary risks, even the problems generated from the use of technology itself, means that technical expertise, rather than public participation, is seen as the way forward (UK report, pg. 7). And as Germany points out, the incorporation of representations of gender, global mobility, or vulnerability may serve to naturalize and reinforce the social structures underlying those representations. This may be most apparent in the depictions of radical uncertainty presented by the

US report, which reinforces the "presumed apocalyptic potential of contemporary threats" (de Goede & Sandalls, 2009: 859) and depoliticizes the call for aggressive counter-terrorism measures. In our analyses of surveillance cameras and associated signage in public space, what appears clear is how these technologies are more than crime minimization strategies but communicative technologies in themselves through which authorities seek to extend representations of cleanliness and safety as part of the rebranding of cities as safe locations to work, shop, and visit under regimes of inter-urban competitions for the people and capital 'of the right sort' that comprise the post-industrial economy (Coaffee, 2008). Privacy, if addressed, is done so begrudgingly and in widely divergent ways.

These findings outlined in the previous section are generally consistent with the findings of WP3 in which privacy was found to largely absent from the business activities of the security industry. In the following section we depart from the empirical orientation of the previous three work packages and draw on existing academic literature in order to develop a common understanding and terminology of what ethical branding is, or could/ought to be.

C. Section Two: Privacy as a Branding Strategy

Israel quotes Fan et. al. (2005) to state, "Ethical branding, as a subset of ethical marketing, relates to certain moral principles that define right and wrong behaviour in branding decisions. A brand needs to be evaluated not just by the economic or financial criteria but also by the moral ones. An ethical brand should not harm public good; instead it should contribute to or help promote public good." Finland offers a similar definition of ethical branding as "a marked name, an known identity composed by given characteristics, which can refer to the cultural, national, business, managerial, political or other kind of aspects of a given security actor or related stakeholder, public, private or individual (pg. 40). These are good starting points, but they remain abstract. What would this look like in practice? What criteria or indicators would have to be fulfilled to be considered ethical?

Bennett and Raab (2003: 121-138) outline a number of models through which security actors could voluntarily adopt in order to promote a 'privacy friendly' stance to audiences. While presented here in categorical form, these models are better understood as a continuum of practices that reflect greater or lesser degrees of engagement with privacy as a meaningful construct. Our discussion will also provide some examples to illustrate these models that are drawn primarily from our research in the US but have, we hope, parallels in other national contexts.

The first model is privacy commitments. Privacy commitments, Bennett and Raab explain, are often brief pledges or statements produced by companies that express a commitment to the protection of privacy. Privacy commitments are not reflections of substantive rules structuring business practices but statements "designed more for external consumption than to affect the internal functioning of the organization" (Bennett and Raab, 2003: 123). The motivation behind privacy commitment can range from self-interested promotionalism to genuine earnestness, but they are often produced as a way to counter negative publicity. A common example of privacy commitments are the privacy statements found in online shopping websites that explain how personal information will be handled

by the company. An example of a privacy commitment in the USA security industry is found in the International Biometrics and Identification Association, the website of which includes four "Privacy Principles" for its member organizations to adopt as part of their business activities[2] (see also the UK D4.2 national report, pg. 54, on the BSIA code of ethics).

The second model is privacy codes of practice. Codes of practice are similar to privacy commitments in that they express adherence to articulated principles but are more developed in that they include rules that structure, or ought to structure, the internal activities of the organization. Bennett and Raab (2003: 123) outline five different types of codes: organizational codes, sectoral codes, functional codes, technological codes, and professional codes. Sectoral codes and functional codes are the most relevant for the purposes of this report. Sectoral codes are sets of rules that, as the term suggests, apply to business or industry sectors as a whole rather than individual firms (as organizational codes would). An example of a sectoral code is the Privacy Guidelines set out by the Security Industry Association (SIA). These guidelines are based on the Fair Information Practice Principles (FIPPs) and propose a series of organizational rules for individual security corporations to build privacy in to their system design when working with clients. Of particular relevance for this project is that the SIA which offers an identifying logo that individual companies can adopt for their websites and other promotional material in order to express commitment to these guidelines (see USA D3.1 and 4.2). Functional codes apply to organizations engaged in a particular activity rather than their sectoral association. An example of this are rules structuring direct-mail or telemarketing activities regardless of whether these activates are done on behalf of banks, insurance companies, or real estate agents (Bennett and Raab, 2003: 125). An example of this in the security field is a compendium of best practices for protecting privacy and video surveillance published by the Department of Homeland Security's Privacy Office (DHS, 2007). Like the SIA's Privacy Guidelines, the DHS guidelines are extensions of the FIPPs of the FTC, and while they are written for government agencies they are intended to be of utility for any entity implementing a camera surveillance system. Codes of practice are voluntarily adopted rules for protecting privacy that are more detailed than privacy commitments, but like privacy commitments there is nothing to guarantee that the organization actually adheres to these rules beyond official pronouncements.

The third model, privacy standards, overcomes this uncertainty by incorporating mechanisms of audit and review so that the organization "says what it does, and does what it says" (Bennett and Raab, 2003: 127). Though not strictly speaking a matter of voluntary self-regulation, the Payment Card Industry Data Security Standards (PCI-DSS) could be considered an example of privacy standards at work. The PCI-DSS provides a framework for all businesses that accept payment cards to ensure the security and privacy of the transaction. Compliance to these standards is assessed by Qualified Security Assessors, which are required before payment cards can be accepted. Because this framework applies to any agency, public or private, that accepts payment cards, the PCI-DSS could be considered a *functional privacy standard*. The Privacy Impact Assessment Process required by the Homeland Security Act of 2002 is analogous to a *sectoral privacy standard* in that it involves a mandatory process of review for all government agencies and initiatives that involve the collection of personally identifiable information. Indeed, this process is essentially the government's 'brand' that a

[2] http://www.ibia.org/association/privacy.php

particular initiative meets existing privacy-protecting standards. However, critics say the drawback of the standard against which these initiatives are measured – in most cases, the Privacy Act of 1974 – is that it is badly outdated by advanced in technology. A logical extension of privacy standards are privacy seals, which are visual marks or brands that "should operate to distinguish the compliant from the non-compliant" (Bennett and Raab, 2003: 131). An example of this is the TRUSTe seal used to evaluate the privacy policies of online shopping merchants and identify those with stringent and robust protections.

As this review suggests, there are a number of models that we can consider as the basis for the branding of privacy awareness and protection in the security industry. We can also see a number of examples of these models in use in the US security field, though none of these examples are without limitations or coexisting within a single program or initiative. In our view, the formulation of a workable privacy brand would have to draw together the strengths of these elements while overcoming their weaknesses. In the interest of doing so and advancing the aim of PATS to "invent a concept of security branding to increase opportunities for voluntary adoption of privacy standards among security organizations," the following elements or 'indicators' of a privacy brand are offered:

- Commitments to the protection of privacy should go beyond general principles about protecting privacy and contain specific rules and regulations about how *specifically* privacy is enhanced by the technologies offered by an organization;

- these rules should go beyond minimal legal standards and strive to meet or exceed the Fair Information Practice Principles of the Organization for Economic Cooperation and Development, or industry- or technology-specific adaptations of these principles, if available (such as the DHS best practices for public video surveillance);

- There should be mechanisms for verifying adherence to these rules, especially if seals or other visually distinguishing marks are used. If such marks are to be more than public relations exercises they cannot simply be adopted by agencies on their own volition but awarded based on the outcome of a process of review, ideally conducted by a third-party.

D. Conclusion

To conclude, we need to consider the question of why individual security firms (or clusters of firms) would voluntarily adopt a privacy brand that reflects these elements. Bennett and Raab (2003: 124-125) explain that self-regulation is generally driven by two main reasons: either to anticipate and/or avoid legal regulation or because there is a direct profit incentive to be privacy-friendly. We see some evidence of both of these at work in the US security field. The former point is reflected by the privacy commitments put forth by the SIA and the IBIA in an effort to counter the possibility of future legal restrictions that would restrict the profitability of the industry. A research paper by IBM reflects the latter point in that it considered how the company can gain a competitive edge over market rivals by proactively adopting privacy-enhancing technologies within its surveillance cameras. The paper outlines how the company's analytic algorithms can enhance privacy by placing varying levels of

protection on the video feed either in the monitoring room or on-board the cameras itself (which they call 'PrivacyCams'). In concluding the paper the authors ask, "why anybody would accept [the] extra burden" of purchasing and implementing this software and hence why IBM should continue developing this product. The authors conclude that entities using video surveillance will either be driven to "do the right thing" by public pressure, or "In the future, it may be required by law that CCTV systems impose privacy protection of the form that we describe" (Senior et al., 2003: 12), and the development of the product would put IBM in an advantageous position over competitors if either scenario were realized.

However, the motivation for self-regulation in the security industry appears to be quite weak, at least in the US. As one of our WP3 interviewees put it, "the economic and political and bureaucratic systems all have incentives to use [technology] to undercut privacy and nobody really has an incentive to use them to protect privacy. The public good of privacy is too diffuse and is not well represented, especially in the United States," and we suspect this is the case elsewhere. Furthermore, one of the common findings of WP3 amongst all partners is that the security industry views itself primarily as a supplier of products to clients, and it is the clients' responsibility to ensure that pertinent laws and regulations are adhered to, not the provider of hardware. While not incorrect, this position is extremely reductionist and can be critiqued on two grounds. The first is that the security industry, like any other industry today, doesn't simply service pre-defined needs but is active in shaping those needs in order to grow the market for the goods it provides. As an active participant in growing the security market by continually unearthing new threats and defining the ways they can be mitigated, it is ethically unsustainable for the industry to disavow any engagement with the issue of privacy protection, particularly given the increasing functional prominence of specialized technical expertise in homeland security today (Klauser, 2009). Secondly, we can critique, as the UK team does, the view from the industry that it simply releases a product into the world. Drawing on an STS line of reasoning, we can invert this relationship to suggest that the industry "builds a world into a product prior to and during its launch" (UK report, pg. 51), and that privacy is noticeably missing in this. In the absence of market-based motivators for self-regulation, these normative arguments provide strong impetus for the industry to proactively embrace the model of privacy as a brand outlined above.

E. References

Aradau, C., & van Munster, R. (2007). Governing terrorism through risk: taking precautions, (un)knowing the future. *European Journal of International Relations, 13*(1), 89-115.

Bennett, C., & Raab, C. (2003). *The Governance of Privacy: Policy Instruments in a Global Age*. London: Ashgate.

Coaffee, J. (2008). Reputational risk and resiliency: the branding of security in place making. *Place branding and public diplomacy, 4*(3), 205-217.

de Goede, M., & Sandalls, S. (2009). Precaution, preemption: arts and technologies of the actionable future. *Environment and Planning D, 27*, 859-878.

DHS. (2007). *Best Practices for Government Use of CCTV: Implementing the Fair Information Practice Principles*. Washington, D.C.: Department of Homeland Security Privacy Office.

Hermer, J., & Hunt, A. (1996). Official Graffiti of the Everyday. *Law and Society Review, 30*(3), 455-479.

Klauser, F. (2009). Interacting forms of expertise in security governance: the example of CCTV surveillnace at Geneva's international airport. *The British Journal of Sociology, 60*(2), 279-297.

Lyon, D. (2003). Surveillance after September 11, 2001. In K. Ball & F. Webster (Eds.), *Intensification of Surveillance: Crime, Terrorism and Warfare* (pp. 16-25). London: Pluto Press.

Monahan, T. (2010). *Surveillance in the Time of Insecurity*. New Brunswick: Rutgers Univeristy Press.

Nemeth, J., & Holander, J. (2010). Security zones and New York City's shrinking public space. *International Journal of Urban and Regional Research, 34*(1), 20-34.

Senior, A., Pankanti, S., Hampapur, A., Brown, L., Tian, Y.-L., & Ekin, A. (2003). *Blinkering surveillance: enabling video privacy through computer vision*. Yorktown Heights, NY: The TJ Watson Research Center.