PATS

Privacy Awareness Through Security Organisation Branding

Ethically focused brand indicators Report *including a method to find out and categorize ethically focused brand indicators*

SEVENTH FRAMEWORK PROGRAMME

Deliverable D 5.4

Report by German Team

Centre for Technology and Society

Carla Ilten

Daniel Guagnin

Dr. Leon Hempel

14/02/11

Project number
230473

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

Funding scheme
Coordination and support action

Inhaltsverzeichnis

1 Introduction

This report is the final report of Work Package 5 which is a core package of the PATS project, which was dedicated to develop a process for privacy branding. Branding is understood as a way of communication between different actors in the security market. The approach of enhancing privacy through branding is situated in the context of self-regulation, CSR, ethical branding/business ethics and ethical consumerism discourses.

The communication about privacy and data protection is often considered as problematic from security organsations, because civil liberty campaigners see no other possibility to encourage a debate than scandalizing privacy infringements. However we propose a proactive dialogue about privacy concerns and solutions which gives security organisations the possibility to present themselves as privacy sensitive and become visibile in the privacy debate through a positive reputation.

First (section 2) we will shortly reconsider the findings from the preceding work packages. Afterwards (section 3) we will conceptualize what our approach for an ethical branding in regard to privacy. We will then contextualize our branding approach with the different types of actors we elaborated during Work Package 2. Finally we give a first outline of how the materialization of an ethical branding process can be kick-started.

2 The WP5 approach – a methodology for developing ethical branding indicators

2.1 Empirically founded models

The PATS concept of branding as a process is based in the understanding we developed of the respective security fields after conducting extensive empirical work. All conceptual elements of ethical branding as put forward here are derived from empirical findings about structures and processes: typologies of security organizations as well as the relationships between the actors in the market are represented in our structure and actors model. Insights about the quality of those relationships have informed the dimensions of ethical branding we have developed.

Methodologically, the empirical findings of the partners were integrated during project meeting discussions and through synthesizing reports at the end of Work Packages 2 through 4. These procedures of generalizing from the data necessarily give some cases more weight than others and block out details in favour of broader concepts that can be applied across the national regimes. Where important differences exist, such as in typologies and actor relationships, it is possible to adapt and re-specify our general concept accordingly.

One important insight from PATS' involvement with security organizations, but also with proponents of the “accountability” discourse, is that regulatory models – especially self-regulation – require down-to-earth knowledge about the everyday practices in the respective field. A relatively ambitious idea such as ethical branding cannot be transferred from other industries to the security field easily, but is a journey that must be set about with deep knowledge of the real structures in place.

We will now give a short summary of the main findings from preceding Work Packages that informed the conceptual work of WP5.

2.2 Security regimes

WP2 has resulted in a qualitative as well as quantitative understanding of the development of current security regimes and industry structures in in the partner countries. The task was to structure and map the field of civil security in a reasonable and systematic manner on the basis of a general historical reconstruction since 1989 and thus provide the "big picture" while at the same time offering a comparative view on the partners' countries.

A basic variable of security regimes is the prevailing **notion and definition of "security"**. While the partners concluded that Finland, Germany, Poland, the United Kingdom, the United States of America and Israel had very diverging notions of security and privacy, one important common tendency concerns the qualitative extension of the term. Safety and security are ever more into new concepts of security – "comprehensive, holistic, networked, global security". The convergence of different securities into one seems to be both a rhetoric strategy for legitimising institutional centralisation, but is also triggered by security technologies that allow multiple use and integration, for example in monitoring devices.

WP2 analysis also showed how the extension of the security term and hence scope is widely justified with new threats. **Securitization** means not only an extension of security discourses, but also of the security market. An increase in private security actors with more and more competences can be diagnosed for all countries in the project. The teams compiled overviews of security organisations in their countries and developed typologies that roughly describe the organisational ecology in the security sector – for example, security technology providers were distinguished from service providers. Security technology producers were again broken down into systems integrators and specialised technology producers in some countries. Public agencies and industry associations were agreed upon as distinct types as well.

Another important development concerns the **role of technology**. Our analysis has worked out the importance of the rise of the network paradigm – both technological and organisational – and related processes of convergence. These can be observed for example in the field of CCTV where digitization leads to a convergence with biometric technologies. A whole new sector has emerged with the IT security industry in response to the new threats produced by the diffusion of Information and Communication Technologies themselves, and the spread of networks such as the Internet. In all, surveillance is becoming ever more technologically mediated and privacy and data protection problems become even less visible to the surveilled consumers and citizens.

WP2 has also discerned the differences between PATS' focus technologies **CCTV** and **biometrics** with regard to discourses, regulation and expectations. While CCTV is a "local" technology, the significance attributed to the more "techno-science" biometrics is much higher – especially within the EU integration framework – because of its perceived abstract possibility to identify humans – stripped of local issues, cultures, places and norms. Video surveillance is being revived conceptually through digital IP video networks. Automated surveillance mechanisms under the network paradigm perpetuate privacy concerns when data is habitually collected.

2.3 Privacy awareness

The third Work Package set out to collect data on the levels of privacy awareness within security organisations. The typologies from WP2 informed the study population and selection of interview partners. In general, relatively **low levels of privacy awareness** were found in most companies interviewed. Interviewees did not always show an understanding of privacy/ surveillance problems and were mostly oblivious to the exact regulations.

Still, differences between the types became apparent. When it comes to service providers, it depends on the national context whether privacy is even a perceived issue. The European reports portray a very low-threshold and barely professional **security service market** where minimal wages are a much more pressing issue. Companies are often very small. State-of-the-art corporate identity and branding is only performed by very large multinational companies such as Securitas – an important insight for PATS' ethical branding scheme.

Technology producers were generally more aware of data protection as a concern for their organisation, but from a very technical point of view that did not extend beyond data security as a concept. Systems integrators were more likely to accept responsibility towards consumers and citizens than specialised hardware producers who only communicate with clients.

This brings us to the most important insight from the interview process: the **opacity of market relationships** within the security sector. Our analysis shows that that the market structures in the security field are obscure to the extent that no incentives for self-regulation are perceived by the actors involved. Security actors are clearly interested in making a profit and do not have sufficient intrinsic motivation to kick-start self-regulation. Demand for more attention to privacy would have to be forced upon these actors, but no one currently articulates this demand within the market. Most interviewees believed that consumers has no particular interest in privacy protection, inferring from careless user behaviour at Social Networking Sites. Not only are market relationships indirect, but **citizens and the public** are rarely even represented in the market at all. Privacy cannot translate into a means of monetary regulation in the marketplace in this set-up.

2.4 Symbolic representations

What is more, security companies tend to support obscuring discourses about threats and security through their communication strategies of naturalisation and invisibility. Work Package 4 looked at the existing symbolic representations of security agencies and functions in the industry and found that privacy is extremely weakly represented in advertising, public signage, brand symbols, texts, and websites. Security and privacy are depoliticized through opaque imageries of potential threats, allegedly vulnerable individuals (women and babies) and through ever rising technologisation. The security industry takes part in the securitization discourse and the employed communication strategies do not invite critical discourse about security and privacy or surveillance.

Recommendations for ethical branding indicators from 4.3 include the specification of general statements and privacy principles, a clear departure from minimal legal standards, and the implementation of mechanisms for verification.

2.5 Where do we stand? Reviewing the PATS premises

In all, our research in the previous work packages has shown that it is important to move beyond mere legal regulation of privacy – or rather, to bridge the gap between provisions and practice. It has also shown that self-regulation cannot be expected to spring up where actor constellations and market mechanisms are structured such as we found them in the security sector. While ethical consumerism is creating powerful demand structures with regard to environmental awareness and social justice (cf. Organic and Fair Trade markets), virtually no pressure or pull is felt by security companies. Different types of organisations exhibit different levels of awareness, but active ethical branding that focuses privacy is a long way from here for most of them.

Accordingly, the PATS concept for ethical (privacy) branding is going to consist of an ideal type composed of a number of graded dimensions. The dimensions will build on each other so that a roadmap for long-term development can be formulated on their basis. The concept is thus intended to be used as a blueprint by security companies who wish to work towards privacy aware practices and communicate about this.

2.6 Ethically focused brand indicators: towards privacy branding

This section describes the methodology we used to develop our ethically focused brand indicators.

2.6.1 Desk work on branding

The development started out with a literature review about “branding” and “ethical branding” as social, economic and historical phenomena. This provided the basic knowledge to support the development of an adapted branding model.

2.6.2 Workshop and e-Process

In a three day workshop in London, the research teams came together with the material collected during the preceding work packages. In a first step we reconsidered the actor constellations we had found in the field and generalised them into a model. The final reports of work package 4 already opened up a perspective towards ethical branding inspired by our research on security actors' symbolic representations, informed by our collective knowledge on security regimes (WP2) and actual privacy awareness and practices in organisations (WP3). With these outcomes in mind, we worked out the basic dimensions of privacy awareness and communication.

2.6.3 Case studies into indicators

The creativity of joint sessions was complemented by separated sessions in which the national teams checked the outcomes of the joint discussions against their collected material of the national context. The teams extracted cases for the dimensions from the material in order to illustrate possible implementations and list indicators for the dimensions. In the conclusion of their reports every team drafted a blueprint of an ideal ethical brand. This "ideal type" includes both indicators we found and which have an exemplary function and indicators that we derived from obvious failures and weak spots. The teams' results were in turn discussed in a joint session where a final version of the branding dimensions was agreed upon.

3 Conceptualising ethical branding

Work Packages 2 through 4 have laid out the groundwork for a comprehensive model of branding in the security sector that incorporates actors, their relationships, and the communications that take place within this social space. The following sections will describe in detail how we conceptualise branding as a process that operates in this framework of *structures*, *processes* and *ideas*.

3.1 Branding as a communication process

After a survey of "branding" as a social, economic and historical phenomenon and its academic repercussions, we set out to determine our understanding of branding within the context of the PATS project. Branding as we conceptualise it does not just consist of imagery or a logo – the visible hallmarks of "corporate identity". Branding here is conceptualised as a communicative process between the brand creator or owner and the audience of that entity's communicative acts.

Conceptualising branding as a process means that it is not perceived as a static state, but as evolving over time and in space. A brand as expressed through images, logos and value indicators is a cultural artefact that represents a snapshot of this evolution of constructed meaning. Brand meaning is co-constructed by a number of actors who take part in creating a brand, perceiving a brand, re-defining a brand, and possibly extinguishing a brand.

This view underlines the ambivalence of branding for the brand owners: communication and self-representation implies vulnerability. As the 5.1 report on branding states, "the brand, whilst being a valuable asset and contributing to corporate reputation is also very vulnerable and its ethical reputation can be easily dented."

3.2 Types and roles of actors

What entities, then, are we looking at? At this point, we can revisit our typologies and WP3 results and list the actors whose communicative acts are the focus of this branding concept:

Universal types in all partner countries	Details
Security Service Providers	Distinction between small & traditional vs. Large & modern companies
Technology Producers	Distinction between systems integrators and specialised technology producers (manufacturers)
Associations and Networks	Industry associations and meta-organisations in the security field
Consultancies	Consulting for security management, IT security, data protection
Research institutions	Security technologies and management research
Specific types in some partner countries	**Details**
Aviation and Defense	Companies that extend their business to the civil security market
Network Security Organizations	Organizations that research or synthesize networks of data for security purposes
Non-security organisations in the field	**Details**
Consumers of large-scale security	Airports, Public Transit, Cities, and other clients of security companies
Stakeholder organisations/ privacy advocates	Privacy and data protection advocates, civil liberties groups, activists

Table 1: Types of organisations and actors in the private security field

The most important distinction between the types of organisations in the security industry listed above is their role within the market as either

- **provider** of security (technologies, services etc.)
- or **client** (the buyer of security technologies, services etc.)
- or **citizen**[1] (wild card for all affected by the production and implementation of security technologies and services, and systems of surveillance)

Of course, companies can fall in both the provider and client role when for example a systems integrator buys specialised hardware from another provider to assemble complex systems that will be sold further. Typical clients include government agencies, companies, public transport providers, airports, shopping mall operators etc. who buy CCTV surveillance systems or hire security personnel. Citizens come as citizens, employees, consumers, and passengers.

What is important here is the actors' role in terms of demand and supply and its impact on privacy protection. So what are the elements of branding processes among these actors?

3.3 Structures, ideas and processes: a branding model

As the above examples indicate, providers, clients and citizens figure very differently in the diverse constellations that can be found in the security field. WP3 research has clearly worked out the fact that technology providers are almost generally unknown to citizens, for example in transport environments or at the workplace. It is not easily discernible for the subway passenger who produced the dome camera in operation, and what algorithms may run on the video material, or how data can be stored. This information would have to be relayed by the client, the transport provider. The client is the main branding actor in this constellation, but security comes as a by-product of the service utilised by the citizen. Comfort, punctuality and frequency of service are probably more central to branding efforts by the client in this scenario – if any: public transport providers offer an infrastructural service with relatively little alternatives.

[1] Some discussion has been held between project researchers on all of the above terms. They are relational (companies can be both providers and clients), and especially the residual category of the people affected by security is difficult to grasp in its complexity. While some literature uses the term “consumer”, we thought this too narrow an economical definition which blocks out the lack of choice in many of the security arrangement, and plays down the political dimension of surveillance. While we are aware that “citizen” also carries an exclusive taste, we are using it in a sociopolitical sense to grasp the entirety of an individual as a member of a social, economic, political, and cultural space.

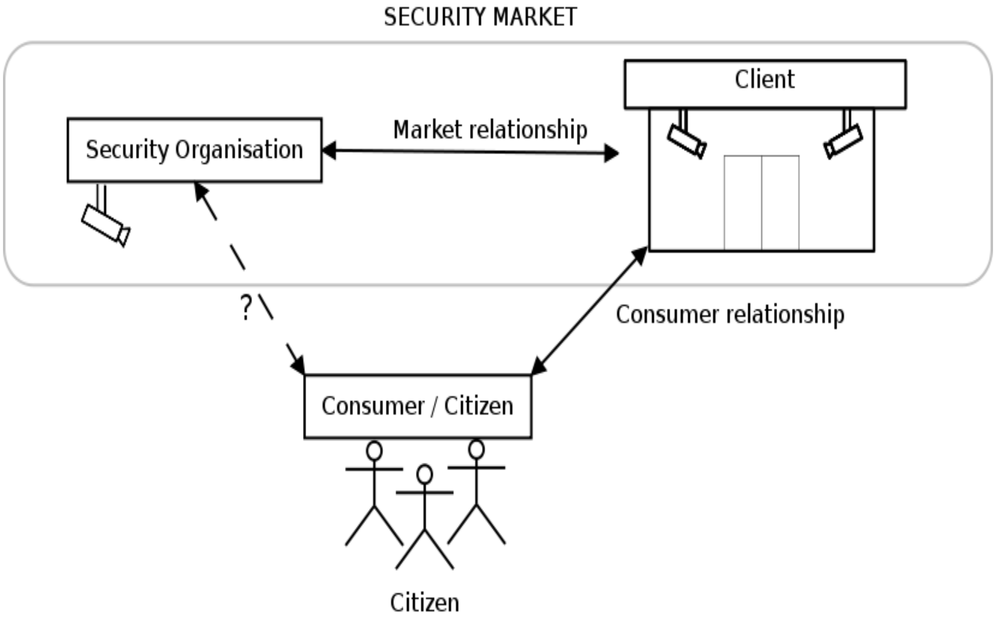
Another scenario is more likely to result in communication about privacy and data protection: the introduction of biometric access control systems at a company's facilities. Here, employees are represented through a works council in many cases, and a more direct relationship between provider (systems integrator), client (company/employer) and citizens (employees) can be established – if the actors are willing.

Security service personnel is often branded through uniforms, so that that their affiliation is visible. The very concept of security services requires visibility. Passengers may notice that one airport engages staff from company A while the other airport hires B staff. The airport's branding and the security company's branding merge into one experience.

It becomes difficult to walk the streets without being captured by a camera, or even realise in whose space – public, private? - one is moving about and whose camera is watching – so how are consumers to exert market influence by pure selection? Accordingly, the actor we expect to demand privacy – the data subject – is utterly uninformed and cannot easily exert influence within the market of security technologies and services.

These examples highlight the different **structures** we find in the security sector. The “immediately fixed frameworks of interaction, the roles assumed by actors, the actors themselves in those frameworks and market pre-conditions that structure relations between actors” (D5.1) make up the complex structures that govern different parts of the security field.

WP3 has given important clues about the specific market relationships between the actors and the mechanisms that underlie their interactions. We have argued that the market structures in the security field are obscure to the extent that no incentives for self-regulation are perceived by the actors involved. Security actors are clearly interested in making a profit and do not have sufficient intrinsic motivation to kick-start self-regulation. Demand for more attention to privacy would have to be forced upon these actors, but no one currently articulates this demand within the market. Not only are market relationships indirect, but citizens and the public are rarely even represented in the market at all. Privacy cannot translate into a means of monetary regulation in the marketplace in this set-up. Missing communication channels facilitate the strategies of accountability shifting that we observed. Resulting from these findings, we can draw the simple conclusion that privacy and data protection cannot be supported through market mechanisms when there are no direct market relationships between those interested in privacy and those interested in the commercial success of security products.



These observations have obviously challenged the PATS project’s premise that self-regulation can be furthered through marketing activities, dialogue and the construction of privacy awareness as organisations’ unique selling points. In our further conceptual work, we have continued mapping the markets and actors’ relationships and roles in order to point to those missing roles (e.g. a popular privacy watchdog organisation) and functions or missing communication channels that inhibit self-regulatory incentives.

Within this actor model, every actor has a particular self-image and perception of their environment, as well as **ideas** about privacy, data protection and other values related to the security field. These ideas can be discourses that are shared among e.g. providers and clients, such as the threats/securitization discourse described in WP2, or a self-regulation and compliance discourse that companies share with their public and investors. Important ideas put forward by security actors we observed in WP3-4 are narrow definitions of privacy (data security), the “natural” (not social) character of threats and accordingly security measures, and the belief in total control through networked security (“cybernetics”/convergence/ubiquitous surveillance discourse). These ideas are shared with and sometimes rooted in political discourses, e.g. the U.S. Homeland Security policy after 9/11, or the Internal Security extensions in Europe.

Importantly, producers and clients exchange ideas much more readily than producers and citizens, as we have shown. Security actors often do not know how security technologies are perceived by the surveilled, or how security measures affect the contexts that they are employed in. This lack of exchange is rooted in the structures that we have described above.

With regard to branding, these structures are accordingly of relevance to the interactions and communications that take place between actors: the actual branding **processes**. The self-presentations of producers are yet rarely aimed at “the citizen”, but at clients and investors. Within these communication processes, privacy is not a relevant topic, as our analysis of interviews and corporate communication has shown. Perceptibility of security technologies is often reduced to signage that is posted next to camera surveilled spaces. Service provision entails more visibility because of staff presence. Companies such as Securitas and ADT outfit their workforce with uniforms that carry the firm logo. While their presence is stronger by default, privacy does not figure in this branding communication either.

3.4 Mapping privacy awareness onto the branding model

The general term “ethical” branding which we use refers both to the quality of the branding process – communication – and the content of branding – privacy. The questions we are posing are both “does this company's branding incorporate ethical issues such as privacy?” and “does the company go about its branding in an ethical way?”. As the 5.1 report stated, the “idea of an ethical privacy-aware brand is one in which structures and sub-processes are incorporated or changed so that awareness, commitment and discourse over privacy impacts can intervene in the brand as processes model.” More specifically, in the security sector this means that citizens get a chance to enter the branding discourse amongst security providers and clients.

The branding model – consisting of structures, ideas and processes – provides us with a very abstract framework of branding in the security field and is unspecific enough to be transferable to other industries. For the purpose of developing ethical branding concepts for industries, it can be used to systematically evaluate the empirical quality of branding and communication processes by investigating the present (market) structures, the actors' ideas and rationales, and the relationships in place.

Our research about privacy awareness of security organisations has shown that we need to differentiate between the individual organisation and the market structures it is embedded in. We have encountered very different levels of privacy awareness and reflexivity in some organisations who operate in the same market. Branding thus begins within the organisation in question and its ideas – which are highly dependent on individuals and their interests, education and competences, as we have found, but also rooted in organisational history and structure.

The organisation's interfaces with other organisations and individuals provide opportunities for communications. At the same time, these structures also constrain an organisation's actions. Privacy aware producers will not be able to pull off privacy enhanced products when their clients are not willing to pay – and clients will not be willing to pay unless consumers exert pressure. If one link in this market mechanism chain is broken – which is what we have observed – the producer's branding process will not reach through to the citizen actors.

On the other hand, market structures and industry cultures can influence organisations positively when for example Corporate Social Responsibility activities become so common that it would be a disadvantage to remain behind. In the case of data protection, the emergence of data protection consultancies is a welcome complement to the individual organisations' competences. These new actors not only introduce expertise, but also voice criticism, possibly within the public sphere, and thus rock the structures and processes.

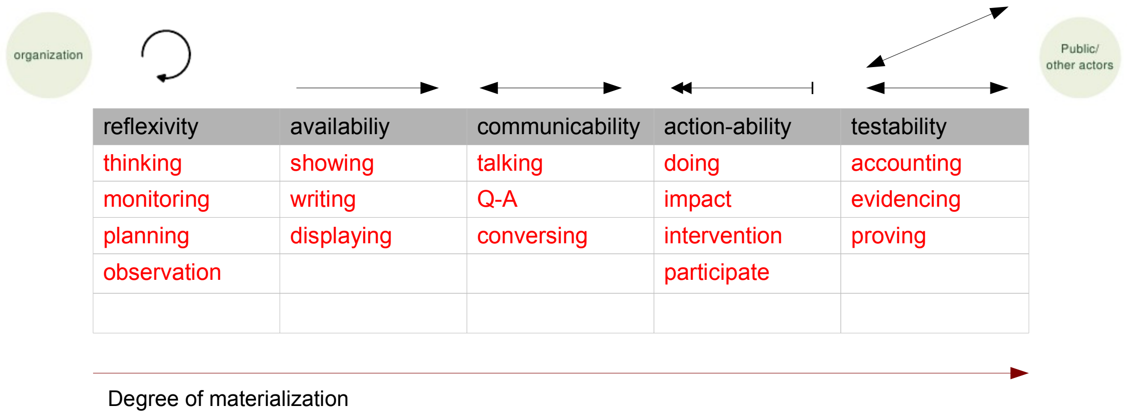
Our model incorporates the idea that "an ethical branding regarding privacy would allow citizens to intervene in the factors that influence the brand." Co-construction implies that companies' self-representation and communication can be scrutinised much more closely – resulting in an ever more exact alignment of word and action. The next step towards ethical security branding is to determine *how* branding processes can be altered so that opportunities for intervention open up and co-construction with other actors and citizens becomes real.

The model we have introduced is useful to find the "weak spots" and missing links in the organisations, market structures, and communications when it comes to privacy awareness and communication. This is precisely what we did in order to "reversely" formulate the structures, ideas and processes that make for ethical privacy branding. We have chosen to conceptualise the "ideal branding process" in terms of dimensions. The examples of indicators we are giving are derived from cases we have researched, or from other industries where practices of ethical branding are more advanced. The ideal ethical brand is a composite concept of bits of reality that we have found – no actor has been found to exhibit high levels of all of the dimensions, and it is unlikely that this will be happening soon. By developing this ideal, we not only gain an analytical concept, but also shed some light on the path that needs to be taken in order to make some progress in transparency and accountability.

3.5 Dimensions of an ideal ethical brand

The dimensions of an "ideal ethical brand" reflect the normative goals of transparency and accountability – the match of word and action and the means to prove this match. Security actors need to develop their privacy awareness and at the same time communicate these changes in an upright way. We have condensed these normative goals into a number of dimensions that would define the contours of an ethical brand. The following table provides an overview over the dimensions, including synonyms that clarify the dimensions, and arrows that indicate the direction of communication between the focal organisation and its environment.

Ethical Branding Dimensions and Operationalization



reflexivity	availabiliy	communicability	action-ability	testability
thinking	showing	talking	doing	accounting
monitoring	writing	Q-A	impact	evidencing
planning	displaying	conversing	intervention	proving
observation			participate	

Degree of materialization

Each dimension is a continuous rather than discrete concept, and for now these dimensions are left as qualitative concepts, though it is conceivable these could be converted into quantitative variables in the future. Furthermore, each dimension ideally builds on the preceding dimensions, a lower-order dimension facilitates the following dimensions. It is only by satisfying all dimensions to a sufficiently high degree that an ethical brand can be said to be materialized, which we understand as being the ongoing co-construction of a culture of privacy in the security field, not an inert and stable visual or material artefact closed to development in light of criticism and debate.

We will repeat a short description of the dimensions here from report 5.1 and proceed to suggest how organisations could go about "materializing" ethical branding with a focus on privacy.

3.5.1 Reflexivity

Reflexivity refers to the extent to which an actor reflects upon their activities/behaviours and alters them in relation to how they impact others. Reflexivity is thus inherently self-referent, as the circle above the dimension indicates in the table. In the context of PATS, the dimension of reflexivity asks: does a security actor reflect on the impact of their technologies and activities on personal privacy? Are they aware of the potential impacts of their technologies, or do they simply 'release' them into the world?

In many ways, reflexivity is a 'backstage' activity that takes place in boardrooms and internal communications, which poses some difficulties for recognizing and providing evidence of this dimension from our external perspective. However, organisations can communicate their internal state of reflexion through structures or processes. Structural indicators of reflexivity might include the existence of powerful privacy officers or departments within an organisation, the existence of institutionalised activities of reflexion such as regular consulting cycles (including privacy issues) or participation in research projects. These activities can be communicated through representations of structures in reports or websites, and through the publication of internal documents such as meeting agendas or minutes discussing privacy.

3.5.2 Information Availability

This second dimension measures an organisation's efforts to make statements about their privacy awareness and standards publicly available. This is closely related to the material that constitutes the dimension of reflexivity, such as internally-oriented documents, reports, etc. Availability, however, refers to material that is specifically oriented towards an external audience. This material can range from brief pledges and principles to highly detailed expositions about how an actor’s institutional rules, procedures, or technologies and their role with regard to privacy.

Typical examples of information made available include documents stating Privacy Principles, white papers, and compliance reports. Both the degree of information depth given and the quality of availability can vary: the usability and ease of navigation of a web interface can be crucial for information seekers. This dimension moves our focus from the “backstage” of the organisation's internals to the front stage, more specifically: its “showcase”.

3.5.3 Communicability

In contrast to the mere existence of the material captured within the dimension of Information Availability, Communicability refers to the extent to which an actor enters a two-sided communication process about their privacy commitments with others. The duplex quality of this communication is emphasized in the double arrow above the dimension in the table.

Communicability can of course be realized to very different degrees: a security actor can be generally open to questions or comments, but they can also create dedicated communication channels, such as a telephone hotline for a particular product or issue, or a dedicated website for e.g. compliance that features the names and addresses of specific contact persons. This dimension thus emphasizes the “listening ability” or responsiveness to feedback on the part of the security actor; the higher the responsiveness, the more an organisation engages in public discourse.

3.5.4 Action-ability

Whereas communicability measures the quality of the communication loop between the security field (private and public actors) and citizens, action-ability is a dimension we use to focus the impact or outcome of these communicative acts. Impact is understood in terms of changing the behaviour – attitude or actions – of the security actor. This is qualitatively different from communicability and shifts the centre of action to third actors, especially citizens, which is illustrated by the reversed arrow in the table.

Indicators that help measure impact are changes in organisational behaviour such as changes in products or services that represent a reaction to public pressure or input. Ideally, companies could involve citizens and experts in institutionalised events that provide space for action-ability such as workshops, focus groups or more product oriented test runs. Impact can then easily be documented and published.

3.5.5 Testability

This dimension is the fulcrum by which any of the above dimensions turn. Testability refers to processes by which a security actor is open to the review of the impact of their products/service/business on personal privacy by external actors. Internal reviews or reviews conducted by government are a step in this direction but fully independent, third party reviews are more robust. Ideally, such processes will be proactive and in advance of failure. This could range from evidence of reviews conducted by internal privacy officers (less robust) to periodic external reviews by independent, external actors (most robust). This could result in the award of a ‘seal of trust,’ such as the TRUSTe seal for web-based commerce, though such seals would have to be awarded by external actors to be considered robust (rather than self-adopted). This dimension covers the much discussed “principle of accountability” in that ideally, structures for providing evidence should generally be put in place by companies who engage in ethical branding. Without testability, co-construction remains skewed because too little leverage would be given to critics and observers in order to develop a trustful relationship.

3.5.6 Materialisation

To sum up, the above described dimensions build on each other to materialize a process of communication and action that takes place within a company and in relationship with its environment. As analytic dimensions, they make up an hypothetical ideal ethical brand which fulfils all of the dimensions to a high degree: we can imagine a company that is highly reflexive, questions its actions and their consequences, and uses external expertise to improve itself. Values that include ethical branding will be spread within this organisation and will be known by most employees, leading to a high identification with the practice of ethical branding. Resources will be committed to generating information and making it available; channels of communication will be created for specific issues and products. The company may engage in public discourse via media and events, and become active in industry associations. Citizens and clients will be invited to join for “input events” or platforms and impact by citizen criticism is documented and made available. Lastly, independent experts are regularly invited to verify the claims made during the branding communication. Citizens can explicitly ask for verification.

Obviously, ethical branding needs to be an ongoing process involving all of the dimensions – just as product development is a cyclical, recurring activity, information needs to be prepared regularly and verification needs to be provided at sensible intervals. Both organisation and context are dynamic, and so should the branding process be.

4 Back to the field: actor types

Now that we have an abstract idea of what makes for ethical branding in companies, how does this pan out for the security actors we have researched? Our typologies indicate that security companies come in very different shapes and colours and accordingly have extremely different starting points when it comes to the journey of developing privacy awareness and ethical branding.

The actors that this concept focuses are technology producers, their clients, and security service providers. The basic PATS claim of “raising privacy awareness through privacy branding”, branding relates to companies – the brand owners. A central project premise was that in line with current self-regulation discourses, branding of privacy could amount to a competitive advantage for companies. We have shown that this is a long shot for most of the actors we have researched, but especially for some types. It is particularly sobering to realize that advanced self-regulation does not spring up independently of market pressure and monetary mechanisms. What we have found, though, are instances of heightened reflexivity in organisations and an associated openness to discourse and influence. While individuals can make a great difference in organisations, our WP3 experiences have highlighted some general structures of opportunity and hindrance for ethical branding.

4.1 Ideas: values

Reflexivity as the basic dimension of ethical branding is a prerequisite for development. While technology producers were found to have more inclination to discuss privacy (as related to data protection), privacy awareness and the sense of responsibility was still relatively low, as our description of “accountability shifting” towards citizens has shown. Reflexivity here means to recognize that products and technologies do impact societal development and social structure, independently of compliance with legal norms – consequences are always produced along the way. It makes sense for technology producers to make use of external resources for raising their reflexivity. Associations and consultancies are available for the industry and privacy is an emerging field of expertise in some countries. The major hindrance for ethical branding is the self-perception as “neutral” and quasi outside of society - “just a producer”. Whether or not a competitive advantage is perceived is dependent on the producer's exposure to clients and consumers. Systems integrators are in a good position to take up reflexivity practices compared to specialised hardware producers, since implementation and consulting is often part of their portfolio, and their range of clients is broader.

Security service providers, on the other hand, are still struggling with professionalisation issues in Europe and rarely perform branding at all. Reflexivity is impeded even more by values that are in direct contradiction with privacy goals. Associations play a vital role in industries that are fragmented with many very small companies. We have observed that larger, transnational companies tend to incorporate more corporate social responsibility goals. While the state of things suggests that ethical branding with regard to privacy is a future vision, it also means that the opportunities to gain competitive advantage are great. The more private security actors are entrusted with public functions, the higher the requirements will become.

Ultimately, reflexivity depends on both organisational culture and on the resources – financial and human – available to companies. Our findings from the field suggest that considerable impulse from external actors is crucial for developing more reflexivity. Research projects like PATS themselves contribute to awareness and reflexivity when interviews are conducted and workshops held – they set an agenda and inspire individual change makers.

4.2 Structures: relationships and new actors

Apart from reflexivity, all of the dimensions necessarily include awareness about or the involvement of third parties such as clients, citizens, or experts. Associations and consultancies can play an important role in some of the dimensions. Reconsidering our WP3 findings about low privacy awareness and opaque market structures, both reflexivity and information availability represent absolute requirements for change. Security organisations currently perceive no need for communication with stakeholders. This is of course a catch-22 situation: will reflexivity have to develop first in order to build new communication relationships, or can reflexivity only be heightened by the involvement of external actors?

Our research suggests that both reflexivity and openness to communication exist to some degree in some organisations. Depending on their specific situation, the lever for introducing ethical branding can be a different one. Companies that already explicitly value their societal role may need external actor involvement to start sharing information and improving their self-representation.

Technology producers who have failed to sell privacy enhanced technologies to clients may work on building communication relationships with citizens and clients' customers. This is again especially feasible for Systems Integrators who already dispose of a distribution network and of extensive marketing departments. A promising field for medium-range ethical branding could be “business security”. Corporate security clients need to communicate their security and privacy policy to their employees and work councils. The setting is clear-cut for negotiation purposes, e.g. in the case of the introduction of biometric systems. A number of meta-organisations and associations exist in the sector that can help set standards.

Specialised producers are more likely to communicate only with their direct clients, a constellation that could be changed by providing information in cost-efficient ways, e.g. with an accessible website. Information could include the clients that use the specialist's parts so that market relationships become more transparent.

Likewise, clients such as transport providers could easily provide the names of their suppliers. Clients usually focus on a core service that is not security, so while shopping mall owners have relatively well established communication channels, the issue of privacy and data protection yet needs to be set on their agenda.

While the mere provision of information about business partners may seem a small step, it enables citizens' advocates and experts to evaluate particular constellations and compile this data in a comprehensible fashion. Web-based portals such as brandkarma that observe brands make use of crowd sourced information gathering in order to assess brands on various dimensions.

Our findings suggest that while privacy and data protection are perceived as very important by individuals, the motivation to demand one's right actively is low in the current situation. Privacy remains an abstract topic as long as it is framed in the legal and technical way that is still paradigmatic. Ethical branding needs experts, advocates and consultants who can translate between companies, legal provisions, and citizens. In some countries, we have found a number of actors that fit this role of translator: privacy and data protection consultancies (often coupled with information security consulting), innovative marketing and communication experts, and privacy advocates and civil rights groups. It is important that official data protection institutions and representatives are joined in the field by more innovative and flexible actors who participate in strategy development or even product development.

Companies can start out building new communication relationships by involving experts first, and citizens later on. This helps mitigating fears of vulnerability that come with openness and transparency. Closed contexts may be favourable at first, especially when this helps building reflexivity.

5 Materialisation of privacy branding

The term "materialisation" carries a number of meanings. As a final dimension in our concept of ethical branding processes, it denominates the "coming into effect" of a co-construction of ethical branding over time and space: the real, tangible process of change along the dimensions of the analytic concept. This can be connected to "material" things and results, such as tangible products or events.

5.1 Quality of ethical branding

As explained above, the ethical branding dimensions build on each other:

1. Reflexivity
2. Information Availability
3. Communicability
4. Action-ability
5. Testability

While the dimensions point to analytically distinct concepts, they can also be read as an ordinal scale. We actually hold that each dimension requires some progress along the preceding dimension in order to be successfully developed. Communicability without reflexivity is unlikely to result in organisational changes; testability cannot exist without information availability.

In our ideal ethical brand, all dimensions need to be actualised all the time. Of course, in practice, there will be scarce resources and other restraints to how intensely a dimension can be performed by a company at a given time. Ideally, an iterative schedule is implemented that sets privacy branding – or one of its dimensions – on the agenda on a regular basis.

In addition to qualitative scope, an ideal ethical branding process should cover as much of an organisational activities as possible. All business processes and organisational procedures should be subject to transparency and accountability efforts. This necessarily implies that many more employees will take part in this process, and that cooperation and communication will have to be intensified within the organisation itself. The development of a new privacy enhanced product would have to involve not only clients, developers and product managers, but also marketing departments, privacy officers, external experts and possibly end-users or citizens respectively advocates.

It is clear that ethical branding performed in the envisioned style is a resource intensive process. While it can be viewed as an investment that return can be expected on, there are ways that companies can make use of external resources to kick-start their engagement.

5.2 Seeding ethical branding – a preliminary guide for security companies

In place of a conclusion, we would like to offer a few questions that can lead the way into an ethical branding process for a security company.

5.2.1 Reflexivity

→ Hire a privacy officer in a responsible position with good time resources. Ask your privacy officer to network with externals and associations, conduct trainings, and report regularly.

What is our notion of security? What is our role in the current securitization development - which security threats are we really tackling?

→ Invite researchers to conduct interviews in the company and research company history. Have the results presented to a wide range of managers.

How do our products and services impact their direct context?

→ Take part in research projects. Contact security and privacy researchers and experts. Contact clients, found work groups that observe the impact of particular products or services.

How does privacy figure in our services and products?

→ Review products and services with the help of external privacy and data protection consultants.

How do our clients use our products, and how are our products perceived by our clients' customers?

→ Contact clients. Conduct market research with a focus on privacy and end-users' civil liberties.

5.2.2 Information Availability

What information are we currently offering clients/ experts/ citizens/ the media?

→ Publish a dedicated website about the privacy officer's work.

How accessible and how current is our information?

→ Create comprehensible articles dedicated to end-users and citizens.

Is there other information that we could offer, e.g. about our clients or suppliers, or about product development?

→ Provide stories about your clients and suppliers along past or current projects, especially security projects in public settings.

What information should we collect about our company for internal purposes and for publication?

→ Find out which employees are motivated to get involved in ethical branding and privacy issues. List competences for communication purposes.

5.2.3 Communicability

Who communicates with us? Who else could want to communicate with us?

→ Have an external expert map your company's communication relationships. Find the blind spots.

What channels of communication are we currently offering clients/ experts/ citizens/ the media?

→ Try some role play: try to contact your company about a privacy question as a client, expert, citizen or journalist. How does that work out? Create visible, easily accessible channels such as telephone hotlines, email forms, or forums.

How do we react to acts of communication from clients/ experts/ citizens/ the media?

→ Invite inquirers to dialogue. Set up events around specific topics.

5.2.4 Action-ability

How do clients, experts/ citizens/ the media currently impact our organisation with regard to privacy and data protection? Which actors are missing in the picture?

→ Think about possibilities to involve missing actors in order to balance your stakeholders more.

Which business processes can be opened up to decision making that includes external experts and citizens?

→ Organise product development workshops. Organise votes or competitions about alternative services or products. For security services, organise roundtables with stakeholders in order to plan services.

Can action and impact by externals be institutionalised for our company?

→ Conduct regular public events. Let the participants pick the topic. Document impact.

5.2.5 Testability

How can we prove our claims of privacy protection to date?

→ Contract an external privacy and data protection consultant for an overall check.

What documentation system do we need in order to track our progress?

→ Start the process of earning a privacy seal or certificate.

5.2.6 Materialisation

Who can take on the job of realising ethical branding in our company?

→ Connect privacy officers and marketing departments. Find enthusiastic colleagues and let them start networking. Become a case study in a research project and have your ethical branding kick-started.

–