PATS

Privacy Awareness Through Security Organisation Branding

Report on the Usefulness of Ethically Focused Brand Indicators as a Means of Managing the Balance between Security and Privacy

D6.4 – Synthesis Report

Deliverable D 6.4

Synthesis Report by GB Team

Lancaster University

Inga Kroener

Daniel Neyland

30.04.2010

Project number
230473

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

Funding scheme
Coordination and support action

Contents

Introduction

The overall objective of PATS is to invent a concept of security branding to increase opportunities for voluntary adoption of privacy standards among security organisations. The project studies the degree of privacy awareness across various sectors, firms and across international government agencies that promote or use security technologies. It focuses particularly on biometrics and CCTV as these two merge continuously with each other and imply a whole range of applications such as motion detection, segmentation, object classification and tracking, background and behaviour identification etc. PATS also examines branding and its relevance for a solution in the conflict between privacy and security. Brands are used to communicate not only products services and systemic innovations (such as better security), but also ethical values (such as privacy). Key questions for the project in relation to branding include:

- Can organisations develop a public offering ('brand') that takes privacy into account?
- Can 'brand' communication methods become a way to enhance accountability to the public?
- Is privacy awareness a 'brand' value?

This synthesis report provides an analysis of the results of various focus groups held across partner countries. These focus groups were set up to assess the dimensions and indicators developed during WP5 of PATS. These dimensions and indicators form the basis for the PATS branding model. This synthesis provides an outline of the findings of each partner country; provides an analysis and assessment of the feedback received on the branding model; and culminates in suggestions for changes to the branding model based on the findings of the focus groups and a cross-country analysis of key themes.

The first part of the synthesis document outlines the findings of the focus groups held in each partner country. The major themes to emerge are summarised, and the implications for the PATS project and branding model outlined. The second part of the report provides an analysis of the partner country's national reports, across a range of cross-cutting themes. These cross-cutting themes are the main issues that arise across all country reports. The third section of the report analyses the implications of findings for the PATS branding model.

Country by Country Analysis

Each partner country held a focus group during the months of July – August 2011. The aim of the focus group was to test the indicators and dimensions developed in Work Package 5. These dimensions and indicators are included in this table:

Dimension	Descriptor	Examples
Reflexivity	Thinking, assessing, considering	Internal reports, meeting agendas/ minutes
Information Availability	Displaying, showing	Codes of conduct, reports, documents
Communicability	Talking, advocating, being active communicators	Promoting, advertising, participating
Action-ability	Closing the communications loop	Focus groups, web forums, privacy officers.
Testability	Evidence of compliance in advance of failure	3rd party privacy impact assessments

The focus group was set up to assess:

- Security organisations' interest in ethically focused brand indicators as a feasible approach to managing security and privacy
- Security organisations' evaluation of the specific indicators developed in PATS
- Challenges involved in current security organisation activities and how these might be re-oriented in line with ideas of brands and ethically focused brand indicators and evaluate opportunities for creating brands for security organisations

Each partner country produced a report of their experiences of running their focus group and the main findings to come out of the event. This section of the synthesis report provides an analysis of the national reports from each partner country. This outline is provided in order to offer detail to the cross-synthesis analysis which follows.

Israel

The Israeli research team found that focus group participants were concerned that it is simply too late for ethical branding to be effective in addressing the privacy concerns raised by surveillance systems. Producers are not interested in privacy issues, nor are customers. The public are seen to be unaware of privacy issues. It is only civil liberties organisations who are aware, so may have the most potential in terms of encouraging adoption of privacy branding.

End users (installers) may have more responsibility towards citizens as they deal directly with them, as opposed to manufacturers. Small companies (manufacturers) should not be responsible (they are too small for that). Focus group participants also raised the issue of technologies being manufactured abroad. The following questions were raised: Is it an international or local issue? How can the local influence the international situation?

In the Israeli case, regulation is seen as a pre-condition for self-regulation. Privacy branding is seen as adding extra costs onto organisations and manufacturers (in an already competitive market). The potential for development of privacy standards to encourage larger companies to adopt them (for competitive reasons) was highlighted by participants as one way forward for self-regulation of surveillance systems.

Finally, PETs should be encouraged by stakeholders, and demanded by end users. The public will benefit from the development of PETs. The conclusion of the Israel team was that a market needs to be created for privacy.

Germany

The German research team found that there is a lack of contact between manufacturers and end users (and the public) and that it is therefore difficult to communicate any notions of privacy branding. Furthermore, participants in the German focus group suggested that there is currently only negative publicity about privacy infringements in the public eye, which derives from civil liberties groups. The report suggests that there is a demand for PETs from end users, however sometimes they cannot be installed due to technical reasons. Also, transparency (in this context, transparency is related to making information about privacy-related activities publicly available) is desirable and PATS can potentially have input in this area in terms of policy recommendations.

In terms of the dimension of reflexivity the German report finds that a level of compliance with the law has to be assessed prior to initiating a process of accountability (making organisations accountable in terms of privacy and data protection beyond the law). Participants suggested that both manufacturers and end users claim that they comply with legislation, however they point out that foreign producers do not comply (and that there is a shift in terms of responsibility and blame). This means that however effective legislation and regulation is in the national context, there is still the issue of manufacturing abroad to contend with (in terms of differing data protection legislation, and enforcement of this legislation).

In terms of measuring internal practices, external experts and consultants were seen as preferable, however it was noted that often companies are hesitant in terms of opening up their business practices to external scrutiny. With regard to internal audit this can be conducted by the company's data protection officer, although there was some confusion over roles and responsibilities of data protection officers. Participants questioned whether a data protection officer would only be responsible for an employees' data or customers' data too.

Manufacturers see statements regarding how they deal with information processing and privacy as unnecessary for them as they do not process data. However, potentially manufacturers could issue best practice guides with their products on how to comply with data protection/privacy laws.

Participants also mentioned that some organisations do not make their codes of conduct public for fear of negative publicity or a backlash from civil liberties campaigners if anything is missing or incorrect. Branding was noted as being a process rather than something which can be achieved immediately. The notion of branding (and privacy branding in particular) was linked to accountability (in terms of practices related to privacy), and a good reputation in terms of privacy (and privacy-related activities). The organisation as a whole has to promote privacy (staff need to be trained well and regularly for example).

With regard to information availability, the German report outlines that organisations should provide information on how data is processed and that functions should also be made visible, e.g. if a camera has added capabilities such as microphones. With reference to the dimension of actionability, the German report states that cameras are often unattended and so images are not viewed. This needs to be rectified - systems need to be watched in order to make them more effective. This then provides an opportunity to implement privacy protecting features into the systems.

In relation to the dimension of testability, participants suggested that organisations need to be assessed with regard to privacy practices and then certified, and that these certificates need to be verified and tested. Furthermore, it was proposed that an independent body with responsibility to provide criteria for certificates, seals etc. might enhance trust in the process.

US

The majority view from industry in the US focus group suggested that there is a lack of financial incentive for ethical branding to be successful. Furthermore, there is a lack of legal requirement for organisations to adhere to data protection legislation. However, the problem lies with enforcement of legislation, rather than with the adequacy of regulation; existing regulation is adequate.

Industry participants in the US case saw security as being more important than privacy. They stated that privacy does not require greater protection, and deemed communicability as unnecessary. Furthermore, privacy is deemed as being political in nature; that politicians play up the risks and stir up fears of privacy invasion in order to gain politically (in terms of portraying themselves as the party with the capacity to protect constituents).

With regard to regulation and standards, US focus group participants argued that it is up to the users of surveillance systems to implement the rules of data protection. There was general consensus that involving manufacturers in Privacy Impact Assessments won't accomplish very much in terms of privacy protection, and that it is the end users of systems who are the important actors in this process.

There were mixed responses with regard to discussions of the possibility of the potential for a privacy certification scheme. Potentially a privacy certification scheme could involve the activities of industry actors being reviewed by an industry association or an external third party against a defined set of standards. Successful industry actors would then receive a mark or symbol that they could advertise as evidence of compliance to this framework. In relation to this, participants raised the question of who sets standards, and what the standards would be based on. Would standards be based on the technological, or would they be policy-based? There was general agreement from trade association representatives that privacy standards could be potentially beneficial if set by industry rather than government (this was seen as a positive thing by trade associations, but was not so positively viewed by industry). They also expressed a need for the creation of a market for privacy. The question was raised of how to create that market. There was general agreement that privacy branding would need to be driven by clients not manufacturers.

Poland

Focus group participants in Poland discussed the range of new technologies (biometrics, CCTV, internet related) with the potential to infringe privacy. They discussed the idea that legislation should evolve alongside the technological developments (and at a fast pace), as currently technological developments are outpacing regulation. Further to this, the development of global standards (due to

privacy not just being a national issue, and some manufacturing of surveillance systems taking place abroad) and adhering to these standards is important and fundamental to protecting privacy.

In terms of the legal aspects, there was general agreement that the storage of data should be regulated, and that this should be regulated at the national level. When discussing communication, participants shared the view that sharing information on security is 'tempting fate'; informing the public compromises security and leaves vulnerabilities open in terms of potential terror attacks (for example). So, there is a struggle between transparency in terms of information and security.

In terms of the responsibility for privacy branding, participants held the view that privacy is valued, however it was widely agreed that manufacturers should have more responsibility in terms of the secure storage of personal data and not infringing on the privacy of individuals, and that this should be regulated and monitored at the global level.

UK

The main themes to emerge from the UK PATS focus group discussions centred on: regulation and legislation; privacy and harms; and branding. The issues encompassed under these themes are complex and wide-ranging with overlapping areas, particularly between legislation and privacy (who is responsible, how do we hold people/organisations to account, and so on), and within the issue of regulation and legislation (who is responsible, how do we ensure oversight and effective enforcement of legislation, what are the steps needed to ensure that regulation is able to be enforced, and so on).

Under the first theme of the ineffectiveness of current legislation, discussions centred on the ineffectiveness of regulation of CCTV. It was stated by participants that the UK has a solid legal framework to follow in terms of data protection; however this is not adhered to in general. Under this theme, UK focus group participants also discussed the idea of voluntary codes. The general consensus was that if legislation is not enforced there is little point in talking about the possibility of voluntary codes. Focus group participants also argued that there have only been few Privacy by Design initiatives in relation to CCTV. In terms of offering a privacy brand to the market place this theme suggests that thus far few moves have been made in CCTV (in comparison to other areas) to recognise privacy as a market value and design privacy protections into technology. A further theme of discussions in the focus group engaged with the issue of whether accountability resides with the end user, the manufacturer, or an external body such as the Information Commissioner's Office. A further theme focused on organisations carrying out their own privacy self-assessments or having an independent body to carry out such. In general, discussions around responsibility and accountability veered towards the negative in the focus group discussions, in terms of no one really being accountable or responsible for privacy and enforcing legislation. The potential for independent certification was discussed as a possibility; however, no consensus was reached as to how this might be accomplished in practice. UK focus group participants also discussed the possibility of mapping CCTV cameras and registering CCTV systems. The discussion focused on the impossibility of current legislation being enforced, or adhered to, without knowledge of how many CCTV systems there are in the UK; who runs the systems; and where they are installed.

UK focus group participants also focused on the potential confusion among regulators of CCTV. The discussion focused on the problems of different surveillance commissioners and different codes of practice in the UK. This leads to potentially conflicting advice for practitioners, end users, and the

public. Overlapping regulations, different advice being issued from different or even the same organisation, and the absence of a single body with undisputed responsibility for privacy and data protection was noted by participants as a further reason why privacy protection through legal enforcement was not taken seriously by organisations. Further to this, discussions also focused on the issue of there being too many privacy laws in the UK; and that these laws are far too complex (even for privacy lawyers to understand fully).

Although the emphasis of the focus group was to test the indicators and the potential for branding, the main conclusion that can be drawn from the results is that prior to branding being a viable option, regulation that is already in place needs to be enforced; UK organisations involved in CCTV systems (the manufacture of, the end use of, the installation of, the distribution of) do not abide by current regulation (on the whole, and for a number of reasons). Participants suggest that existing legislation should be enforced prior to branding.

Cross-cutting themes

This section provides an analysis of the partner country's national reports, across a range of cross-cutting themes. These cross-cutting themes are the main issues that arise across all country reports. The aim of this section is to show the major issues and areas of concern (or interest) in the branding model, in the dimensions and indicators proposed by the PATS project, and the areas where change in relation to privacy is needed.

Regulation

The first cross-cutting theme involves regulation. The findings of the focus groups suggest that existing regulation needs to be enforced before self-regulation is possible. Participants voiced a strong view that prior to self-regulation being obtainable or even something that is desirable, the legislation already in place would need far greater enforcement. There was an overwhelming response that existing legislation is adequate, and that the fundamental legal basis does not need restructuring. As an example:

> "At the moment we have a comprehensive set of regulations for CCTV under the Data Protection Act 62 legislative standards. Now, those are ignored. Now, this is legislation and criminal law yet it's ignored by 90% of the organisations with CCTV" (UK Consultant)

> "These things [should] be covered by a legislative framework and frankly it's [about] empowering a legislative framework" (UK Manufacturer)

It was argued strongly that prior to thinking about voluntary codes regulation would need to be enforced. Once this has taken place, it may be possible to start thinking about voluntary codes although the overall response from focus group participants was that making principles and codes voluntary was not the way forward due to conflicts of interest. For example:

> "So if they're totally ignoring the law, to start thinking of voluntary codes … [they] would be no more effective than the one on the Press Council, which is very much in the news at the moment. … asking the manufacturers of surveillance equipment and installation companies to get on board and really promote privacy is a bit like asking turkeys to vote for Christmas because it is almost diametrically opposed; they want people to install CCTV" (UK Consultant)

Whether voluntary or legally enforceable, discussions in the focus groups also encompassed the issue of what sorts of standards should be developed. As an example:

> "The problem becomes what sort of standard do you develop. Technological standards? Policy standards? That's a tough question because the security industry is so diverse. But yes, the idea of being able to buy something privacy-related that has been certified by Underwriters Laboratory or some other association is a good one. I just don't know how that would work in practice." (US trade association)

Therefore, the idea of designing a set of standards has potential in terms of people buying into the idea that something holds a certain level of privacy protection (which could also potentially be a step towards branding), however the issue of competing standards and interests also arose (depicting the difficulty involved in trying to encompass the differing desires of various actors, involved in the security sector, under one 'umbrella' standard):

> "There's a whole range of different competing sets of standards that might be in place at any one time. Standards around evidential quality, which one group of people might be interested in. Standards around what we're talking about here, about protecting privacy, and so on; so a range of interests that might be cohesed together in some way" (UK private sector)

Alongside the issue of competing sets of standards, focus group participants also pointed out the possibility of a need for global regulation (rather than a need to reinvent national legislation). For example:

> "Why do we have to complain about the lack of privacy branding activities of technology vendors in Israel? The technologies are being developed in places like Japan anyway, so they can't possibly be blamed for the lack of privacy branding". (Israel)

This point is also tied in with the issue of responsibility and accountability (which will be returned to later in this analysis), and the potential problem that the PATS project is too state-focused to deal with issues of regulation and responsibility (and reiterating the need for a global rather than national strategy as mentioned above):

> "Who should be accountable for it, who should be accountable for its ethnicity and its proportionality and it ethicality? Who – where do you locate that responsibility? If you were going to challenge it in any way who would you challenge and why and I think this is part of what you're getting at isn't it?" (UK - Academic)

Whether voluntary or involuntary, national or international, there was general agreement across the various focus groups that regulation is the way forward in terms of forming a stable foundation for privacy. This regulation would need to involve penalties (on the basis that voluntary codes will only enable limited progress):

> "We think that we need also to define sanctions against companies and organizations that break these regulations. If we use the issue of privacy as an advantage of branding on a voluntary base, we think that it can be done on partly. While the branding is not enough, we need to use also some legal means". (Israel – Ministry of Justice)

Furthermore, regulation would eventually enable ethical guidelines, which would be devised and implemented due to a public want and push for these principles to be enforced (again with the comment that self-regulation or voluntary compliance will only enable limited progress):

> "Regulation is the best policy measure. The product has to comply with ethical regulations, and this should be enabled by public pressure.
>
> Self- regulation: I simply don't believe in it. The industry is already very competitive, and self-regulation will add another cost component that companies would like to avoid". (Israel – technology producer)

The cost of privacy branding

A second cross-cutting theme that arose was the issue of the lack of incentives for manufacturers to adhere to data protection. Participants voiced the issue of there not only being no (positive) incentives for manufacturers and technology producers to abide by data protection regulation but that

conforming to principles and legislation provides little financial benefit and actually adds more costs to the organisation. For example:

> "My first reaction is that product manufacturers aren't going to want to do this. First of all, it's another level of activity that simply doesn't pay off. How profitable would this be? My sense is that it wouldn't be profitable at all." (US)

Alongside the view that there is little financial benefit for organisations to adhere to data protection legislation, there are also no current legal incentives (linking back to the previous theme of enforcement of regulation being necessary prior to other things happening):

> "I don't think you'll get a buy in from industry because they could lose too much and there is no gain. So to embrace it on any significant scale within the industry, I'm not sure I can envision it. It's an interesting concept but I don't think you'll get the involvement you want because it's not advantageous to business, and there's no legal reason for them to do so." (US)

> "They [installation companies] don't want to know about the Data Protection Act because there's no money in it for them and it just takes time and training" (UK - Consultant)

Again, the issue of enforcement of regulation arises, only in the context of incentives. Participants pointed out that, not only is there little or no risk of punishment, there are actually only negative impacts from taking privacy into account. In other words, those who 'buy-in' to the idea that data protection and privacy is important and should be taken into account essentially lose out in terms of time and money, rather than gaining anything positive.

Designing in privacy

A third cross-cutting theme focused on the idea of Privacy by Design and Privacy Enhancing Technologies (PETs). A general issue that arose out of focus group discussions was that privacy does not have a market value (currently). For participants, the use of privacy enhancing features and technologies should be promoted:

> "The use of PETs should be encouraged, but the question is how? The potential customers of PETs should make PETs a reality by creating demand so that a market for PETs can be formed. The need for PETs should be branded". (Israel)

In the context of the Israel findings (as well as the UK and US findings) there is an absent market in terms of privacy. There may be some consumers interested in PETs but this number may be too small to be sustainable in an economic sense. Privacy enhancing products may therefore be desired but there is simply no market there currently. This implies that in order to bring PETs to the market, there is a need for market stimulation (which is linked to developing a social and market value for privacy, which is returned to later in this report).

Responsibility

A fourth cross-cutting theme to emerge from the various focus groups was that of responsibility. The general consensus across the focus groups was that manufacturers or technology producers are not responsible for privacy protection. This statement was made either in a normative sense – that manufacturers *should* not and *are* not responsible for privacy protection – or as a statement regarding the way things currently stand (without a normative statement regarding whether this is right or

wrong). Within this idea that manufacturers and technology producers are not responsible two (not always separate) views emerge: 1. it is end users who install the system and are responsible/need to conform, and 2. that an independent/external body should be responsible for ensuring privacy protection.

In terms of the first view that it is the end users who install the system and are responsible for privacy, the emphasis is on how systems are used and the variety of potential uses that are out of the control of the manufacturers. The responsibility lies firmly with the end user, and regulation should be set up in such a way as to hold the end user accountable:

> "It's ultimately about the end user, not the manufacturer. It's not the camera manufacturer that sites the camera or designs policy about how cameras are used. It wouldn't make sense to focus on industry for those reasons. It's got to be about the end user." (US – industry representative)

> "It's really not up to the [technology] providers to see if their technologies are used in privacy-protecting ways; it's up to the user. It's really up to the implementer, so that's where the policies, guidelines or standards could be applied, not the technology providers themselves". (US – trade association)

However, for some participants it is not always as easy as simply holding the end user accountable. Firstly, the legal framework needs to be adhered to before anyone can be held accountable. Secondly, some participants took the idea of responsibility one step further to discuss not only issues of responsibility but also potential ignorance on the part of the end user:

> "The point is, the end user doesn't know what he wants, therefore when the CCTV company send him a quote saying – this camera will cover the playground – that's good. He doesn't realise that it needs to say 'facial recognition of a known person', which is the term from the Home Office document" (UK - Consultant)

So, in this case there is unintentional contravention of data protection or privacy principles on the part of the end user. Further to this, the point was also made that CCTV systems are installed as a solution to a specific problem and then forgotten about (which again is unintentional avoidance of data protection legislation, albeit in a slightly different context):

> "They [installers] want to put up a CCTV system and then forget about it, you know. It satisfies an insurance problem that they have, or they're reacting to a crime situation – they had a problem, they think 'we'll put some cameras up' and then, especially with a digital system, they then don't look at it again – it might be several days later" (UK - Trade Journal)

However, focus group participants also raised the issue that for some end users there is an active avoidance of data protection compliance due to the same issues raised previously; that it takes time and money to comply (and that this can be avoided due to ineffective enforcement in terms of regulation).

In terms of responsibility being attributed to an external body, there was agreement that this could potentially be a way forward for developing privacy protection; however the practicalities of such attribution raised some concerns. For some, passing the responsibility onto, for example, a trade association creates problems in terms of knowledge about legislation and regulation:

> "They [trade associations] don't, as far as I know, there is nothing there about privacy, data protection etc. It's more about technical quality than installation. So there isn't anyone really" (UK Consultant)

This was also cited as a potential problem within organisations, i.e. who is responsible internally:

> "You have your data controller and almost all organisations already have a data controller who would automatically double as an officer ... so who is your data controller? Do they have responsibility for privacy and if not who does?" (UK Consultant)

Finally, participants pointed out that many technology manufacturers and importers are located elsewhere, making responsibility for privacy in the product destination country somewhat difficult (and linking this to responsibility and potential for privacy branding):

> "The branding of privacy should be linked to the security technology user and not to the technology developer or installer. There are multitudes of importers who simply bring existing security technology to users and they cannot be involved in privacy branding since they are too small and have no authority over the large producers overseas". (Israel)

Reputation

A fifth cross-cutting theme was that of reputation as providing a potential for change. Participants focused mainly on negative press as potentially providing an incentive for organisations to become more privacy aware. However, fear of loss of reputation could also potentially hinder a company publicising their privacy activities (as mentioned earlier in this report under the German summary) for fear of recrimination by civil liberties organisations if the privacy activities are perceived to be lacking in some area or another.

Financial gain was cited as a method of providing incentive for change in terms of privacy-related activities. The process of gaining financially would involve becoming market leader in privacy; utilising privacy as a unique selling point. The question arises here whether privacy currently has a market or social value? Without a market value the idea of an organisation becoming market leader becomes complex. Does the market arise through companies and organisations placing a value on privacy, or does the market need to be there before companies and organisations will place emphasis on privacy in their products and services?

Challenges of communication

A sixth cross-cutting theme which arose was that of communication. This arose under two contexts: that of communication from organisations to the public, and that of inter-organisational communication. This section will look at the challenges of communication from organisations to external audiences and inter-organizational communication will feature in the following section. One of the main issues that arose in the focus groups was that of an uninterested public, which in turn makes it difficult for industry to foster trust with the public (in this sense then privacy is about trust and building relationships). This has negative implications for branding in terms of the lack of a communication channel through which to 'sell' the idea of privacy protecting products and services. Furthermore, in order to 'buy into' a brand the public would need to trust in the product and/or the organisation, which is difficult to cultivate without effective communication. Added to the problem of an uninterested public, is the issue of industry not currently placing a value on privacy. The US focus group

highlighted this within an example encompassing what is deemed by industry to be the political exploitation of public fears regarding privacy:

> "The preoccupation with privacy and the protection of privacy is misplaced and unnecessary. Frankly, industry is a little fed up with it". (US)

This unsympathetic view towards a need for privacy adds to the problems of communication. The combination of an uninterested public and an industry that doesn't place a value on privacy does not hold much hope for the potential for privacy branding to be recognised by the security sector.

Participants also raised the issue that there is potential for communication to go wrong. In this sense, companies are hesitant to communicate their ideas about privacy and any privacy protection or initiatives they offer due to a risk of negative publicity. It was also pointed out that to be effective, communication needs to be a long-term process rather than a one-off event. Finally, participants also suggested that prior to organisations being able to communicate to the public, the problem of a lack of engagement between producers and end users needs to be focused on. This inter-organisational communication forms the seventh cross-cutting theme.

Inter-organisational communication

The seventh cross-cutting theme of note centred on the idea of inter-organisational communication. This theme focused on the idea that interests of organisations differ, and that technology manufacturers and producers are not interested in privacy (and not responsible for it, as mentioned earlier in this report). In terms of the relationship between technology producers and manufacturers, and end users, participants pointed out a general lack of communication between organisations concerning privacy and data protection. This in turn means that there is little communication to the public. Furthermore, there is no relationship or engagement beyond that of manufacturer and customer/user, as well as little transparency and no shared responsibility.

In terms of communication to the public the various focus groups highlighted a fear of gaining a negative reputation as a major factor in organisations keeping quiet about any privacy-related activities they may enter into. Even if the aim was to promote a positive commitment to privacy the focus groups showed that manufacturers are concerned that the media or civil liberties groups may portray these commitments in a negative light.

Although some of these issues are subtle throughout the partner country reports, there is a general feeling of very separate entities in terms of security organisations and the market.

Negative connotations of branding

The eighth cross-cutting theme centred on the negative connotations of branding. For some, the very idea of branding goes against the fundamental principles of privacy. One focus group participant suggested (and encountered agreement) that branding invades privacy:

> "Do you find that there's a whole thing here that goes against privacy and the very idea of brand that targets an individual, picks them out of the crowd and then targets all of their advertising at them? That seems to me to be the complete opposite of privacy and saying no, I want to sell something to you I don't care who you are almost. Sell stuff, it's all fine. We're not going to then be selling on marketing details because it's all about extending the brand

> and the brand opportunity to the retail part as well. I thought part of this was to you know, reduce some of that." (UK - Public)

For others it was not the idea that branding invades privacy that was the issue, but that brands don't mean anything:

> "You can convince somebody that because it has a fancy brand on it that it's worth ten times more than the one that doesn't have a brand on it ... and it's a way of charging a higher price" (UK – Trade Journal)

> "It is exactly the same [a product with a brand]; almost indistinguishable from the other" (UK - Trade Journal)

So, under this viewpoint brands do not add value to a product; they simply allow a company or organisation to charge a higher price for the same product. However, although the following quote was delivered in a negative context, for the PATS project and the idea of branding privacy the following idea has potential:

> "Just picking up on that I agree entirely that in all likelihood it will become a marketing exercise." (UK - Consultant)

Although for some a marketing exercise may be something negative, in the context of privacy branding this still has the potential to make a positive impact. For instance, in the UK The Body Shop (ethical, fair-trade beauty products) has carved a niche in the market through marketing itself as the most ethically aware cosmetics company; it may be possible in future to develop an equivalent privacy aware market leader.

Implications for the branding model

This section will bring together the various threads of analysis and results from the focus groups in order to draw out the implications for the branding model developed under PATS. The first sub-section looks at the question of who the model is for (who might find it useful, who are we targeting, and so on). The second sub-section discusses the dimensions and indicators developed under the branding model in more specific detail, including potential changes to be made with regard to terminology. The third sub-section discusses the possibility of augmenting the branding model.

Who is the model for?

There were differing discussions of the dimensions and indicators throughout the various focus groups. In the UK the general consensus was that the branding model developed under PATS might be potentially useful for the public sector (and the dimensions and indicators were discussed mostly in the context of the public sector). The general feeling of participants was that branding was not really applicable for CCTV or the majority of users of CCTV systems, there is potential for local authorities to brand themselves as privacy aware. This is interesting in terms of the manner in which participants take up the concept of brands; thinking of local authorities branding themselves, rather than buying an existing brand. This is also interesting in terms of the public dimension and encouraging public participation in surveillance issues. There is potential for local authorities to brand themselves as responsible for, and protecting privacy of individuals; and to impart this information onto the public. However, local authority run CCTV systems are a minority and doubts where raised as to whether this idea could be applicable to the wider users of CCTV.

In the US focus group there was a general agreement from industry representatives (manufacturing) that uptake of the branding model would not be high for industry due to a lack of financial or legal incentive (and in fact would generate a loss in terms of finances, due to time and money spent on training personnel in and implementing data protection principles). Industry representatives also voiced a general agreement that privacy is not in need of greater protection (and for some is too highly valued already). Industry representatives were not easily convinced of the worth of the branding model due to their general dismissal of the value of privacy. In particular, the dimension of communicability was rejected by industry due to the opinion that enhanced communication with the public about issues of privacy and data protection is not necessary. In terms of regulation and complying with data protection legislation there was agreement that it is up to the end users of systems to comply. The branding model could potentially have some value in terms of public authorities and their management of surveillance systems in public space.

In the German focus group the dimensions and indicators were discussed as being potentially useful for others. For example, the dimension of reflexivity was viewed as beneficial to those who do not comply with existing regulation and legal structures. Both technology producers and end users of CCTV systems stated that they comply with existing regulation and that it is foreign producers that need to be held accountable in terms of privacy protection. Technology producers did not see a need to implement anything further than codes of conduct in terms of privacy protection, and that further responsibility and accountability lies with the end users of the systems. The process of reflexivity involves 'making public' privacy practices, which manufacturers are not willing to do for fear of negative feedback. In terms of the dimension of information availability, there is potential for both technology manufacturers and end users to make information available on data processing, storage and access, and so on. With regard to the dimension of communicability opinions were expressed that it

is important for end users of surveillance systems to communicate good practice to the public. It is not deemed to be important for the technology developers and manufacturers. Overall, the branding model seems to be potentially useful for end users of CCTV systems, and dismissed overall by industry.

The Israeli focus group experience shows that privacy is not currently highly valued by manufacturers and technology producers. Regulation needs to be enforced prior to industry placing a value on privacy, and this needs to be a top down approach (from Government). A major concern for the participants in the Israeli focus group was that it is too late for privacy branding and the branding model. In terms of communication, the participants suggested that industry and end users are not interested in issues of privacy and therefore not interested in the dimension of communicability in the branding model. However, civil liberties groups were highlighted as potentially being able to communicate the importance of privacy to the public. In terms of privacy branding in general, focus group participants suggested that technology manufacturers and developers are too small to be interested in privacy branding (as was the case in the UK), however end users of the systems could potentially benefit from the branding model.

In the Polish focus group, the dimension of communicability was discussed in relation to the reluctance of public sector organisations to communicate and disseminate information about security related activities for fear of compromising safety and increase the risk of, for example, terrorist attacks. For the private sector, communication centres on technological capabilities and gaining market position. However, communicability in relation to privacy activities does not feature in their activities. In the Polish case the potential for privacy branding is not clear for either the private or public sector.

In sum, across the different partner focus groups, the question of the focal point for the PATS branding model was consistently raised. The implication of these discussions was that the model would mean very different things for different groups (a cost for some organisations, a focal point for communication for others, a value for civil liberty groups and an irrelevance until legislation is enforced for others). The next section will now address what these implications mean for the dimensions of the PATS branding model.

Problems with the branding model

For many focus group participants, the term ‘branding’ has negative implications (even when not connected to privacy). It is a term used for products and services that do not offer more to consumers but are increased in price. The term also has negative implications in terms of targeting consumers in order to sell an idea, or a service. For some this is in contradiction to the aim of the project; that the idea of privacy branding goes against the fundamental idea of privacy itself (to remain anonymous or unidentifiable).

It is therefore worth considering renaming the model in order to open up discussion, rather than generating a problematic barrier through branding terminology. Potential terms which could be used might include: the privacy model; the privacy awareness model; or the privacy authenticating model.

Added to the issue of the use of the term ‘branding’ the terminology used in relation to the dimensions was not generally or universally understood by focus group participants. Terms such as 'reflexivity' and ‘testability’ were found to be too abstract or semantically difficult. One possibility to make the terminology more accessible would be to change ‘reflexivity’ to ‘awareness’. Furthermore,

the term 'testability' could be changed to 'accountability', utilising a term that is already in the public domain and is understood to relate to privacy and data protection due to on-going discussions, for example by European Union Member States and the Article 29 Working Party. In terms of altering the terminology used in the model it might be beneficial to develop two related models: one academically rich analytic model and a practitioner's direct policy model. The terms used could differ in order to be understood by different audiences; however the fundamentals of the model would remain the same.

The following table is an amended version of the branding model for policy makers:

Dimension	Descriptor	Examples
Awareness	Thinking, assessing, considering	Internal reports, meeting agendas/ minutes
Information Availability	Displaying, showing	Codes of conduct, reports, documents
Communicability	Talking, advocating, being active communicators	Promoting, advertising, participating
Action-ability	Closing the communications loop	Focus groups, web forums, privacy officers.
Accountability	Evidence of compliance in advance of failure	3rd party privacy impact assessments

Augmenting the branding model

Discussions in the focus groups showed that prior to an in-depth analysis of the dimensions presented there is a need for a zero dimension of 'Incentives'; a form of preconditions (based in policy) required prior to the subsequent dimensions. These incentives could be internal/external, or positive/negative.

These incentives could include, for example, boosting internal communication to make sure everyone is aware of privacy as a priority (intra- rather than inter-organisational communication). Although inter-organisational communication is important, prior to this being able to be effective, intra-organisational communication needs to be improved. This provides a foundation on which to build a value for privacy, prior to it being opened up to the public/the market. Until those manufacturing, selling, distributing, installing, utilising, and managing surveillance systems place a value on privacy within their own organisations, conveying privacy as a marketable good in the public domain does not seem a viable option.

A further possibility for incentives is the implementation of obligatory Privacy Impact Assessments (PIAs). These assessments are utilised in organisational and institutional settings to assess and protect against any potential privacy invasions. PIAs are not simply legal compliance checks, or privacy audits; they are used to warn against potential risks but also to mitigate these risks, and to change the development process accordingly. Implementing compulsory PIAs would need a top-down initiative from government to industry (backed up by the threat of fines if PIAs are not put in place). If this were backed up by legislation and enforced regulation this could potentially place a greater value on privacy, both in terms of a social good (that privacy needs to be taken into account and be pro-

tected), and a market value (in terms of the organisation losing out financially). The PATS branding model would then be in a position to shape the way organisations provided privacy aware communicative offerings (based on their PIAs) internally and to external audiences.

There is also the possibility of positive incentives in the form of subsidies for privacy protections. This might take the form of financial incentives for organisations working in the area of Privacy by Design, and Privacy Enhancing Technologies. Further to this, another incentive might be the introduction of awards for privacy. This could be included as part of trade associations annual awards for the security sector. Placing privacy within a positive context, perhaps stimulating organisations to seek Privacy Enhancing Technologies, enhanced communication, accountability and transparency would once again put the PATS branding model in a strong position. Once committed to the pursuit of privacy awareness, organisations could use the PATS model to review and authenticate their privacy related activities.

A further possibility for incentivising organisations to take privacy protection into account is related to the longer-term potential for a cultural shift. The first step towards this would involve greater public participation in the policy process on security and surveillance technologies. Encouraging a dialogue between industry, practitioners, politicians, and the public may prompt the public to place a greater value on privacy and the need to protect it and citizens' fundamental civil liberties. In the longer term, a greater awareness of the need to protect privacy may lead to a cultural shift similar to that of the modern Environmental Movement in the 1960s. The PATS branding model with its emphasis on accountability, transparency and communicability could play a modest role in shaping the emergence of a privacy culture.

The following table is an amended version of the branding model, taking into account the possible changes outlined above:

Dimension	**Descriptor**	**Examples**
Incentives	Incentivising, privacy as a priority	Internal communication, PIAs, privacy awards, subsidies, dialogue
Reflexivity	Thinking, assessing, considering	Internal reports, meeting agendas/ minutes
Information Availability	Displaying, showing	Codes of conduct, reports, documents
Communicability	Talking, advocating, being active communicators	Promoting, advertising, participating
Action-ability	Closing the communications loop	Focus groups, web forums, privacy officers.
Testability	Evidence of compliance in advance of failure	3rd party privacy impact assessments

Conclusion

This synthesis report has provided an outline of the findings of the various focus groups conducted under Work Package 6 by the PATS partner countries, assessing and analysing these findings in the context of other findings (in a cross-cutting thematic analysis), and assessing the implications of these findings for the branding model. The first part of the report has provided a summary of each country's findings. The second section of the report takes these findings and analyses them under a number of cross-cutting thematic headings. This section highlighted the overwhelming similarities across the partner countries in terms of notions and viewpoints on privacy, responsibility, accountability, legislation, and branding. The third section of the report analyses the previous findings in the context of implications for the PATS branding model.

In terms of the implications for the branding model, the findings suggest that the model may be potentially useful for end users of systems, and in particular the public sector. Participants argued that privacy is not the responsibility of manufacturers or technology developers; that it is end users who are responsible for adhering to data protection and privacy principles. There is potential for end users to brand themselves as privacy aware; in particular local authorities installing public space video surveillance systems. Currently, it was suggested that there is no financial or legal incentive for technology developers and manufacturers to adhere to data protection legislation or privacy principles. To make the model relevant for developers and manufacturers it was suggested that incentives were required (see below).

With regard to the terminology used in the branding model, this report has shown that there should be a consideration of changing the terms used both within the model, and for the model itself. For the majority of focus group participants the term 'branding' has negative connotations. Changing the name of the model should therefore be considered. Potential names for the new model were suggested. Furthermore, changing certain terms within the model should also be considered as these proved difficult to understand. An amended version of the branding model for policy makers was presented in this section.

The final section of the report provides suggestions for augmenting the branding model. This section highlighted the need for a zero dimension of incentives (which are included in an example amended table at the end of the section). These incentives are a form of preconditions (based in policy) required prior to the subsequent dimensions. These incentives are shown to be potentially internal or external, and positive or negative. This zero dimension for the branding model potentially solves the issue of a need for regulation to be enforced prior to the possibility for self-regulation, or privacy branding. Incentivising organisations to place a value on privacy (whether through subsidies, risk of fines, or other means) may stimulate organisations to seek Privacy Enhancing Technologies, enhanced communication, accountability and transparency, which would, in turn, put the PATS branding model in a strong position.