Project acronym:	SAPIENT
Project title:	Supporting fundamentAl rights, PrIvacy and Ethics in surveillaNce Technologies
Project number:	261698
Programme:	Seventh Framework Programme for research and technological development
Objective:	SEC-2010.6.5-2: Use of smart surveillance systems, data protection, integrity and sharing information within privacy rules
Contract type:	Collaborative project
Start date of project:	1 February 2011
Duration:	36 months

Deliverable 2:

Engaging stakeholders and civil society in the assessment of surveillance practices

Editor(s):	Michael Friedewald (Fraunhofer ISI)
Dissemination level:	Public
Deliverable type:	Report
Version:	1.0
Due dates:	29 February 2012; 31 May 2012; 31 July 2012
Submission date:	26 September 2012

About the SAPIENT project

The SAPIENT project that is expected to provide strategic knowledge on the state of the art of surveillance studies, emerging smart surveillance technologies, and the adequacy of the existing legal framework. In addition to addressing these core research goals, the project will entail the development and validation of scenarios around future smart surveillance systems, and will apply the best elements of existing PIA (privacy impact assessment) methodologies to construct a surveillance related PIA framework.

The work of the project will lead to a practical handbook which will help policy makers, technology developers and other stakeholders to better understand how and when smart surveillance should be used, and apply criteria to assure that such systems respect the privacy of citizens.

Terms of use

Suggested citation: Friedewald, Michael (ed.), "Engaging stakeholders and civil society in the assessment of surveillance practices", Deliverable 2, SAPIENT Project, 2012. `http://www.sapient-project.eu`

Document history

Version	Date	Changes
0.5	22 June 2012	First Version of D2.1 (containing only 2 scenarios)
0.7	03 September 2012	First part (D2.1) completed
0.8	23 September 2012	Cross analysis (D 2.3) added
1.0	26 September 2012	Workshop reports (D2.2) added

Contents

1. Introduction

Michael Friedewald (Fraunhofer ISI)

In its first year (2011), the SAPIENT project has defined and characterized smart surveillance within technological, social, political, legal, and ethical contexts, ranging from current studies of state-of-the-art of surveillance to emerging technologies and related applications expected over the next decade. This analysis gave a picture of today's surveillance society and the trend towards a "generalisation" (pervasiveness and banalisation) of surveillance (Gutwirth et al., 2012). In order to develop a methodology for an early assessment of privacy impacts of emerging smart surveillance technologies it is necessary to engage stakeholders as early as possible in the development and/or deployment process (De Hert, 2012, p. 70).

The first cycle of engagement of stakeholders and civil society in the assessment of (smart) surveillance practices was implemented in two steps: In the first step scenarios are deemed a useful tool to approach and consider key concerns and issues, including privacy, data protection and integrity. In the second step the scenarios were used as the starting point collecting interests and concerns of different stakeholder in a number of focused workshops.

1.1. The SAPIENT Scenarios

1.1.1. Why Scenarios?

Scenarios are considered as one of the main tools for looking at the future, although there are many other prospective methods such as Delphi expert panels (Georghiou et al., 2008). It is important to underline that scenarios are not predictions. Rather they describe plausible and/or desirable futures and possible ways on how to realise these futures. In particular, they can provide provocative glimpses of potential futures and are developed to stimulate the debate on these possible futures. The use of scenarios is a tool to stimulate debate, to structure thinking, to facilitate 'What if' games to aid in the synthesis of realistic future plans as well as to help in raising awareness intuitively (Ringland, 1998; Godet, 2000). The scenarios developed by SAPIENT share these generic goals with other scenario exercises.

The following three scenarios have been developed in ways similar to other mainstream scenario exercises. The major difference is, as mentioned in the section above, that they focus on dark situations, i.e., situations that enable us to highlight vulnerabilities

and threats. As there is no unique method for developing scenarios and as there are different approaches to scenario writing, it is important to clarify and explain the approach and methodology used. The SAPIENT scenarios are so-called trend or reference scenarios (Masini and Vasquez, 2000). This type of scenarios extrapolates certain trends in society, technology, industry, international relations, etc. (as analysed in SAPIENT Deliverable 1) and projects these trends into the near future (time horizon chosen: 10 years from now). In particular, the SAPIENT scenarios exemplify the current trend of contemporary surveillance to become "quotidian activities that we undertake on a day to day basis" and draw on current research in this area which sees humans being increasingly relegated to the role of "second-level decision makers".

The objective of many scenario exercises and foresight studies is to present images of desirable futures and sometimes to determine the necessary steps to realise such futures. Consequently, they have an inherent bias towards presenting only optimistic visions of the future. The SAPIENT scenarios are different because they present certain visions of the future that we, in principle, do *not* want to become realities. They depict a future that could emerge from the applications discussed by typical end-users, policy-makers and from the technologies that are currently being developed in the FP7 Security Research Program. Still, they are not the mere transcription of some actors' discourse on future technological developments. To different degrees and in different manners, the three scenarios attempt to also highlight the tensions, the mismatches and the paradoxes foreseeable in the next future, or even already announced in present days.

To facilitate identification of risks, but also to provide a comprehensive picture of future Smart Surveillance applications, the scenarios assume a wide deployment and availability of those technologies, which are announced to solve current and future threats to security. It assumes that technology operates in the background while computing capabilities are everywhere, connected and always available. It takes care of needs and is capable of responding intelligently to spoken or gestured indications of desire. It can even engage in intelligent dialogue as it is about human-centred computing, user-friendliness, user empowerment and the support of human interaction. But, again, technical failures, inconsistent and incomplete implementations, and errors are mentioned, not for a bias against technology, but to avoid a too deterministic approach.

1.1.2. Methodology

The following three scenarios have been developed in ways similar to other mainstream scenario exercises. The major difference is, as mentioned in the section above, that they focuses on dark situations, i.e., situations that enable us to highlight vulnerabilities and threats. As there is no unique method for developing scenarios and as there are different approaches to scenario writing, it is important to clarify and explain the approach and methodology used. The SAPIENT scenarios are so-called trend or reference scenarios (Masini and Vasquez, 2000). This type of scenarios recognises certain trends in society, technology, industry, international relations, etc. (as analysed in SAPIENT Deliverable 1) and projects these trends into the near future (time horizon chosen: 10 years from now).

In particular, the SAPIENT scenarios exemplify the current trend of contemporary surveillance to become “quotidian activities that we undertake on a day to day basis” and draw on current research in this area which sees humans being increasingly relegated to the role of “second-level decision makers”.

In order to trigger a lively discussion among the different experts and stakeholders, and thus to achieve high public attention towards technologies and policies with a severe impact on individuals’ privacy the team decided to write "polarized" scenarios. The scenarios concerning ‘security in public places’, and ‘smart surveillance in business activities’ were drafter as proper *dark* scenarios, while the scenario on ‘border security and immigration control’ was conceived as a sort of *mixed* scenario. The main difference between these two categories is the emphasis devoted to alternative options and the role played by different actors. While in the dark approach the possibility to modify a scenario once technologies are deployed is pretty reduced, in the mixed approach the option to revise, even in ten years, the course of events is more evident. Still, to keep such reversibility option open, the role played by different actors is described in a different way, with more attention dedicated to dissensus and technical malfunctioning.

From this outset, the SAPIENT consortium decided to develop a limited number of scenarios. In principle, a virtually infinite number of possible futures could be developed, but a selection has to be done to allow the management of the exercise for both the developers and the readers of the scenarios (Godet, 2000). The topics of the scenarios include applications in the centre of the EC’s security research programme as well as in the developing Internet economy (e.g., surveillance of customers for marketing purposes). Three domains have been selected as particularly sensitive, and thus selected as focus of the scenarios.

- The first scenario deals with the role that smart surveillance could play in law enforcement, especially for security in an urban environment (using the example of a mega event such as the FIFA football World Cup).
- The second scenario describes how smart surveillance could impact business activity (i.e., the role smart surveillance plays in consumer marketing activities).
- The third scenario depicts how the various trends in smart surveillance technologies and practices for border management and immigration control could constitute a new EU Border Management System in the future.

In more practical methodological terms, the conception and drafting of the scenarios was tailored on their main stated goal, e.g. a first engagement with stakeholder to critically think about key concerns and issues of smart surveillance technologies deployment. Hence, the scenarios were developed in a lean and fast process (sometimes called "scenario thinking", Wright and Cairns, 2011) through a combination of desk research and interactive workshops within the consortium and with a few external experts.

The scenarios have been developed on the basis of the results from the project’s first year (Gutwirth et al., 2012). For the scenario development, the SAPIENT consortium has held an internal workshop to identify the application areas to be covered (i.e. the three scenario topics), the dimensions along which the scenarios had to be developed and to collected a first list of relevant technologies and devices as well as possible drivers and barriers.

In a next step, the team collected and collated information on recent developments within each of the three scenarios identified in cross-consortium discussions. The collection included news stories, documents of public authorities and private actors, as well as reports from non-governmental organisations and academic contributions.[1] The three scenarios were fleshed out by small teams who did internal brainstorming and scenario development workshops to develop the final story lines. Finally, the ultimate draft of each scenario was circulated to the other members of the consortium to receive feedback. The consolidated version of each scenario (Part I of this deliverable) was the distributed to workshops' participants few days in advance.

1.2. Stakeholder Workshops

1.2.1. Concept

The scenarios formed the starting point for the engagement of stakeholders, including civil society, with the objective to develop a view on how and when smart surveillance should be used, to target critical parts of security and its characteristics, to be effective and scalable, and to rapidly adapt to changing situations. To collect key concerns and issues, including privacy, data protection and integrity of future smart surveillance systems the SAPEINT partners organized three workshops that took place between June and September 2012.

These stakeholder workshops included planned but open discussions among a small group (6 -12 persons) of stakeholders facilitated by a skilled moderator and designed to obtain information about the preferences and values pertaining to a defined topic and why these are held by observing the structured discussion of an interactive group (similar to "classical" focus groups involving laymen/ordinary citizens). The approach is particularly useful when one is interested in complex motivations and actions, when one will benefit from a multiplicity of attitudes, when there is a desire to learn more about consensus on a topic and when there is a knowledge gap regarding a target audience (Slocum, Steyaert, and Berloznik, 2006; Dürrenberger et al., 1997). With this workshop concept the SAPIENT consortium aimed to:

- gauge the nature and intensity of the stakeholders' concerns and values about the issues,
- obtain detailed reaction and input from stakeholders to preliminary options
- determine what additional information or modification may be needed to improve the scenarios and to develop issues for a PIA scheme customized to the specifics of surveillance technology.

[1] A particular attention was given to scenarios developed by FP7 Security Research Projects – either as part of defining technical requirements or as a means to communicate the (expected) project results to the public. In particular the promotional video of the INDECT project (`http://www.indect-project.eu`) raised a lot of public attention and criticism for developing 'Orwellian' surveillance technology (Johnston, 2011).

1.2.2. Procedure

To prepare for the focus group events the SAPIENT teams determined core questions to be addressed by the group. While the three events focused on different scenarios the core questions were basically be the same (see Appendix B).

The group invited to the workshops aimed to have a good mixture of all relevant stakeholder groups (industry, law-enforcement, policy makers, civil society organizations, academic researchers).

The stakeholder workshops were half-day events, that took place in Hoofddorp (near Amsterdam) on 27 June 2012 and in Brussels on 07 September 2012. The group-discussion was initiated by a short pointed presentation of the respective scenario. The group was then lead by the moderator through a semi-structured discussion to draw out the views of all of the participants and then summarised all of the main issues and perspectives that were expressed.

All three workshops had been recorded (with the agreement of the participants). The SAPIENT partners produced extensive proceedings of each workshop. These were first analysed separately to work out scenario specific issues (see part II of the deliverable). Drawing on these reports from the stakeholder workshop a cross-cutting analysis was conducted to provide views of stakeholders from industry, government, law enforcement agencies, policy-makers and civil society organisations on how and when smart surveillance should be used (see Part III of the deliverable).

Part I.

Deliverable 2.1: Scenario Report

2. Smart Surveillance and Securing Public Spaces

Philip Schütz, Michael Friedewald, Dara Hallinan, Kerstin Goos and Jana Schuhmacher
(Fraunhofer ISI)

Highly complex and at the same time powerful crowd dynamics have always been a phenomenon of herd animals such as the human species, which both fascinated and frightened people in power or pursuing the same. Although these dynamics are difficult to steer and even harder to control, political actors throughout history, also those being elected, were regularly trying to win over the masses and gain popular support by taking advantage of mass movements and profit from mass gatherings.[1]

Today, and probably even more relevant in the future, so-called mega-events such as the Olympic Games, the Football World Cup or the Expo have become an outstanding opportunity and an unrivalled platform for politicians and industry of the host nation and/or city to create an image of stability, openness, and prosperity. Being highly prestigious and having important long-term economic impacts, mega-events have not only grown bigger in recent decades with regards to numbers of visitors and television viewers, but also the expectations to present the host nation in the best light have become very high.

That is why security issues, from sophisticated safety plans to smart surveillance technologies, are playing a more and more salient role in the preparation and realization process of these events. Since not only the demand but also the societal acceptance of otherwise as privacy-invasive perceived security measures is usually very high in the context of mega-events, the Olympic Games or the Football World Cup serve as a window of opportunity for security service providers to experiment with and showcase the latest cutting-edge security technologies.

2.1. Football mega-events and their security challenges

Football is the most popular sport in the world. Attracting zealous tourists and football fans around the globe, the Football World Cup 2010 was one of the most-watched television events in history, including world records of spectators in the stadiums, in areas of public viewing and on the Internet.

[1] The Nobel Prize-winning novelist Elias Canetti has dedicated a whole book to the relationship between crowd control and power, hypothesizing that there is a thin line between ruling and paranoia (Canetti, 1960).

Since the tournament presents an unprecedented platform for international publicity, politically motivated activities aiming to attract public attention should be considered in a sound security concept. However, there is a broad scope of these activities from legally correct announced demonstrations to terrorist attacks. Due to its monopoly on the legitimate use of physical force, the modern constitutional democratic state needs to reconcile the risk of violence, being used in such political activities, with the degree of surveillance and other preventive law enforcement procedures.

Particularly in the context of football games, a very special form of violent but usually times not politically motivated behaviour is hooliganism. This phenomenon of violence in and around the football stadiums is increasingly shifting to other places in order to make the intervention of police forces more difficult.

Taking these forms of violent behaviour into account, security concepts need increasingly to consider security issues beyond locations in and around the actual football venue. They also have to offer special safeguards in public viewing places, around lodging areas of participants of the championship as well as in central transportation hubs such as airports and train stations.

2.2. The FIFA Football World Cup 2022

The security concept of the Football World Cup 2022 entails three pillars:

- The preventive and precautionary collection, storage and processing of vast amounts of data of football fans, tourists and local citizens being actively or passively involved in the World Cup,
- Surveillance in and around the stadiums of people and objects, and
- Monitoring of places with relevance to the World Cup such as lodging areas for the national teams, public viewing areas of fans and transportation hubs.

2.2.1. Preventive data collection and processing

During the past decades the security discourse especially with regards to mega events has more and more shifted from reactive measures to preventive strategies. The goal of the security concept of the Football World Cup 2022 is, thus, to completely control and reduce as far as possible potential security risks way in advance of the actual happening.

Predictive analyses are not new, but the comprehensiveness of the data sets providing the basis for a sound analysis has changed dramatically. Important aspects of our day-to-day life are increasingly transcending into cyberspace, leaving traces when-, where- and whatever the user intends to do. That way a finely nuanced *profiling* of (potential) perpetrators of violence at the Football World Cup can take place.

Security service providers do not only have access to police databases with a variety of information on criminal offenders, they also cooperate with large private IT companies in

order to create profiles of people who could attract attention through violent behaviour during the World Cup. In order to discover, for example, hooligans who do not already have a criminal record, Internet forums of fan communities and social networks are systematically scanned and automatically analysed. Raising an alarm and creating a preliminary blacklist, the fully automated analysis does not only consist of a search of keywords but draws on new *semantic web technologies* that are able to put words into the correct context and gain the relevant information out of billions of entries.

Additionally, fan communities such as fan clubs are tasked with monitoring relevant forums for suspicious comments, receiving rewards in the case of giving valuable hints about plans and activities of (potential) hooligans. On the one hand, this form of outsourcing monitoring activities reduces the costs of commercial and state security providers significantly; on the other hand, civil society gets engaged and committed through such collaborations.

Beyond hooliganism, politically motivated violence plays an important role in the security concept of the World Cup. That is why online activities of political activists from left and right wing extremists to religious fanatics are being carefully watched and analysed, *categorising profiles* into different *levels of risk*. On the basis of these analyses, attempts to proactively engage with potential aggressors are being made. Differentiation tools that take the motivation of each potential aggressor into account and create an even more detailed profile allow for personalised and group specific approaches. That way, on the one hand, products and services are being offered that are supposed to help working against radicalisation and marginalisation. In the case of (potential) hooligans, they are confronted with offers on their smartphones to do an internship with the police or to join an anti-violence training, both with positive and negative financial incentives such as offering modest rewards or threaten to cut social security benefits. On the other hand, everybody once listed as a potential aggressor is unable to buy or consume products or services encouraging violent behaviour such as ego shooter video games or paintball.

The *smartphone revolution* has brought ubiquitous computing, including continuous sharing of *location* and *communication data*, its break through. Smartphone location data is most prominently used by law enforcement agencies to watch compliance of criminal offenders after their penalty. This enables the police in the context of the World Cup to monitor the whereabouts of hooligans and other violent criminals.

But not only ex-convicts are being routinely tracked. In 2022, dynamic Internet protocol addresses are abolished and the new Internet Protocol Standard of IPv6 plus with *fixed IP addresses* allows for the exact identification of every computing device such as the old fashioned personal computer at home, every laptop and smartphone, as well as other digital devices being able to enter the online world. Linking the unique identifying number to the person who bought the digital device has had the consequence that anonymity in cyberspace only remains a relict of the past.

Furthermore, smartphones are equipped, by default, with an *NFC* (near field communication) chip that is able to communicate and match personal data with a system close by. Hence, smartphones are increasingly used to identify oneself in situations such as buying alcohol or entering a music club. An *eID application* has specifically been developed for these purposes and although citizens are not obliged to draw on their smartphone as an ID, they are getting more and more used to do so.

Surveillance on the Internet has largely been expanding. The security team of the World Cup has access to a vast amount of data collected from everyone searching for certain keywords online such as ”World Cup“, the names of the stadiums or host cities, as well as names of specific football players. Everyone who is booking a train, bus or flight ticket to a host city for the time in which the World Cup takes place is automatically captured and profiled. Although there are certain limits to data retention periods in general, specific exemptions apply for databases relevant for the security concept of mega-events.

All (service) products that are sold in relation to the World Cup including tickets or Computer Games are only available online so that personal data gained from a transaction can be fed into the existing database. There is no choice; customers have to carry out their desired action online when they want to receive a FIFA product. Here, the convenience aspect for customers to buy online becomes less relevant, and the fact that personal data is transferred in order to reveal what kind of person is interested in the product becomes a necessary security requirement for the vendor.

2.2.2. Surveillance in and around the stadiums

The areas in and around the stadiums are maximum-security sectors. Nobody can enter them without having gone through heavy security checks. Access rights are only given out to stadium personnel, nation team players and their staff as well as visitors of the game with a valid ticket. The personnel working in and around the stadiums need to identify themselves through a retina scan (high resolution retina images are also used by the employers to reveal drug abuses or illnesses such as diabetes of the employees); participants of the World Cup and their staff have special biometric photo IDs, and the visitors have to be in possession of a personalised ticket on their smartphones on which the eID application is running that has in a lot of cases substituted the traditional ID card.

Preventing weapons from being brought in, *full body scanners* represent the main security gate control technologies. They are complemented by *smart scent sensors* that are able to detect even single segregated molecules of explosives such as TNT or pyrotechnic materials. Additionally, these sensors have also the ability to give warnings about somebody who is carrying drugs or who is drunk.

Within the stadiums and during the game smart infrared cameras, which have been previously installed to record the football players’ performances in order to analyse it later on, are now also used to watch in real-time for an increased level of stress and aggression in the audience. After applying face recognition and identifying single fans, who are about to reach a certain limit of body heat or show (facial) movements which are overly aggressive, warnings and a threat of penalties are sent out to the smartphones of potential aggressors.

People with ADHD (Attention Deficit Hyperactivity Disorder) and other behavioural and psychological disorders that are perceived as having tendencies toward a violent and aggressive conduct have to expect to be put under special individual surveillance. Potential aggressors who are nevertheless admitted to access the stadium because they are ranked as a rather low-level risk are not only monitored more thoroughly, security service provider in collaboration with governmental agencies are also trying to subtly influence and educated

them by presenting deterrent effects, as well as by proactively offering certain anti-violence products and services.

Furthermore, the information initially collected for security purposes is also used to tailor public announcements and governmental success stories to the visitors of the football game. Highlighting the latest reduction in crime rates, for example, governments and security providers can present themselves in a better light, also legitimising the heavy security measures.

2.2.3. Urban surveillance

Since violent behaviour is not restricted to the high security sectors in and around the stadiums (maybe even pushed outside these areas), crowd control and reactive security measures in neuralgic locations of the host cities are crucial, as well.

In public viewing places and so-called *fan zones* access control of football fans, tourists and locals is much more difficult because there are no tickets to be bought, and hence, no identification is necessary. However, minimum safety and security standards such as checking for (potential) weapons, for example knives, pyrotechnic articles, or glass bottles, are maintained at the barriers by smart gates that do not look like scanning devices but have built-in sensors of various kinds.

Public viewing areas and fan zones are characterised by a smart environment and ambient intelligence: automated systems such as hidden face recognition cameras, biometric and thermographic CCTVs and scent sensors are collecting vast amounts of data in real-time being transferred to a central headquarter, analysed or matched with criminal records and lists of potential aggressors. Since the organisers of the World Cup want to maintain a pretence of openness and of a liberal society, most of the urban surveillance technologies in public spaces are increasingly concealed in clever ways embedding them into the environment or drawing on miniaturisation.

The fan zones are a perfect example of the merging of private and public interests. On the one hand, these clearly demarcated areas present a wonderful opportunity to control the marketing of specific brands and products being sponsored by partners of the FIFA. On the other hand, they facilitate reducing the risk of violent incidents.

Police officers and security personnel wear glasses with built-in micro cameras and a virtual retina displays (VRDs) transmitting information about people surrounding them directly onto their retina. Based on the profiles about political and religious activities, radicalisation and social status, as well as criminal records, policemen are able to identify individuals presenting a potential source or catalyst of the outburst of violence.

Security staff is additionally supported by a variety of different unmanned aerial vehicles (UAVs) flying soundlessly in and above the cities hosting the World Cup. Unmanned drones equipped with high-resolution cameras are able to provide the security headquarter with real-time videos of the city's inhabitants and visitors. As a result, critical masses of unwanted gatherings of people such as groups of hooligans or rioters can be swiftly identified and taken actions against.

Within urban areas and infrastructures so-called *quadrocopter*, i.e. dinner plate-sized unmanned helicopters with four instead of one propeller, are often deployed. These small extremely handy and precisely manoeuvrable drones are able to enter buildings through open windows or doors. They are equipped with highly sensitive microphones and cameras streaming audio-visual data to the headquarters. However, the latest form of UAVs has been insect-like drones, not recognisable and distinguishable from their natural equivalents.

What all of these drones have in common is that they can stay up in the air much longer than conventional aircrafts. The smaller drones can be wirelessly recharged at special docking stations, and although all of them have remote control systems integrated in their design, the drones often move and work autonomously, executing tasks automatically. That way they patrol clearly defined routes being however able to report on and react flexibly to unexpected situations.

Since the World Cup takes place in a democratic European country, citizens of the host nation have, of course, the right to protest and organise demonstrations. Nonetheless, the organisers of the World Cup and the police forces of the host nation are interested in preventing violent behaviour against property and/or other individuals from happening under any circumstances. Furthermore, security service providers aim to maintain a smooth and frictionless flow of processes at the mega-event, which blockades caused by political activities would threaten.

That is why any kind of mass gatherings of political activists, rioters or hooligans in forms of legally correct announced demonstrations to spontaneous flash mobs are carefully watched. Drones as well as security staff are not only provided with smart video cameras that are able to record facial features of the surveilled, but also with a so-called DNA spray that is used to mark individuals suspicious of committing a felony during a mass gathering. Later on, the spray can be unambiguously detected on clothes, hairs or the body of the marked suspect.

2.3. Societal consequences and surveillance legacies of mega-events

All in all, the security concept of the World Cup in 2022 relies increasingly on preventive measures, drawing on the collection and processing of vast amounts of personal data in order to better predict and react to potential threats from violent individuals or groups of people. The semi-clandestine nature of collecting this data is of the utmost importance, since otherwise potential perpetrators of violence would shield information about themselves from being collected and analysed.

Most of the public has long ago begun to accept being put under general suspicion, especially when securing public spaces in the context of hosting a mega-event. But even more important, people perceive the algorithms, software and technologies behind the complex data processing operations as neutral, most precise and inerrant procedures, providing for the greater good for society. Thus, technological determinism is widely spread, and results of, for example, profiling practices are rarely contested. As previous mega-events have already shown, most of the preventive and reactive security measures installed in the host

country and cities remain in place long after the end of the actual event. These surveillance legacies comprise a technological, informational, legal, geographic and cultural dimension. For example, once, police forces are equipped with the latest surveillance technologies such as drones or VRDs, they retain and also take advantage of such an equipment later on. The data collection and processing operations are also kept up by law enforcement agencies, which argue that they are needed to continue to effectively combat terrorism and reduce crime rates all over the country.

Laws and regulations influenced by the security discourse before and during the World Cup present another crucial long-term consequence for the surveillance culture of the host nation. Furthermore, surveillance infrastructures from audio-visual face recognition cameras to scent sensors or body scanners continue to operate.

All of these factors have eventually an impact on the societal perception of surveillance as an unavoidable instrument for ensuring security, stability, and peace, resulting in a spiral of social pressure towards total transparency of the country's citizens, and the spreading of the paradigm "If you have nothing to hide. . . ".

3. Smart Surveillance and Personalised Advertising – 23 March 2022

Rachel Finn, David Wright and Kush Wadhwa (Trilateral Research & Consulting)

The last 10 years has seen the explosion of ”smart“ personalised services based on the collection of consumer and citizen data and the creation of specific profiles. These services were supposed to increase customer satisfaction, help governments to understand citizens and benefit the economy by boosting consumer demand and thus productivity. However, as they proliferated, the effects of these technologies have become increasingly grim, including the identification and manipulation of individuals, a chilling effect and rising inequality and economic stagnation. Although small pockets of resistance have developed, these practices and the negative social effects that have followed have become part of the social fabric.

3.1. Intended Benefits

The introduction of smart personalised services was intended to benefit consumers, companies, government and society. Spam, as a concept, quickly became abolished, and goods and services were tailored to individuals. As computing media proliferated and became more individualised, people very seldom experienced general advertisements. In fact, mass media advertising through broadcast television and radio has largely disappeared, and has been replaced by public service announcements, political announcements, etc. Advertising for products or services only appears on downloaded, on demand or web-streaming media content and is tailored to individual user profiles. For most people, the distinction between public service announcements, political lobbying messages and advertising disappeared as all of these messages became so personalised they appeared to be notices about information or products the individual needed to solve a particular problem, rather than something that is being ”sold“ to the person.

Companies were set to benefit from these practices since much less money would be spent on advertising, because consumers are better understood by commercial organisations. Commercial organisations sought to match products, services and retail outlets to micro-segments of consumers, and because they generated significant interest through this targeting, click through rates initially increased substantially. This cost savings also allowed commercial organisations to differentiate their products further in order to more completely match their products with consumers’ desires and interests.

Society was also set to benefit through an increase in demand for data professionals such as data analysts and statisticians that would lead to more investment in science and technical education, and a better trained, more educated workforce. Pundits also thought that smart advertising would boost demand for consumer items, increase production and produce a ”trickle-down effect“ that would benefit the economy and society.

All of these benefits were supposed to be realised through greater powers for companies and the government to collect data on consumers and citizens in virtual space, in-store or shopping centres, in public space and in the home.

3.2. Data Collection

3.2.1. Virtual Space

The collection of personal data in virtual space began with the advent of popular use of the Internet in the 1990s. By 2022, Internet purchases, browsing and media consumption (which is almost entirely consumed on individual computing devices or smart televisions) are all routinely monitored. For some time, advertisements have been tailored to the types of purchases made, websites visited and media consumed. Companies compensate consumers for the harvesting of their personal information via reduced rates for web browsing, landline or mobile communication and media content (movies, television, music) hardware and services in exchange for targeted advertising based on usage and communication monitoring. However, a small portion of the elite pay for supposedly non-monitored communication. All websites or content databases are instantly pre-configured to highlight items, which are most relevant to the person. Other content is searchable.

The government ramped up its data collection with the introduction of a ”voluntary“ ID service to enable individuals to access benefits and discounts proffered by the government. For example, individuals are encouraged to provide their government ID number to get personalised discounts on healthy foods, exercise equipment, participatory activities, plus benefits associated with particular sectors that the government is promoting. Many of these benefits are linked to DNA information either provided voluntarily by the individual through their healthcare provider in order to access personalised discounts on health-related items or activities, or as a result of DNA profiling techniques that include family names. Some individuals have also accepted an invitation to tie these government ID numbers to their primary mode of payment as a convenience, and because of how often such initiatives change as a result of political wrangling. However, any data associated with the government ID number is also the property of the government, who mines this data to make predictions about spending, financial health, physical health, etc., both for society and for individuals. The government collects this data both in terms of online spending, which must be paid by debit or credit card and in-store transactions paid by card or where the person’s government ID number is referenced.

The presentation of adverts on computers and mobile devices is based on the monitoring of key words contained in e-mail and text message communications. Government agencies routinely monitor web and communications traffic to detect deviant behaviour,

including communications, media content or purchases that may signal intent to participate in criminal or terrorist activity. Governments monitor purchases and social media consumption to detect benefit fraud and to glean data on individuals' behaviour and health. Political parties have outsourced data mining to Google to better understand political party affiliations and issue-based chatter on social networks and in personal communications.

3.2.2. In-Store

The line between in-store shopping and online shopping has become increasingly blurred. Some individuals use a personal shopping application which reserves items based on previously supplied information or preferences. Individuals then agree to a purchase, or elect to stop into town to view or try on an item before purchasing. Data aggregators have merged and consolidated into a handful of large corporate entities that have entered into deals whereby they collect information from retail outlets as well as online and provide discounts or bonus points as a result of shopping within the conglomerate. The aggregators collect data associated with government ID numbers loyalty programmes, DNA information from healthcare providers, location determination technologies, RFID and sensors in stores and shopping centres.

When someone enters a shop or mall, identity and positioning information in their mobile phones is ”read“ and many stores display items presumed to be of interest to the passing individual on screens at the front of or inside the store. Shops track individuals around the store to gather more information on what people are interested in. Customers are tracked via RFID chip readers and encouraged to visit specific sections of the store based on items they are known to have purchased previously. New items are also suggested, particularly those, which match well with items they have in their cart since these, were instantly read by ”smart“, RFID-enabled shopping carts. ”Smart“ refrigerators and other home appliances store data on the cloud, which is accessible to individuals' mobile devices when they visit the store, so that they can be prompted to buy specific items that they are running low on, or which will expire soon. For some frequent shoppers who are signed up to conglomerate based loyalty systems, individual preferences are also recorded on RFID-enabled loyalty cards. Retail staff members address shoppers by name since their data is read by customer intelligence software as they enter. Some cost-savvy shoppers have noticed that if they come in and view an item on three separate occasions, they are often offered a discount on the item by a sales person who was pinged by the in-store customer intelligence software.

Clothing stores often install sentiment analysis devices and body scanners near racks of new items or in public areas of changing rooms to better understand customers' feelings about an item. For example, if customers seem positive about an item at the rack, or on the shelf but look negative when trying the item on, the store knows that customers are interested in the item but that there is a problem with the cut or the fit. This can be segmented and linked with body scanning devices, for example, if individuals with long legs do not fit into an item as well, the store can introduce a ”long and lean“ line. Body scanners are also used to assist customers in finding the right sizes for particular products, to categorise them and alert them to special offers or discounts on particular sizes (e.g.,

10 per cent off because only size medium is available) or to encourage consumers to act quickly in order to get the items they want (e.g., ”Hurry, only two size small left!‘).

Sensors are deployed in shops to detect health or medical conditions and offer products associated with health profiles. While body scanners are used to identify persons with weight problems, the integration of specific sensors in pharmacies gleans health information including temperature, cardiovascular and respiratory health, as well as specific odours. This is often linked with DNA information to identify whether an individual might be showing early symptoms of an illness to which they are predisposed or which matches their profile characteristics. These data may be further combined with RFID-enabled smart cards or location determination technologies to identify what prescription drugs an individual often purchases (to glean health data), to change the products offered to individuals when they enter the store (e.g., bananas for a detected or heritable potassium deficiency) or to change the prices associated with particular items based on health profiles (e.g., making sure non-discounted prices are displayed to overweight customers). However, these practices are not as individualised as they initially seem. Instead, as will be discussed further below, most in-store advertisements are based on a set range of consumer profiles.

3.2.3. Public Space

In public space, advertisements appear based on what types of persons are detected nearby, the time of day and local behaviour. These personalised adverts are the product of sentiment analysis, location determination technologies, biometrics and CCTV scanners as well as data mining. Individuals have gotten used to their profiles being identifiable based on the vehicles they drive, their facial characteristics and the items they carry (including the clothes they wear and their personal communication devices). Billboards read this biometric information and alter their displays based on the age, gender and ethnicity of the person passing by. They display different advertisements to middle-aged Asian women, to young, white men or teenage girls. Much like in-store advertising, high street advertising also utilises screens that ”read“ and/or identify individuals passing by shops. Teens are often embarrassed by advertisements directed at parents or other adults and they compete with one another to discover who can have the trendiest ads displayed to them.

Location determination technologies have become pervasive in public space. Many mobile devices include applications branded as ”location services“ or ”entertainment services“, but which are actually advertising. These mobile applications detect individuals’ location or travel patterns and offer solicited or unsolicited ”suggestions“ about places to eat, entertainment venues, activities, new stores or new sales all based on previous visits, expressed interests and/or profiles. These can be highly personalised, where, for example, based on location information, an app detects that a person is on his way to work and pings a new ”sandwich of the month“ for him at his favourite local lunch place. While consumers may think that these suggestions are based on preferences only, in fact, the application only displays suggestions linked with subscribed shops, restaurants and entertainment venues.

3.2.4. Home

Smart advertising technologies have long since permeated the home. In addition to monitoring usage, reduced-rate hardware supplied by commercial organisations and/or media companies (e.g., Smart TVs) also includes biometric recognition and sentiment analysis features. Biometric recognition features are part of the hardware security to prevent unauthorised usage or theft. However, they also identify the characteristics of the individual(s) using the hardware or accessing the content. This information is recorded and fed back to companies, political lobbyists and government actors. Sentiment analysis and, increasingly, micro-behavioural and neural analysis are used to determine how individuals experiencing ads or media content on close proximity devices (televisions, computers, mobiles, etc.) emotionally respond to them. Information on this emotional reaction is fed back to commercial organisations (and, where appropriate, their political clients) and used to continually ”tweak“ the advertisement or content for different segments of the population. Sophisticated systems can also identify the objects in a room, including an individual’s clothing, to recognise brands, models, etc., either using visual data or RFID data embedded in the objects to both deduce disposable income levels and individual preferences. Such dynamic analysis is in particular valuable for identifying visitors and friends. Advertisements are also based on this information as well as data collected from accessories for devices already purchased or new models when detected devices are aged.

The collection of such information was initially deemed to be an invasion of privacy and a curb on individual free will. However, political arguments about the personal benefits and greater social good that would come from a relinquishment of some aspects of privacy prevailed over the privacy arguments. Politicians pointed out that individuals were not required to take advantage of the discounts and offers available to those who signed up for these various services, and that even discounted products could be later ”upgraded“ if an appropriate fee was paid. However, as the years passed, and as people got used to the system, it became increasingly difficult to obtain goods and services without submitting data to the mass data bank. As more people shopped online, shops on the high streets began to close. Thus, while it is still possible to obtain some goods for cash, cash transactions have significantly diminished and cash itself is rarely used. In fact, cash payments have become a sign of poverty and illegality, as mostly those without proper credit lines or questionable purchases prefer them to digital transactions.

3.3. Profiling

The purpose of collecting all of this information from consumers and citizens is to create ever more precise personal profiles. Although many adverts seem highly personalised, they are in fact based on a set number of sophisticated consumer profiles. Despite the fact that the initial intention was to provide personalised content, companies soon found that this was not cost effective, so they pared down their content to be based on profiles. In 2022, there are 127 different personal profiles. These are divided by age (child, teen, young adult, middle aged, pensioner), class group (professional, middle, lower and under), special interest (sports, home décor, etc.), gender, family type (hetero-sexual couple, same-sex couple,

nuclear family, single parent, etc.), political party, known hereditary or active health issues (obesity, diabetes, etc.) as well as others. Data sharing conglomerates and third-party companies aggregate information from the databases of different subscribed organisations to provide a more complete picture of profiles and individual customers. Because these databases of information are combined, customers are often surprised to learn that their health insurance rates have decreased with the purchase of a treadmill or that their flat-rate communication subscription fees have increased once their child becomes a teenager.

Government agencies and departments also access these profiles and build their own. The police and security services are given access to the aggregated data held by the government ID programme about individuals and have a budget to purchase additional information from data vendors about shopping habits, media consumption, etc. They use this information to build profiles of potential offenders and block particular purchases. Government departments also tie benefits to aggregated and individual consumption patterns. While many individuals get the discounts and conform to government expectations around purchasing behaviour, some working class individuals (particularly those most in need of the discounts and offers) find themselves inexplicably prevented from accessing particular goods and services. In fact, only certain authorised individuals are able to purchase items such as weapons, alcohol or specific media content, and they use their government ID card, with their personal shopping profile, to prove their ability to make these purchases.

3.4. Manipulation

Because decision science has revealed that habits are so entrenched, companies have sought to break the habit cycle entirely in order to have more control over customer purchasing. One of the effects of these smart advertising practices is the manipulation of consumers.

Profile-based media content is full of embedded advertisements, and consumers are informed about their ability to purchase goods that they see on television, films or hear about in radio advertisements through applications on their TV, phones or computers. Many companies take advantage of decision science sensors to monitor the items (clothing, electronics, etc.) in which an individual notices or expresses an interest in and highlight these for the consumer within their social media streams (e.g., ”Simon just bought the new X11 camera for 299,-. Read the review here and profit from 15% discount if ordered by Saturdayi‘) or through traditional-looking (but highly personalised) ads at the end of a TV-show or internet video. Mouse-over messages explain the features of a product tailored to the individual (”The Krups X51 links with your Samsung 3100 alarm clock to automatically start your coffee whenever you set your alarm“) through purchase data stored on the cloud and linked with other appliances or company records. This information is combined with demographics, income and credit information to highlight either more affordable, similar items or to identify finance arrangements that customers could access in order to obtain items. Customers have already been ”sold“ the idea that scientific marketing provides needed information and necessary updates about available products and services.

Partly because of the closure of most high street shops, many customers are signed up to personalised shopping services for their clothing which highlights items that they

may be interested in, much like stores previously used in-store displays and mannequins. These suggestions are based on profile category and previous shopping selections. For a monthly fee, new clothing items are automatically shipped to consumers based on their preferences or the preferences of their friends as gleaned from social networking data. Such subscriptions to mainstream store conglomerates are relatively affordable for the vast majority of families and as a result, a few mainstream chains control most clothing distribution. Because of the finite number of profiles, as well as considerable overlap, individuals often find that they are wearing very similar clothing items. Self-expression, through dress, is undermined as specialist-clothing items are increasingly expensive for all but high-income families. However, people often have one specialist item that is far more expensive than their other clothes. High-pressure sales tactics (”Hurry, only 2 left“) are often used and may be integrated with social networking platforms (”88% of your friends already have one, don’t be last“). This marketing strategy has proved particularly effective for young people.

As a result of research findings in neural modulation that magnetic fields may have an effect on an individual’s mood, some stores are experimenting with magnetic devices at store entrances. These devices are thought induce a low mood when individuals are in the shop in order to increase spending. Shoppers are told that the devices are in operation to ”manage customer behaviour“. Many shoppers do not realise that they are being manipulated in this way, because they assume that the devices are intended to have a calming effect on unruly individuals displaying ”anti-social behaviour“. Although shoppers who do understand the devices are unhappy about them, retailers are within their rights to install such devices without consumer consent because stores are considered private property.

Political parties, governments and interest groups have been using personalised advertising for the last five years. Political parties, lobbying groups and other organisations with specific political agendas (e.g. energy companies, religious groups, etc.) all purchase media time and target advertisements to individuals thought to have particular viewpoints. This could include shoring up support for particular political issues, or attempting to influence the opinions of individuals thought to be undecided. The vast majority of individuals and groups receive content, which supports and cements their established opinions; however, some independent individuals thought to be amenable to influence are bombarded by constant and confusing political messages. Political parties heavily target these undecided voters, and cater policies to them. The result is an increasingly fractured, centrist political system that satisfies none of the established opinion frameworks and is plagued by delays and conflicts. Despite the increasingly political character of advertisements, interest in politics decreases further, and turnout at the last general election was only 20%. Many people no longer see the point of voting. The social landscape has stagnated and unemployment remains relatively high because of the focus on consumer goods rather than political and social progress. The promised ”trickle-down effects“ of personalised advertising in terms of increased consumer spending and thus increased production fail to materialise.

3.5. Inequality

Smart advertising practices have also increased social and economic inequality. Advertisements are tailored to class profiles, and because generalised advertisements are so unusual, people have very little information about products and services not linked with their profile. In relation to health or financial services, individuals on low incomes, or who live in low-income areas, have little information about more generous financial packages (e.g., lower interest rate mortgages) or more expensive health-related products (e.g., treadmills or whole-grain foods). This leads to greater social segmentation and stratification.

One of the major innovations of the last 10 years is the ability of organisations to alter their prices based on the profile of the person purchasing the item. Online, the stratification of prices has been occurring for some time through pre-configured web displays. Inside stores, this has been accomplished because cash registers are directly linked to customer database, allowing them to offer individual discounts at checkout time. Consumers can additionally use smart phone applications to scan prices on individual items to uncover their personalised discount during shopping, or get recommendations on ”their“ discounted products when they enter a store. Stores themselves are also stratified, since less well-off individuals cannot afford to purchase items in high end stores without such discounts, and insulated, high-end shoppers are discouraged from shopping at bargain stores because of the lack of discounts for their profile category (and the supposedly unpleasant clientele). Due to the widespread availability of discounts, shoppers rarely realise that stratified pricing occurs, but instead appreciate them as benefits for valued customers. People’s social networks are increasingly mined for information about lifestyle, which could impact the prices they pay for financial services, luxury food items (e.g., junk food, alcohol, etc.) and some electronic devices.

This has a particular effect on financial services and health services. For example, those with financial difficulties or whose profiles match individuals with financial difficulties are charged full price for financial services while others receive generous discounts. People who mention drinking, gambling, risk-taking behaviour, etc. on social networking sites are also charged full rates for loans, mortgages and insurance or denied financial services, while those with a ”clean“ profile receive lower prices. Those with particular, preventable health problems or whose DNA profiles suggest a predisposition to health problems such as obesity, type II diabetes and high cholesterol are charged MSRPs (manufacturer suggested retail price) for video games, junk food and alcohol, while those without such diseases enjoy discounts. This means that the poor, older people and those who already have health problems find that they spend more of their relative income on food and other essentials. Governments and retailers justify this pricing by stating that these individuals are instead offered discounts on ”good“ items, such as fruit, exercise equipment and running shoes and that this balances any price discrimination in terms of junk food. People who purchased junk food or cigarettes early in life also find that their health care coverage is significantly more expensive than someone who purchased healthy food and did not smoke in their 20s. Increasingly, private health care organisations are effectively refusing coverage for individuals who make unhealthy purchases or who have particular DNA profiles by offering coverage at very high rates only, which has significantly increased pressure on state funding

for health care. Those who refuse to provide such data are automatically classified with the highest rates in private health coverage. The higher prices charged for obese people of those with health problems for junk food is intended to defray the costs of their state health care.

Because more and more devices integrate keystroke recording, police can obtain the full contents of a suspect's text-based communication (e-mail, social networking, text messages) and their movements with appropriate warrants. Individuals who communicate with a suspect and/or who were at the same place at the same time as a suspect face police questioning. As a result, more individuals have contact with police, and are more likely to experience being a suspect than previously.

3.6. Identification

The identification of individuals, including their name, address, and age as well as connecting them with particular characteristics is another feature of smart advertising. Shoppers are greeted by name in stores and individuals are authorised to purchase certain specialty items (e.g. weapons) and may be authorised to purchase items such as alcohol or cigarettes at particular discount prices. Such purchases require the customer to display their government ID number. These practices of identification make it difficult for people to purchase items for one another, or to do family shopping. For example, partners with different health characteristics may be forced to make multiple shopping orders for groceries or other items in order to take advantage of competitive prices, protect their health insurance premiums and/or their financial credit rating.

In-store and public space advertising based on biometrics and/or identification also mean an individual's personal or health characteristics may become public knowledge. Teens with skin problems find themselves more often exposed to advertisements for acne medication, while those with mental health problems may see more ads on counselling or new pharmaceuticals. Given that all public advertising is targeted, teenagers often harass each other if a particularly embarrassing advertising (e.g., offering advice on incontinence) appears near their group. This can lead to embarrassing interactions in shops and public spaces and has prompted shy individuals with such conditions from refraining entering such spaces close to their homes where they might run into friends or acquaintances.

3.7. Chilling Effects

Individuals have become wary of doing Internet searches about particular medical symptoms, social issues (bankruptcy) or political issues because such search information could be collected by third-party organisations and used to influence either advertisements that appear or financial or health-related products and services targeting the inquirer. Such searches become ”public knowledge“ once they occur; and some people have suffered consequences such as reduced credit ratings after searching for bankruptcy or higher health insurance costs after searching for information on diabetes symptoms. In less democratic

countries, political dissidents have also been prosecuted for visiting pro-democracy or opposition political party websites. School children and university students have repeatedly come under investigation by the security forces after doing assignment-related research on sensitive chemistry, geography or political topics, so teachers and professors have begun to explicitly register such assignments and the list of students involved in them. While some computer-savvy individuals understand how to use proxy websites and ghost log-ins, other less sophisticated ICT users are prevented from or shy away from gaining vital health, political or financial information because of fears about how it may affect their access to services. The media rarely report such abuses, partly because they are so frequent and partly because the media fear being an object of investigation themselves.

3.8. Conclusion

Although small pockets of resistance to smart advertising practices have emerged, the social effects for the vast majority of individuals remain negative. Proxy web sites, web browsers and pirate or anonymous pay-and-go Internet connections have become more common as individuals attempt to avoid Internet surveillance. While most members of the population do not make use of such systems, they are used by a small subset of privacy activists, individuals with socially unpopular interests (pornography), political activists and marginalised individuals in less democratic and liberal countries (civil rights activists, pro-democracy agitators, etc.) and criminal elements. Similarly, while most people simply accept stratified and high pricing for particular items, a significant black market trade has also emerged. However, the impact of this resistance is limited, since cash is used so infrequently and large sums of cash can be difficult to handle without raising the interest of authorities, and because people are generally concerned about gaining a criminal record and the additional changes to their lifestyle that this would engender. As a result, many smart advertising practices, particularly when they are combined with other security and surveillance technologies that have proliferated in the last 10-20 years, have social consequences that effectively reduce democratic choice and free will in terms of access to goods and services, media consumption and people's relationship with government.

4. A New EU Border Management?

Rocco Bellanova (VUB-LSTS)

Ceuta, Spain. 30 Sept. 2022. Today, 8 years after the adoption of the so-called 'smart borders legislative package', the EU Commissioners for Home Affairs and for Justice, Fundamental Rights and Citizenship have jointly called for the immediate suspension of many of the related border security programs and stated the "urgent need" for its thorough review.

The announcement has been released at the end of a special meeting held in the Spanish enclave of Ceuta, where the two Commissioners had been invited, together with EU interior and justice ministers, to attend the final works of the European Parliament (EP) temporary committee on borders. While far reaching in its consequences, the decision of the European Commission does not come unexpectedly, as the eight years of EU smart borders have been accompanied by increasingly harsh criticism and have been plagued by several inefficiencies and continuous malfunctioning.

The very decision to create an ad hoc EP temporary committee two years ago signalled a first move out of what has been defined 'ultra-surveillance' and its rhetoric, e.g., the political and economic marketing of smart surveillance measures as definitive solutions to border related issues.

To some extent, this rhetoric, pretty successful in the first decade of the millennium, was a victim of its own ambition and its tendency to cover and ingest a wider scope of social, economic and political activities, and thus a growing number of individuals and stakeholders. Not only were criticisms raised in terms of fundamental rights, but they were soon coupled by accusations of inefficiency when the first measures were implemented at full scale in the second half of the 2010s. Specific cases of malfunctioning systems have triggered serious violations of human rights, as reported by NGOs and the press, and hampered the very work of border controls agents, who tend to rely still less on the 'decision support tools' put at their disposal.

4.1. The Italian incident

Probably less serious, but of high impact in terms of public visibility, a series of accidents involving smart border surveillance devices have contributed to the questioning of ultra-surveillance. To date, the most famous case is, possibly, the trapping into automated border gates of several members of a delegation of the Italian parliament, back from a mission to Syria. After matching their identity documents and travel information with other databases,

the system ranked the deputies as potential terrorists, sealed the doors of the cabins and triggered the Special Forces alarm. The border control agents supervising the automated gates were not alerted by the system - supposedly because of a technical bug, and were not able to intervene to un-block the secured doors before the arrival and deployment of the counter-terrorism unit. The members of the Italian parliament were 'freed' only two hours later, when the media had already published the news and posted videos and photos taken by other travellers. While imprisoned in an automated border gate, two members of the Italian parliament suffered from severe panic attacks, one of them fainting. The event attracted further media attention to other similar accidents, and to the general issue of false positive matches.

4.2. General trends of smart border management

Despite the official emphasis on a holistic approach to border controls, the programs proposed and put in place in the last eight years are extremely scattered. Still, some general trends are noteworthy. First, there is the emphasis on a tailored and targeted approach: on the one hand, two individuals will rarely undergo the same kind of controls at the same point of entry, and, on the other, the devices and interfaces at the disposal of border officials are designed to be highly customized, taking into account the style in which each official carries on his duties.

Second, the interest in checking the identity of people crossing a border, or the consistency of their travel patterns, has been matched by an interest for the data and information they convey, store or access by their own devices. Retention is supposed to be the exception, that is, only when the screening has provided positive matches, but official figures on stored data are very high. Besides telecommunication devices, the surveillance of objects crossing the borders has been heightened.

Third, many border controls are increasingly conceived so as to afford a sort of 'variable geometry'. The goal was to push further the idea of interoperability among different systems: vertically, so as to make available a larger amount of data and information, and horizontally, so as to extend the reach of specific devices by coupling two or more of them in case of need. Widening the net and thinning the mesh. The 'variable geometry' approach has clashed with the not only with the fundamental rights of privacy, fair trial and the presumption of innocence, but also with the principle of purpose limitation in data protection. It has also paved the way to a much wider use of the same smart surveillance technologies at internal EU borders, first especially when political meetings or other big events are scheduled, and later on, people getting used to it, as a permanent device that can be activated at will even by medium level officials.

Fourth, firms provide services, software and tools to public authorities, and in several scenarios they directly enforce controls. But their role is difficult to discern and ascertain, since many companies play a sort of passive role, by either providing access to their databases, or pushing information when requested, so as to avoid government fees, or to obtain financial help from Member States. A particularly interesting trend concerns the decision of some airlines, with their routes covering the Mediterranean Sea, to install specific

radars and sensors on their carriers, which are able to transmit in real time information to Member States' border units. In the EU Commissioners joint statement, three programs were mentioned as high-priority for review: the Borders Common Information Sharing Environment (BCIS), the Mobile External Units (MEU) and the Enhanced Automated Border Gates (EABG).

4.3. Three programs under the Commissioners' spotlight

In the EU Commissioners joint statement, three programs were mentioned as high-priority for review: the *Borders Common Information Sharing Environment* (BCIS), the *Mobile External Units* (MEU) and the *Enhanced Automated Border Gates* (EABG).

The first program was presented eight years ago as the outcome of the first attempt to create a common European system of border surveillance. As a "user-friendly, dynamic system of systems", in the words of the then EU Commissioner for Home Affairs, it was supposed to provide a smart interface amongst different databases, tailored to respond to the needs and behaviour of each user. In other words, the platform was to connect officials to all "border relevant databases", either held by public authorities or by private players, sifting and prioritising information on the basis of their official mission and their precedent behaviour in the use of the same system. The project has been highly criticised from different perspectives: the highly intrusive nature of its functioning; the linking and merging of a too comprehensive list of "border relevant databases"; the elevated costs incurred in the development of the sifting software; the technical difficulties in the effective implementation of the connection; the scarce relevance of information provided to field officials. Given these and other issues, many commentators were already expecting a suspension and review of the Borders Common Information Sharing Environment.

The second program at stake concerns the *Mobile External Units* (MEU). Initially presented as a mere support tool to assist third countries with limited assets for border management, they have acquired a strategic and controversial position in the EU system of external border management. MEUs are composed of a mixed team of local and EU officials (from border and law enforcement agencies). They are equipped with mobile surveillance and communication systems, able to connect to both third countries' and EU databanks, and to collect information and personal data from the dispatched location. From the point of view of several critics, rather than missions of technical cooperation, these units have been designed to push border controls way beyond the physical border of the EU. Furthermore, little formal overview is granted over their field operations, and several NGOs focusing on the human rights of migrants and asylum seekers have questioned their inability to ensure high levels of protection, or the possibility to start a request of asylum.

Finally, among the three programs prioritised for review, the *Enhanced Automated Border Gates* (EABGs) is probably the smart border control system most widely known by the public. EABGs have been developed to foster the previous pilot projects carried on at the main international airports. The initial goal was to provide a swift and fully automated process of ID controls, to be matched against specific databases. Human intervention was foreseen only in the case of positive matches, and, in case of the identification of a terrorist

suspect, special units of the army were also alerted. But, one step further, similar machines were developed for other scenarios to collect, analyse and match additional kinds of data. These machines exploit the time individuals are queuing to operate random or targeted controls on them and the devices they are carrying. The first bunch of Enhanced Automated Border Gates have been requested by several law enforcement authorities for exceptional deployment at internal EU borders, when important EU or international political meetings have been held outside of Brussels, with the aim to screen and sort out potential troublemakers. Both their intensive use in conjunction with political meetings and their highly intrusive and secretive functioning have sparked sharp criticism. Despite the modification of technical features concerning data storage and human overview, EABGs soon became the symbol not only of the infringement of fundamental rights of a large number of citizens, but also of the political stakes in the design and deployment of these measures. Several cases have been brought to the European Court of Human Rights, and a decision is expected soon.

4.4. Rising criticism

As mentioned above, the creation of the ad hoc EP temporary committee was not the only, or isolated, sign of critique towards the evolution of EU border management. From the outset, many actors and events have challenged the apparent consensus around smart borders. In particular, critical voices from field officers, court cases finding violations of privacy, data protection, non-discrimination and other fundamental rights, a continuous resistance from advocacy groups and lay citizens, and unveiled scandals concerning public/private partnerships kept the attention high on the deployment of these measures. So far, criticism has also been boosted by the inability to complete the implementation of many measures, and, in several cases, the collapse or continuous malfunctioning of extremely expensive technologies. Furthermore, the measurement of the efficiency of the measures has proved particularly problematic, and some of the metrics initially established are no longer considered relevant.

Strong political pressure and constitutional courts' decisions have already pushed some Member States to give up the implementation of specific measures, generally the most controversial ones. Even before today's announcement, several EU Commissioners have expressed caution on smart surveillance technologies, engaging in a series of open consultations with stakeholders, this time including victims of the malfunctioning of deployed systems. The most important sign of change is probably the presentation of a legislative proposal on the establishment of common system of Protected Entry Procedures (PEP), tabled by the Commission two years ago, and strongly supported by the EP. If adopted, the regulation should create a mechanism which would facilitate the submission of asylum requests for individuals unable to reach the territory of a EU Member State.

4.5. Still many pending issues

Hence, today's announcement an historic step towards a new EU style of border controls, one that takes respect, hospitality, transparency and fundamental rights, but also correctness and firmness, as a starting point instead of suspicion, fear and exclusion. Despite the enthusiasm of many members of the EP and delegates from civil society, the answer should be cautious. Many important issues are still pending. If setting up a system, even an unachieved one, required a lot of efforts, time and money, its removal and reconversion, are an open challenge, especially if public attention will not remain alerted. Many agreements with third countries are still secret, and transparency in the field is still to be achieved. The sharing of competences in this area is a particularly complicated matter, and co-ordination around a new project will surely take time, efforts and compromises.

But, more importantly, fully alternative paths for border controls should still be defined. A new language, of words and things, has still to be fine-tuned.

Part II.

Deliverable 2.2: Report on stakeholder workshops

5. Workshop on "Smart Surveillance and Security in Public Spaces"

Silvia Venier (CSSC)

This chapter collects the main topics discussed during the 1st stakeholder workshop on “Smart surveillance and Security in Public Spaces” that took place on 27 June 2012 in Amsterdam. Participants included representatives from SAPIENT partner institutions, members of CSOs and consumer rights associations, officials from the law enforcement sector, representatives of data protection authorities, research organisations and industry.

The sections below present the main topics discussed during the meeting more in detail.

5.1. Technological innovation in the public security field: who is the target? who is vulnerable? who benefits?

The issue of the availability of technology is one of the key concepts that were discussed during the first part of the workshop. The scenario mainly focused on the technologies currently available or emerging in the very near future.

A key question introduced by a workshop participant and partner of the SAPIENT project was whether technology is introducing a real novelty in this field, or is this just a different way to do something old. One participant from the defence research sector followed up this consideration to state that the main differences in what we are witnessing these days is that surveillance can be done in real time, on demand. Some participants enlightened that the difference today is that have also much more data available and we often don’t know how this data is handled by the controllers. As one representative of the law enforcement sector mentioned, it should be noted that in some circumstances much higher quality of data can also mean enhanced data protection for the data subject.

Other points raised by representatives of the law enforcement sector were that smart systems are self-deciding, the use of these instruments is automatically leading to intervention. When a decision is automated this introduces fundamentally new differences. As suggested by CSO representatives there is also the danger of data mining, with too much reliance on the data itself. One participant from a CSO replied that what is fundamentally different from the past is the focus on prevention by removing the potential “trouble makers”[1] before the actual event. In this context, deterrence is simply removed (e.g. cameras

[1] This term, used in the scenario, was highly criticized by some workshop participants as an euphemistic way to say that visitors of an event are under general suspicion, and surveillance is even targeting offenses that do not justify an infringement of privacy.

are hidden): everything is about taking the potential “trouble makers” into custody before anything happens. This can significantly erode the presumption of innocence and the principle of “nulla poena sine lege”. There is additionally the risk of moving towards a police state, where public security agencies have to answer critical questions, such as what does it take to be regarded as a potential “trouble maker”.

Another point was made with reference to the increasing reliance on technology systems. An example was provided by a SAPIENT partner that when new technologies were introduced in the medical field, these resulted in a decrease of diagnostic capacities of doctors; however there was also increased reliance on screenings with many consequences in terms of costs, false positives, and so on. The question was thus posed whether we are going to see a similar situation in the security field. The key issue is that by increasing our faith in technologies, we seriously risk to decrease our reliance on human intelligence, which is the most important element in any field. This may lead to an increase in pretended (but not real) security at the expense of significant privacy infringements. In this respect, other CSO representatives suggested that the human involvement in technology use is always desirable, others recalled the concept of “security theatre”.

A different perspective was offered by a SAPIENT partner on how to conceptualize the scenario from a different perspective, by enlightening the social functions and narratives of the events described in the scenario. This was suggested because it is always important to contextualize the broad concept of security, to consider it in a specific context. With reference to the proposed scenario, the football world cup can be seen as a simulation of war, a way to express “legitimate” or “symbolic” violence. The key question is what is the proportional level of violence that is acceptable? While deciding to implement a security measure, responsible agencies have to take into account also the social functions of the event they protect.

A representative of a research organisations also suggested that one thing that is missing in the scenario is the consideration of the sabotage effect, i.e. the attempts to circumvent and spoof the systems. The technology push is so strong that it will certainly move forward, but technology can fail (e.g. false positive and false negatives), or can be voluntarily circumvented, and this requests a sort of counter action. There should be an interest in knowing more on the counter measures to this sabotage potential, and to see how different actors may behave in this respect. Usually, however, the malfunctioning of or resilience towards new technology does not mean that the technology will be abandoned or not implemented.

5.2. The Rule of Law – How technology interacts with the legal and policy framework

More detailed considerations on the implications for the right to privacy, data protection and related issues, as well as societal needs were also provided by participants during the workshop.

First, the importance to define data ownership as well as clear rules for the public/private partnership in data sharing was mentioned by a representative of the law en-

forcement sector. It is becoming more and more difficult to know who is accountable for the protection of the collected data. As noted by a CSO representative the privatization trend in security and surveillance, as well as the concept of informed consent in consumer and privacy law are crucial in this respect (e.g. information on the rights and which data will be stored and how it will be used). A CSO representative also pointed to a contradiction in the scenario: it describes hidden surveillance measures and at the same time claims that in the depicted future most people accept surveillance. If this was the case, why had surveillance to be hidden?

A representative of a research institution raised the question of hidden or even open resistance, giving the example of the current strikes in Québec and the news of government law prohibiting assemblies in public spaces. This is a privacy relevant case, because privacy is also a matter of intrusions on social relations.

During the second part of the workshop, an in-depth discussion took place with respect to the right to self- determination and anonymity. A CSO representative suggested that a question missing in the scenario is whether do we have the right to anonymity, which is crucial for developing our own personality and society as a whole. The right of self-determination and the right of association are preconditions for the development of a free and democratic society. The right to be forgotten was also discussed as one of the main novelties of the proposed new EU data protection regulation. This right is, in the words of Vivian Reding, “a completely unfeasible right”. It cannot be enforced in the digital world, a virtual place where you can not erase digital traces. An effort was requested by a representative of a research institution and partner in SAPIENT to conceptualize this right in a different way, since the worst thing for a right is not to be enforceable. Actually the right we want to protect in this case is the right to be ignored, the right to discretion. This means that you cannot erase traces but you can oblige authorities or private companies not to use the information about you, to ignore that information. Privacy is not the absence of information, it is rather restricted use of information. Other CSO representatives argued that the right to be forgotten cannot be seen on equal terms with the right to anonymity (that includes the obligation to make our identity evident), and that this is a political question. The point is that we should be able to delete traces when possible.

An industry representative suggested that, on the one hand, there are laws and ethical principles, on the other hand it is crucial to take changing public perceptions of technologies into account. With respect to the criteria to define “social impact” and “public acceptance” of such technologies, an ongoing EU project (ValueSec) is preparing a decision support system for decision makers; and one of the main pillars of this project is defining qualitative criteria of the social impact. A set of social criteria (120) to be used to assess social impact has been identified by ValueSec. The draft list is going to be used as a reference for the use cases, when the list will be revised by end users. There is also the need to understand the difference between societal impact (which is an area of huge scientific ignorance) and ethical analysis.

5.3. Privacy related issues and other societal implications

More detailed considerations on the implications on the rights of privacy, data protection and related issues, as well as societal needs were also provided by participants during the workshop.

First, the importance to define data ownership as well as clear rules for the public/private partnership in data sharing was mentioned by some participants. It is becoming more and more difficult to know who is accountable for data protection. The privatization trend in security and surveillance, as well as the concept of informed consent in consumer and privacy law are crucial in this respect (e.g. information on the rights and which data that will be stored and how will they be used).With this respect, a participant also enlightened a contradiction in the scenario: the paper describes hidden measures of surveillance and at the same time claims that in this future possible scenario that most people accept surveillance. If this will be the case, why surveillance has to be hidden?

Another person talked about the question of resistance, giving the example of the current strikes in Québec and the news of government law prohibiting assemblies in public spaces. This is a privacy relevant case, because privacy is also a matter of intrusions on social relations.

During the second session of the workshop, an in depth discussion took place with respect to the right to self determination and anonymity. A participant suggested that a question that is missing in the paper is whether do we have the right to anonymity, that is crucial to develop our own personality and society as a whole. The right of self-determination and the right of association are preliminary conditions for the development of a free and democratic society. The right to be forgotten was also discussed, as one of the main novelties of the new data protection proposed regulation in Europe. This right is, by the own words of the Vivian Reding, a completely unfeasible right. It is not enforceable in the digital world, a virtual place where you cannot erase digital traces. An effort was requested by a participant to conceptualize this right in a different way, since the worst thing for a right is not to be enforceable. Actually the right we want to protect in this case is the right to be ignored, the right to discretion. This means that you cannot erase traces but you can oblige authorities or private companies not to use the information about you, to ignore that information. Privacy is not restricted information, it is rather restricted use of information. Other participants argued that the right to be forgotten cannot be set at the same level of the right to anonymity (that includes the obligation to make our identity evident), and that this is a political question. The point is that we should be able to delete traces when possible.

A participant suggested that if from one side there is law and ethical principles, from the other it is crucial to take into account the perception of the technologies in the public. With respect to the criteria to define “social impact” and “public acceptance” of such technologies, in a recently funded EU project (ValueSec[2]) they are preparing a decision support system for the decision makers, and one of the main pillars of this project relies on the definition of qualitative criteria of the social impact. A set of social criteria (120) to

[2] http://www.valuesec.eu

take into account to assess social impact have been identified taken into account. The draft list is going to be used as a reference for the use cases, when the list will be revised by end users. There is also the need to understand the difference between societal impact (is empirical question, and this is an area of huge scientific ignorance) and ethical analysis.

5.4. Solutions: legal, technical, political and the role of stakeholders

The main means to govern technological innovations mentioned in the discussion were regulation, control, technical solutions, accuracy, transparency and education.

Focusing in particular on the proportionality of the security measures, it is important to consider that several levels of protection can be distinguished, as suggested by a representative of the law enforcement sector. The threats are numerous and can come from different sources, and a good early assessment of the risk, of the possible threats is a central point. With respect to the risk assessment, it was suggested to consider the concept of collateral damage, i.e. considering the objective you want to achieve, which is the acceptable damage. This concept needs to be included in an impact assessment.

Taking into account that there is always a gap between the legal framework and the technological progress, technology has to be included as part of the solution: Technological approaches to data minimization and purpose specification have to be taken into account, for instance privacy enhancing technologies (PETs) and privacy by design (PbD) principles should be implemented. This was suggested by a representative of a research organisation.

A CSO representative also brought up the problems emerging with public and privacy partnership in data sharing. Looking at the scenario from a data protection point of view, the main challenge will be to control the flows of data collected by private companies and the access granted to third parties including public actors such as the police. Conditions for this kind of data sharing need to be defined. The education of actors in law enforcement such as police officers that data protection is an important part of their security and law enforcement goals needs also more attention.

It was also suggested by a representative of a research institution that there is a difference between “targeting” and “accuracy”. In many systems it is not necessary to use the most detailed and accurate data, and different actors need different levels of accuracy in this respect. However, usually the same software seems to be available to all kinds of end users, without taking into account the different levels of accuracy needed. Is accuracy a way to enforce rights? Should regulation enforce higher accuracy?

Another idea suggested by a representative of a research institution was that the solution is not merely a technical issue, but depends on good communication practices with the public. Most of the people are not aware, are not conscious of the concerns with respect to privacy and data protection, this is why education is crucial. Investigation through focus groups on public perception of privacy and security is also paramount.

6. Workshop on "Smart Surveillance and Personalised Advertising"

Rocco Bellanova (VUB-LSTS)

The Workshop took place at TNO, Hoofddorp, The Netherlands, 27 June 2012, 14:00 - 17:00.

The second stakeholders' workshop focused on smart surveillance and personalised advertising. The workshop was composed of two sessions of debates, separated by a short coffee break, and moderated by a member of the SAPIENT consortium. At the beginning of the first session, the SAPIENT partner responsible for the drafting of the scenario provided a short presentation of the scenario itself, as well as of the methodology followed and of the main purpose of the workshop (cf. introduction of the same deliverable). In this occasion, the scenario was explicitly labelled as 'dark', so to sketch a possible picture of what could happen if no regulation at all is enacted. After this short introduction, both sessions were mainly devoted to debate among the participants. At the end of the second session, a short wrap-up note was provided by a member of the SAPIENT team.

Workshop participants included officials from national authorities, representatives of different private firms; researchers from academia and think tanks, and from different disciplines; members of civil liberties associations and consumer rights groups; as well as partners of the SAPIENT consortium. It should be noted that some stakeholder representatives had also participated in the first workshop.

6.1. The economic and market dimension. Which benefits? For whom?

The debates triggered by the consortium scenario touched upon several different topics, but many of them related to the economic and market dimension. The very characteristics of the market environment depicted in the scenario were a first issue of discussion, as a representative from a consumer rights association noted the need to account not only for the development of privacy-intrusive techniques, but also for the possible growing market of privacy preserving tools. Still, within few minutes, the 10-year forecasting element of the scenario led the way to a discussion more focused on current practices concerning personalised advertising. Hence, participants focused on the related topic of the potential or effective benefits of the technologies and practices of personalised advertising, comparing different techniques, already fully developed or currently under development. Indeed, as stated by a representative from a private company, the potential benefits for consumers

should also be acknowledged. The question of potential benefits paved the way to several controversies among the participants, touching specific topics such as their eventual distribution, their social or individual dimension, the correlative sharing of costs, and the transparency and design of the economic and technological models on which benefits are generated. For example, a representative from a consumer rights organization underlined the tendency of some business models to make those who do not participate to loyalty schemes pay the costs of the benefits that they offer to specific clients who do. An advocate from a civil liberties organization underlined that even if some systems can offer benefits to customers, they still risk endangering the societal dimension. Another advocate, also from a civil liberty organization, questioned the very basis of the current debate on benefits, underling the misleading character of the 'privacy versus benefits/free services' approach, and proposed rather to understand where the effective benefits, in terms of economic gains, lie. Triggered by an explicitly provocative comment from a SAPIENT member, this debate also took into consideration the potential commodification of personal data, as, de facto, most of the business models offering free services are requesting customers' data in exchange, and are using them to make profit. From this point of view, it would be necessary to explicitly acknowledge the economic dimension of personal data, and include in the discussion the ways in which a better economic deal could be reached.

6.2. On consent, transparency of data management and customers' awareness

The benefits debate was intertwined with three other key issues: the technical and legal possibilities of consent; the transparency of the data management systems; and the awareness of customers.

The question of consent was first raised by representative of a civil society organization. The advocate was keen to highlight how consumers often do not really have the possibility to understand what happens to their data (because the operations concerning personal data are far from being explicit), or that they do not have any effective possibility to refuse the collection and processing of their data, as the only alternative is to risks full exclusion from a set of services. From these perspectives, the very meaning and effectiveness of consent could be lost. A possible solution proposed by the same expert was to further generalize the opt-in approach. This sort of 'opt-in default solution' was questioned by a representative from a private firm, who proposed rather to differentiate between different spheres of activities, identifying those were a 'true opt-in' is necessary, and other were the 'opt-out' approach could be maintained, even if more clearly and friendly communicated. As noted by other two participants, from a data protection authority and from a civil liberties organization, the choice operated by companies between an opt-in or an opt-out approach is particularly important at the moment that new customers register, as the technical design chosen seems to influence the behaviour of people signing-in new services. Finally, a member of the SAPIENT consortium noted the risk of taking 'informed consent' foregrounds the consumers-companies relationship. Not only does the 'informed consent' model risk weakening the power position of people, rather than empowering them, but it is also heavily based on the 'rational choice' model, which is often far from reality.

In parallel, many experts representing different stakeholders raised the issue of the transparency of data management systems. For example, a member of the SAPIENT consortium raised the question of the sharing of personal data beyond the company initially collecting them, and a researcher from academia pointed out the need, even in the scenario, to further clarify the inherent risks of creating a database, and also to take into consideration business models that remain successful (and even propose to consumers free services) without using profiling. Another member of the consortium underlined the potential advantage, for both service providers and consumers, derived from a more aware involvement of customers in data collection and processing, which could ensure the delivery of a service that is more tailored to the effective needs of consumers. Also, a researcher from a think tank noted that the very business model of some companies is based on the concealed processing of information. Such a lack of transparency is also problematic because it hampers the ability to fairly balance the economic and social perspectives.

Closely related to the question of transparency is the topic of consumers' awareness and education. As stressed by a representative of a private company, the ability of consumers to understand the data processing schemes is crucial to ensure a level of trust. Another participant, from a data protection authority, underlined the role that should be played by education, as technologies are an integral part of individuals' lives. Without proper education and awareness on the effective uses of personal data, it is difficult for data subjects to exercise their rights, and thus, will require higher standards of protection. This is the reason why technologies should be conceived as privacy-friendly by default. Another option, proposed by the same participant, is to implement a 'label system', as in the case of food commercialization, which permits consumers to operate a choice between different services and systems.

6.3. On-line and off-line shopping. What are the specific challenges?

Another issue that emerged in these debates concerns the specificities of each buying environment, not only the differences between on-line and off-line shopping, but also the trend towards partial integration of these two, and the parallel segmentation of the on-line market. Participants underlined that the understanding of the developments of the market is important to both assess the emerging risks, but also to avoid overlook the different practices and techniques deployed. For example, as a researcher from a think tank pointed out, the blending of on-line and off-line shopping poses new threats that should be addressed specifically, such as the manipulation of data. On the other side, a representative from a private company stressed the growing segmentation of the Internet market, with different products and different business models currently under development, and potential transformation of the Internet intp a series of walled gardens.

6.4. Possible solutions. Which kind of regulatory processes? Which scope for Privacy Impact Assessments?

Another central topic of debate concerned the possible regulatory solutions to apply to the deployment of the techniques at stake. A participant from a private company stressed that, first of all, different levels of regulation can be envisaged, and, in particular, three key layers are the legislative, the administrative (data protection authorities' supervision) and the business one. A representative of a data protection authority also proposed to include an educational level. A member of the SAPIENT project suggested an alternative perspective, proposing to use a continuum of regulatory possibilities ranging from state regulation to self-regulation, and including possible forms of co-regulation, for example thethe use of privacy impact assessments. So far, co-regulation has been applied in the case of RFiD, implying many different actors. Still, if co-regulation does not work, the more classical form of top-down regulation should be applied. According to a representative from a consumer rights organization, self-regualtion should not be used in this field, because it does not work at all. One of the main limits of self-regulation is linked to the continuous blending of private and public information, and the combined use of multiple technologies. The challenge is then to understand what is the entire range of citizens' data that is used, and not merely focusing, one by one, on a specific technology. In a similar vein, a representative from a private firm underlined that several systems operate at the same time, and this poses the question if they have to be checked, assessed and regulated singularly or jointly to understand their effective combined impact.

The issue of more effective regulation was strictly linked, and intertwined, with the possible development of a privacy impact assessment (PIA) model. As mentioned by a member of the SAPIENT project, PIAs are currently discussed in the framework of the reform of European data protection legislation, and part of the first proposed text of the Commission. A representative from a private firm raised a series of questions concerning the ways in which PIAs will be carried on, their purposes and the best strategies to communicate them once achieved. According to a representative from another private firm, the experience of the United Kingdom data protection authority could be particularly useful, as the release of a public version of PIA became an integral part of the auditing routine of private companies, with a positive effect in terms of reduction of data loss.

As for the scope of the PIA, participants raised two issues. The first concerns the already mentioned challenge of the growing combined use of multiple technologies. As stated by a researcher from a think tank, a PIA covering different related systems should be preferred over one-system based PIA, as this model could also take into account the impact in terms of social values beyond privacy. Indeed, the second issue concerns the scope of PIAs in terms of rights and values. According to one advocate, a PIA model should also include other fundamental rights, for example the freedom of communication, as well as the clear listing of all the costs engendered by a system and their distribution. In relation to the proposal of using PIA to make the systems more transparent, a researcher from a think tank underlined the continuous debate over the possibility to make the profiling algorithm used by technologies available to the public. According to the same participant,

the Commission proposal for a new regulation has contented itself with an obligation to disclose the logic behind profiling algorithm rather than the algorithm itself.

Apart from PIAs, some participants mentioned other tools to influence the decision-making, regulatory process. According to one advocate for civil liberties, an important strategy is to closely monitor the European proposals in relevant fields to both avoid that some institutions bypass decision-making systems, and that private actors are too tempted to move somehow illegally in this very rich market. A representative from a consumer rights organization mentioned the possibilities opened by the adoption of the EU Charter of Fundamental Rights, but also highlighted the differences in the enforcement of legislation, especially for individuals, given the lack of direct access to non-national courts. According to the same participant, the possibility to start 'class actions' in this field would be a useful tool. The idea of enhancing oversight of people was shared by a representative from a private company, who also advanced the idea of a more important involvement of the Fundamental Rights Agency, possibly along the lines of the work done by the European Data Protection Supervisor. Finally, an official from a data protection authority also mentioned the role of enforcement and supervision, coupled with sanctions, so to ensure the respect of the chosen regulation.

6.5. The challenges and difficulties of stakeholders' participation

The question of the best instruments to ensure adequate regulation and effective supervision brought to the fore the issue of the asymmetrical stakeholder participation in different decision-making processes. From a practical perspective, according to two participants (from civil society organizations), not all stakeholders have the same possibility to participate in key meetings and key moments of the decision-making, and, even when they can attend, they do not have adequate resources to weight their opinions in the same way as other non-institutional actors (such private companies). This is particularly relevant when the co-regulation model is chosen. According to a member of a civil rights group, this asymmetry in terms of weight should be compensated by the role of the government, which should not play the neutral arbiter but engage on the side of citizens.

Furthermore, as mentioned by a representative from a private firm, the effective participation of civil society organizations in the decision-making process or a PIA exercise has an effect on the credibility of the assessment itself. Indeed, PIAs are often presented as 'blessed' from civil society, so that if a civil society organization was not able to fully and fairly engage, there is a risk of PIAs lacking credibility. According to a representative of a consumer rights group, it is also important to clearly decide what should be discussed in critical meetings, as the consumer groups themselves have no interest in defining company business models, but only in ensuring specific protections.

Finally, a member of the consortium highlighted what seems an important contradiction between the very idea of 'stakeholders' and fundamental rights. Fundamental rights implies a relation between citizens and the state, so there are, properly speaking, no stakeholders. To speak in terms of stakeholders risks to introduce a sort of neo-corporativism, in

which the direct relations between the citizens and the state is substituted by the actions of intermediary bodies. According to the same participant, this is not an adequate model when fundamental rights are at stake.

Marginal notes of the SAPIENT team

The majority of the stakeholders quickly ‘moved away’ from the scenario to explicitly focus on current practices and ongoing policy and legislative proposals. In the few cases in which participants referred back to the scenario, the issues introduced were again refered to current practices and controversies.

Given the topic of the scenario, most of the first session revolved around the economic and market dimension. Then, it is noteworthy that a lot of attention was dedicated to the issue of regulation and, in particular, privacy impact assessments.

All along the two sessions, discussions were particularly vivid, with strong polarizations around specific topics (eg distribution of benefits, lack of transparency in the business model of data processing).

7. Workshop on "Smart Surveillance for Border Security and Immigration Controls"

Philip Schütz (Fraunhofer ISI)

The Workshop took place at KoWi, Brussels, Belgium, 07 September 2012, 10:00 - 14:00.

This high level summary collects main themes discussed during the 3rd stakeholder workshop on “Border Security and Immigration Control” that took place on the 7th September 2012 in Brussels. Participants included representatives from the SAPIENT consortium, members of civil society organisations (CSOs), policy-makers in the field of home affairs, as well as representatives of data protection authorities (DPAs).

After a brief presentation of the scenario, in which its author explained key messages, the methodology used and the main purpose of the focus group meeting, a first session of discussion among the participants started. The intensive debate was followed by a short lunch break that introduced the second session of discussion. In the end, a wrap up of key points raised during the workshop was presented.

The following text summarises these key points raised by the experts of the focus group meeting.

7.1. Key challenges in the field of border security and immigration control

Policy-makers in the field of home affairs pointed to the increasing number of travellers as one of the main challenges in border security. Today, there are over 400 million people per year crossing borders of the EU, and in the near future it will be 700 million. In trying to guarantee mobility, providing security and controlling illegal immigration at the same time, policy-makers and border security agencies face a complex and sometimes incompatible set of tasks. Additionally, new forms of border crossings, such as on the Mediterranean Sea, make the professional and correct exercise of the tasks even more difficult.

DPA stakeholders were emphasising that a key challenge lies in how the data collected by border security providers is handled. In many instances, it is not known what kind of data, e.g. biometric data, is collected and what happens with it later on (function creep). Also the retention period as well as the number of actors who are able to access the data,

e.g. law enforcement agencies, remain often unclear. The exchange and dissemination of this data between public actors, public and private sector entities, as well as the transfer to third countries poses a threat to an effective enforcement of data protection. Eventually, a central data protection principle, i.e. purpose limitation, can often not be guaranteed.

The issue of an effective and efficient technical functioning of border security technologies was raised by CSO representatives. DPAs agreed that, for example, the percentage of false positives in an inspection of a specific technology would play an important role in the evaluation of that technology. However, it is crucial to distinguish whether the causes for false positives are bugs that can be fixed, or features that are inherent in the conceptual design of the technology. Policy-makers admitted, furthermore, that the false acceptance rates for automated border control systems at airports were relatively high, while the false rejection rates were significantly lower. The first is mainly due to a non-avoidable trade-off in practice, which is that the control of travellers can only take a reasonable amount of time, which in turn, of course, reduces the quality of control.

Another challenge that was addressed was transparency, not only concerning technological border security systems, but also regarding policies (and their development) governing these technologies. Particularly civil society does often neither know nor understand the technical processes and mechanisms behind the results produced by border security technologies.

7.2. The rule of law and its interpretation in the context of border security and immigration control

All stakeholders agreed upon the importance of complying with data protection law when applying border security and immigration control. However, it was also mentioned that the security staff would probably like to use their technologies and data to the full extent, which often conflicts with central data protection principles. Moreover, there are numerous exceptions, lacunae and a lack of an effective control over the actual compliance, when it comes to the processing of data for security purposes.

CSO participants also questioned surveillance as being a panacea or a definitive solution for providing security. They argued that the work of border security agencies such as Frontex would neither fulfil the adequacy nor the proportionality requirement, especially with regards to the constant violation of human and other fundamental rights in the Mediterranean. In some instances, Frontex would even contribute to a higher death rate of refugees on the sea, because they would take more dangerous routes in order to avoid being detected.

7.3. Privacy and other societal benefits

Despite providing airport security, i.e. the prevention of any violent acts at the airport or in any plane, there were other objectives of border control systems and security guards

mentioned, such as to prevent non-EU citizens from entering without a visa, or to stop trafficking. Thus, for example, a participant referred to some human traffickers who could be arrested due to the analysis of their passenger name record (PNR) data.

Another expert was arguing that border control technologies are increasingly legitimised on the grounds of an effective prevention of pandemic diseases, being able to not only stop and put the suspected carrier of a disease in quarantine, but also to trace the virus/bacteria back to the original source.

Most of the stakeholders shared the opinion that, beyond privacy and data protection, other crucial societal benefits such as security, mobility and health ought to be considered. However, each of these benefits has to be part of a balanced approach not dominating too much such as security in a lot of instances does.

7.4. Who is discriminated by border security technologies?

CSO representatives were pointing to the fact that refugees are often not recognised as political asylum seekers at the external borders of the EU, frequently without even checking their formal requests. After a participant started to argue that political asylum seekers are less than 1% of the total number of immigrants, he was countered by the argument that in Greece, a country with one of the highest immigration rates in the EU, only 0,1% of immigrants reaches the status of political asylum seekers, whereas Sweden acknowledged 40% of their immigrants as political refugees. CSO stakeholders were therefore concluding that differentiating between economic, political and other refugees is often a mere arbitrary act, and that new border security and immigration control technologies would discriminate especially those refugees being entitled to seek political asylum. In addition, they called attention to the often unnecessary and unjustified criminalisation of refugees, supporting criminal careers and resulting in a decrease of security in society.

The concern of social sorting at borders was expressed as well, and participants agreed on the fact that technological advances are most often accompanied by negative effects for certain groups of people. That is why border security technologies should always take the level of vulnerability of the checked traveller into account, as well as provide transparency over the technical processes that categorise people into desirable and non-desirable travellers.

7.5. Drivers of border security and immigration control

One of the experts mentioned that many of the discussed border control technologies are not from scratch, originally being developed by the defence industry. All participants agreed on the fact that these technologies are normally very expensive, and that there is an enormous interest of the producing industry to sell as much of their products as possible. So the economic driver in the field of border security is huge (hidden agenda) and the industry lobbies for a prevalent deployment of their technological systems at airports and other border areas.

In that context the issue of efficiency and effectiveness of border security technology was raised. Policy-makers critically remarked that 700 million Euros for a technology that is automatically checking travellers at airports can not be called one of the most cost efficient methods. It is furthermore unclear who is checking on the quality of these expensive technologies and their value for money.

On the one hand, the media was identified as another major driver for the set up of border security and immigration control technologies. CSO representatives spotlighted that the media has often pushed and reduced the debate on immigration towards the fear of huge waves of migrants, stealing EU citizens their jobs and contributing to higher crime rates.

On the other hand, news coverage has also contributed to a more critical public perception and sometimes even rejection of certain border control systems such as full body scanners. DPA stakeholder also brought up that people refused to travel to the US since they were forced to disclose too much personal information. One participant started to argue that negative headlines could also be seen as a corrective, triggering learning processes by producers and security service providers. However, he was countered by the argument of DPAs that scandals should better be avoided by investing in quality control, mainly for the purpose of maintaining a good reputation and a long-term trust relationship towards the end-users.

7.6. Proposed solutions

In order to deal with the challenges of increasing numbers of travellers, at airports for example, the quality of control had apparently to be reduced in order to guarantee a constant flow of passengers through the security gates. With regards to the challenge of new forms of border crossings, e.g. increasingly over the Mediterranean Sea, CSO representatives were suggesting to not only focus on control but also on protection of people trying to cross EU borders, taking Frontex up on their promise to save lives, which is in fact not more than a lip service until now.

It was also mentioned that smart immigration control technologies and procedures should be designed to recognise why people are entering a country, detecting their level of vulnerability. However, most of the participants figured that this would rather be a matter of policies governing technological systems than features of the technology itself.

Stakeholder emphasised furthermore that issues such as sustainable development cooperation with, and fair trade conditions and programs for developing countries, especially in Africa, should be taken much more seriously into account when searching for an effective long-term strategy to combat illegal immigration and related security problems. In that context, a participant pointed to the relationship between the Mexican drug war and the problem of illegal immigration in the United States.

All experts agreed on the need for more transparency not only regarding technical processes of border security technologies, but also when it comes to policies governing these technologies. It was argued that transparency presents an important driver in order to make the assessment and evaluation of these technologies more accessible to the public.

With regards to the question as to how surveillance before and after someone crosses the border should look like, DPA stakeholder recommended a privacy by design approach, installing a software that automatically erases the collected data after a certain time period.

Finally, DPA representatives discussed data protection and privacy impact assessments as a tool to provide more transparency and raise awareness among producers, service providers and end users. A border security technology should therefore not only fulfil the three classical principles of data security, namely confidentiality, integrity and availability, but should also meet the privacy requirements of unlinkability, transparency and intervenability. These principles were already discussed and successfully applied to cloud computing and ambient assisted living (AAL) projects (Rost and Bock, 2011; ULD, 2011).

Part III.

Deliverable 2.3: Consolidated analysis of stakeholder views

8. Summary of stakeholder consultation workshops

Rachel Finn (Trilateral Research & Consulting)

As part of its work on addressing the potential impacts that current and emerging smart surveillance technologies could have on privacy and other fundamental rights, the SAPIENT consortium invited stakeholders to participate in three scenario-based workshops. Invited participants included academics, policy-makers and representatives from industry (including private companies and R&D specialists), public authorities, law enforcement, data protection authorities (DPAs), civil society organisations (CSOs) and research institutions. As stated in the introduction to this deliverable, the consortium drafted three scenarios, focused on security in public spaces, border security and immigration control, and business practices such as personalised advertising. The goal of the scenarios was to trigger discussion among workshop participants in order to develop a view of when it is appropriate to deploy smart surveillance and how fundamental rights should be protected.

Each workshop generated its own distinct discussions based on the issues raised in the scenarios. However, the SAPIENT project aims to develop an understanding of over-arching issues of concern and a protection framework that can be applied to different technologies, practices and sectors. Therefore, this chapter consolidates the feedback from the individual workshops to examine these over-arching themes and solutions. In the sections that follow, we first discuss workshop participants' discussions around the drivers for the use of smart surveillance technologies, the role of the current "rule of law" including related to transparency and consent, the relative vulnerability of individuals and possibilities for resistance and finally, potential solutions to address threats to fundamental rights. Second, the diversity of participants at the workshops also enables the consortium to understand how stakeholder views are spread across different categories of stakeholders. Using this information, this chapter also identifies areas where different types of stakeholders were largely in agreement, and areas where conflicts need to be resolved.

8.1. Drivers for the use of smart surveillance technologies

A key issue of concern across all three workshops were the different drivers of the use of surveillance technologies which may impinge upon privacy. This included economic, social and political drivers.

Economic drivers include the ways in which private companies' interests are shaping security policies and the associated economic benefits. For example, one of the experts

from the border control workshop mentioned that many border control technologies are not designed from scratch, and were originally developed by the defence industry. These industrial companies are looking for new markets for their products, and the industry lobbies for a prevalent deployment of their technological systems at airports and other border areas. One benefit is that the creation of a market for these technologies fuels economic growth, and another is that surveillance technologies sometimes offer the possibility to design new products and services. In the personalised advertising workshop, a representative from industry argued that the potential benefits for consumers, such as the provision of free services, must be acknowledged. A representative from a consumer rights association also noted the need to account for the possible growing market of privacy preserving tools alongside privacy intrusive techniques. However, this question of potential economic benefits, most strongly supported by industry, generated significant controversy in the views of other stakeholders.

Political drivers included the mobilisation of political issues to encourage or support the use of surveillance technologies in public space, personalised advertising contexts and border control. For example, one participant stated that certain political circumstances would be needed to produce a situation where a police state emerges and privacy is undermined. The media often play a key role in these political mobilisations. In relation to the border control scenarios, some elements of the media have often led the debate on immigration and contributed towards the fear of huge waves of migrants appropriating EU citizens' jobs and contributing to higher crime rates. On the other hand, news coverage has also contributed to a more critical public perception and sometimes even rejection of certain border control systems such as full body scanners. A public authority representative noted that negative headlines could also be seen as a corrective, triggering a change in the way surveillance systems are developed and deployed.

Societal drivers included the need to efficiently deal with social changes. Most of the stakeholders in all three workshops, but most especially in border security, shared the opinion that, beyond privacy and data protection, there were crucial societal benefits of surveillance technologies, such as providing security, mobility and health that should be considered. Policy-makers in the field of home affairs explained that the introduction of border surveillance measures were important to guarantee mobility as well as provide security and control illegal immigration which sometimes seem to be opposing tasks. In another example, a border control workshop participant referred to some human traffickers who could be arrested due to the analysis of their passenger name record (PNR) data. An expert from a data protection authority argued that some important societal benefits of border control technologies could also be the prevention of epidemic diseases, by being able to trace carriers of a disease back to the original source. However, each of these benefits has to be part of an approach that does not undermine privacy while providing security.

8.2. Rule of law

A second key issue to emerge from the three workshops was the ways in which current laws provide protections against the over-zealous use of surveillance technologies in all

three sectors. Although some law enforcement and public authority representatives acknowledged that security providers would probably like to use technologies and data to the full extent, which would conflict with central data protection principles, all stakeholders agreed upon the importance of complying with data protection law when developing and deploying surveillance technologies. A participant with a law enforcement background reminded participants that law enforcement has to guarantee all constitutional freedoms, not just safety and security; thus data protection and other fundamental rights must also be protected by the police. Thus, surveillance operators must consider include proportionality, transparency, adequacy and data ownership. However, CSO representatives in two different workshops noted that the current legal framework in Europe allows circumstances for exceptions to the protection of privacy in the public security field. Thus, CSOs felt that the rule of law was a less strong protection than public authority and law enforcement stakeholders claimed.

In relation to the proposed Data Protection Regulation announced by the European Commission in January 2012, participants acknowledged that this would introduce a right to be forgotten. However, stakeholders supported the words of Vivian Reding that this is "a completely unfeasible right", because it cannot be enforced in the digital world, a virtual place where you can not erase digital traces. Instead, a representative of a research institution and partner in SAPIENT suggested conceptualising this right in a different way, i.e., the right to be ignored or the right to discretion. This would mean that individuals cannot erase traces but they can oblige authorities or private companies not to use the information about them, or to ignore that information. Participants from the CSO sector argued that the right to be forgotten cannot be seen on equal terms with the right to anonymity. Instead, we should be able to delete traces when possible. Thus, again CSO representatives were sceptical about the ability of the rule of law to offer adequate protections.

8.3. Transparency and consent

Participants in all three workshops identified a key failure of the current rule of law as a failure of transparency and consent. One researcher from a think tank noted in the personalised advertising workshop that the business model of some data collection and processing companies is based on the concealed processing of information. While in the border security workshop, DPA stakeholders emphasised that in many instances, people do not know what kind of data, e.g., biometric data, is collected by border control authorities and what happens to it later (function creep). Also, the data retention period and the number of actors able to access the data, e.g., law enforcement agencies, often remain unclear. The exchange and dissemination of this data between public actors, public and private sector entities, as well as the transfer to third countries poses a threat to an effective enforcement of data protection. Finally, purpose limitation, a central data protection principle, often cannot be guaranteed.

A representative of a civil society organisation raised the question of consent in that consumers often do not understand what happens to their data because of this lack of transparency. As a result, they do not have any effective possibility to refuse the collection

and processing of their data, since the only alternative is to risk being fully excluded from a set of services. In consequence, the meaning and effectiveness of consent as a data protection measure could be lost. However, a member of the SAPIENT consortium underlined the potential advantage, for both service providers and consumers, derived from a more aware involvement of customers in data collection and processing, which could ensure the delivery of a service that is more tailored to consumers' needs.

8.4. Vulnerabilities and Resistance

In terms of those who are targeted by surveillance technologies, two key issues emerged from the workshops – the use of surveillance technologies for social sorting and the potential for citizen resistance to surveillance. Participants at the border control workshop expressed concern about social sorting at borders, and agreed that technological advances are most often accompanied by negative effects for certain groups of people, e.g., refugees and irregular migrants. Thus, border security technologies should always take the level of vulnerability of the traveller into account, as well as provide transparency about the technical processes that categorise people into desirable and non-desirable travellers. In the personalised advertising workshop, a representative from a consumer rights organisation underlined the tendency of some business models to make those who do not participate in loyalty schemes pay the costs of the benefits that they offer to clients who do participate. However, a civil liberties organisation representative pointed out that the benefits of personalised advertising primarily lie with the businesses providing the service, not the consumers. Most of the business models offering free services are requesting customers' data in exchange, and are using them for profit. Finally, in the public space security workshop, a CSO representative pointed out that what is fundamentally different from the past is the focus on prevention by removing the potential "troublemakers" before the actual event. In this context, we are required to wonder what it takes to be regarded as a potential "troublemaker". Thus, civil society organisations were particularly concerned about citizens and consumers being vulnerable in the face of smart surveillance technologies.

Yet, individuals are not passive subjects of surveillance and may resist surveillance in unexpected ways. A participant in the public space surveillance workshop noted that citizens in Québec resisted a government law prohibiting assemblies in public spaces by organising mass strikes. In the same workshop, a representative of an R&D institution suggested that stakeholders should consider the sabotage effect, and try to understand how different actors may behave in this respect. Finally, in the border security workshop, a CSO representative noted that Frontex systems and operations may actually contribute to a higher death rate of refugees on the sea, because they take more dangerous routes in order to avoid being detected.

8.5. Potential solutions

In all three workshops, stakeholders proposed possible solutions to better protect privacy and other fundamental rights given the proliferation of smart surveillance technologies. For

some CSO stakeholders, this meant redefining the terms of the debate. For example, in the border security workshop, one CSO representative suggested that border security should focus on the protection of people trying to cross EU borders as well as the protection of citizens, while another argued that issues such as sustainable development co-operation and fair trade programs for developing countries should be taken more seriously when searching for an effective long-term strategy to combat illegal immigration and related security problems. However, most other stakeholders focused on possible solutions that more directly addressed the key terms of the privacy and security debate, including better enforcement of existing rules, education, privacy-by-design approaches, self-regulation and privacy impact assessments.

8.5.1. Better enforcement of existing rules

As described above, workshop participants noted that significant privacy and data protection rules already exist in current legislation to provide some protections from smart surveillance technologies. However, many stakeholders felt that these rules were not enforced strongly enough, and that better enforcement would have a positive impact on citizens' privacy. This discussion was strongest in the personalised advertising workshop, where a representative of a consumer rights organisation mentioned that the EU Charter of Fundamental Rights provides significant opportunities to protect fundamental rights, but this legislation is not well enforced and individuals lack direct access to the courts where they could challenge practices. The idea of enhancing oversight of people was shared by a representative from a private company, who also advanced the idea of a more important involvement of the Fundamental Rights Agency, possibly along the lines of the work done by the European Data Protection Supervisor. Finally, an official from a data protection authority also mentioned the role of enforcement and supervision, coupled with sanctions, to ensure respect for the chosen regulation.

Another possible solution proposed by representatives of civil society organisations was to further generalise the opt-in approach. However, private firms preferred a differentiated approach to opting-in where some spheres would require a "true" opt-in, while others used the opt-out approach. As noted by two other participants, from a data protection authority and from a civil liberties organisation, the technical design chosen by the service provider seems to influence the behaviour of people who are signing-in to new services. Finally, a member of the SAPIENT consortium noted the risk of requiring informed consent relies upon the consumers-companies relationship as its primary model. Not only does the informed consent model risk weakening people's power, rather than empowering them, it is also heavily based on the rational choice model, which has been heavily critiqued. Thus, representatives from all stakeholder categories supported better enforcement of existing regulations. However, the following, additional suggestions demonstrate that better enforcement alone will not protect individual privacy and fundamental rights.

8.5.2. Education

Consumer or citizen education emerged as a second important way to improve protections for fundamental rights. This was shared between different workshops and different

stakeholder categories. For example, in the public space workshop, a representative of a research institution argued that privacy protection depends on good communication practices with the public. Most people are not aware, and are not conscious of the concerns with respect to privacy and data protection, and this is why education is crucial. In the personalised advertising workshop, a representative of a private company stated that the ability of consumers to understand data processing schemes is crucial to ensure trust in surveillance systems. Another participant, from a data protection authority, underlined the role that education should play as technologies become further integrated into people's lives. Without a proper education and awareness of the effective uses of personal data, data subjects will have difficulty exercising their rights, and will require higher standards of protection. One option, proposed by the same participant, was to implement a label system, as in the case of food commercialisation, which permits consumers to understand their choices between different services and systems. Finally, a CSO participant felt that it was not only consumers who needed education. Rather, law enforcement and police stakeholders also needed better education about their role in protecting privacy and personal data.

8.5.3. Privacy by design

Privacy-by-design approaches were mentioned in all three workshops, and primarily supported by data protection authority stakeholders and industry representatives involved in research and development. In the border security workshop, a DPA stakeholder recommended a privacy-by-design approach for smart surveillance technologies, such as installing software that automatically erases the collected data after a certain time. In the surveillance in public spaces workshop, an R&D representative argued that because there is always a gap between the legal framework and technological progress, technology has to be included as part of the solution. Privacy enhancing technologies (PETs) and privacy-by-design principles could be implemented to assist with technological approaches to data minimisation and purpose specification. Finally, as mentioned above, a DPA participant in the personalised advertising workshop noted that opt-in or opt-out issues were important to address in the design of an information collection system.

8.5.4. Self-regulation

Self-regulation was primarily discussed in the personalised advertising workshop. Representatives of private industry were particularly keen to support self-regulatory initiatives in this workshop, although one acknowledged that regulation involved three potential layers: the legislative, the administrative (data protection authorities supervision) and the business layer. In a similar vein, a member of the SAPIENT consortium proposed an alternative perspective, using a continuum of regulatory possibilities ranging from state regulation to self-regulation, and including possible forms of co-regulation as is used for RFID systems. However, a representative from a consumer rights organisation argued that self-regulation should not be used at all, because it does not work. One of the main limits of self-regulation is linked to the continuous blending of private and public information, and the combined

use of multiple technologies. Thus, different stakeholders had significantly different views about the potential role of self-regulatory initiatives.

8.5.5. Privacy impact assessment

The co-regulatory privacy impact assessment (PIA) model was discussed in all three workshops. As mentioned by a member of the SAPIENT project in the personalised advertising workshop, PIAs are currently part of the proposed Data Protection Regulation. One industry representative expressed concern about the ways in which PIAs will be carried out, their purposes and the best strategies to communicate their results once they are undertaken. According to a representative from another private firm, the experience of the United Kingdom data protection authority could be particularly useful, as the release of a public version of PIA became an integral part of the auditing routine of private companies, with a positive effect in terms of reduction of data loss. In the border security workshop, a DPA representative also offered data protection and privacy impact assessments as a tool to provide more transparency and raise awareness among producers, service providers and end users. Technologies and systems should not only fulfil the three classical principles of data security, namely confidentiality, integrity and availability, but should also meet the privacy requirements of unlinkability, transparency and intervenability. In the public space workshop, a representative from a research institution noted that impact assessments should consider risk and the acceptable level of "collateral damage" to privacy or other fundamental rights. PIAs should also consider smart surveillance systems rather than technologies, and according to a researcher from a think tank, a PIA covering different related systems should be preferred. Another PIA advocate noted a PIA model should also include other fundamental rights, for example, freedom of communication, as well as the clear listing of all the costs engendered by a system and their distribution.

The use of PIA and other supervision mechanisms that rely upon stakeholder consultations engendered a discussion within the personalised advertising workshop about the issue of asymmetrical stakeholder participation. Two CSO participants pointed out that the availability of internal resources impacts upon an organisation's ability to participate in key meetings and key moments of decision-making. Furthermore, their lack of resources impacts upon their ability to ensure their perspective has the same weight as actors such as private companies. This is particularly relevant when a co-regulation model, such as PIA, is chosen. According to a member of a civil rights group, this asymmetry in terms of weight should be compensated by the role of the government, which should not play the neutral arbiter but engage on the side of citizens. CSO representatives also noted that PIAs are often presented as "blessed" from advocacy organisations, even if their concerns or recommendations are ignored. Therefore, if civil society organisations are not able to fully and fairly engage, there is a risk of PIAs lacking credibility. Thus, civil society organisations ought to be better supported in participating in PIAs and ensuring that their concerns are given adequate consideration by governments or private companies with significantly more resources. Thus, while data protection authorities, think tank representatives and some industry representatives welcome the introduction of measures such as PIAs, other stakeholders point out considerable issues in their implementation.

8.6. Conclusions

This analysis suggests a range of important considerations when examining over-arching concerns about smart surveillance technologies and practices as well as potential solutions. First, stakeholders acknowledged that the drivers behind the introduction of a smart surveillance technology are an important consideration when making decisions about their introduction. Although stakeholders acknowledged that the rule of law provides current protections, CSOs were particularly sceptical about the ability of these measures to provide adequate and consistent protection due to a number of exceptions and inherent weaknesses in particular measures. Specifically, participants identified two key failures in the rule of law, namely transparency and consent. Data protection authorities and CSOs were most concerned about failures in these areas, as a lack of transparency makes it difficult for consumers and citizens to practise informed consent. Representatives of civil society organisations, including human rights organisations and consumer organisations, were particularly concerned that smart surveillance makes certain categories of people vulnerable, while a range of stakeholders also noted that individuals were not passive subjects of surveillance and may find ways to sabotage or otherwise resist surveillance.

Given these potential issues, stakeholders identified five different ways in which privacy and other fundamental rights might be better protected in relation to smart surveillance technologies and practices. All stakeholders supported a better enforcement of existing rules and regulations; however, as noted above, this alone is not sufficient to guarantee protections. Industry, DPA and CSO representatives all argued that consumers and authorities needed better education about data practices as well as their rights and responsibilities. Data protection authorities and industry representatives, particularly those involved in research and development, supported privacy-by-design measures to enhance privacy, including safeguards regarding the deletion of data when it is no longer necessary. Industry representatives were also likely to support self-regulatory mechanisms, although this was challenged as ineffective and inadequate by CSO representatives. Finally, many stakeholders supported the use of a co-regulatory mechanism such as an enhanced privacy impact assessment, or a surveillance impact assessment, that increased transparency and addressed other fundamental rights in addition to privacy. However, CSOs cautioned that such co-regulatory mechanisms often favoured organisations, like industry, with significant resources and made it difficult for under-funded organisations to participate equally. Inequality between stakeholders should be addressed, for example, either by the government supporting CSO positions or CSO participation.

9. References

Canetti, Elias (1960). *Masse und Macht*. Hamburg: Claasen.

De Hert, Paul (2012). “A Human Rights Perspective on Privacy and Data Protection Impact Assessments”. In: *Privacy Impact Assessment*. Ed. by David Wright and Paul De Hert. Vol. 6. Law, Governance and Technology. Dordrecht: Springer, pp. 33–76.

Dürrenberger, Gregor et al. (1997). *Focus Groups in Integrated Assessment: A manual for a participatory tool*. ULYSSES Working Paper 97-2. Darmstadt: Darmstadt University of Technology, Center for Interdisciplinary Studies in Technology. URL: `http://www.jvds.nl/ulysses/eWP97-2.pdf`.

Georghiou, Luke et al., eds. (2008). *The Handbook Of Technology Foresight: Concepts and Practice*. PRIME Series on Research and Innovation Policy. Cheltenham: Edward Elgar.

Godet, Michel (2000). “The art of scenario and strategic planning: Tools and pitfalls”. In: *Technological Forecasting and Social Change* 65.1, pp. 3–22.

Gutwirth, Serge et al. (2012). *Smart Surveillance - State of the Art Report*. Deliverable 1. SAPIENT project. URL: `http://www.sapient-project.eu`.

Johnston, Ian (2011). “EU funding ’Orwellian’ artificial intelligence plan to monitor public for ’abnormal behaviour’”. In: *The Telegraph* (19 September 2011). URL: `http://www.telegraph.co.uk/news/uknews/6210255/EU-funding-Orwellian-artificial-intelligence-plan-to-monitor-public-for-abnormal-behaviour.html`.

Masini, Barbieri and J. Medina Vasquez (2000). “Scenarios as seen from a human and social perspective”. In: *Technological Forecasting and Social Change* 65.1, pp. 49–66.

Ringland, Gill (1998). *Scenario Planning: Managing for the Future*. Chichester: Wiley.

Rost, Martin and Kirsten Bock (2011). “Privacy by Design und die Neuen Schutzziele: Grundsätze, Ziele und Anforderungen”. In: *DuD - Datenschutz und Datensicherheit* 35.1, pp. 30–35.

Slocum, Nikki, Stef Steyaert, and Robby Berloznik (2006). *Participatory Methods Toolkit: A practitioner’s manual*. Brussels: King Baudouin Foundation.

ULD (2011). *Juristische Fragen im Bereich altersgerechter Assistenzsysteme*. Vorstudie im Auftrag von VDI/VDE Innovation + Technik GmbH. ULD Unabhängiges Datenschutz-Zentrum Schleswig-Holstein.

Wright, George and George Cairns (2011). *Scenario Thinking: Practical Approaches to the Future*. Basingstoke and New York: Palgrave Macmillan.

A. Participants of the stakeholder workshops

1. AK Vorratsdatenspeicherung, Germany
2. AK Vorrat International, Hungary
3. Atos, Spain
4. Digitale Gesellschaft, Germany
5. Dutch Ministry of the Interior and Kingdom Relations, The Netherlands
6. Dutch National Police Agency, The Netherlands
7. European Data Protection Supervisor (EDPS)
8. Europol
9. FOI Swedish Defence Research Agency
10. Google, United Kingdom
11. HW Communications, United Kingdom
12. Information Commissioner’s Office (ICO), United Kingdom
13. Innocentive, United Kingdom
14. Leeds University, United Kingdom
15. Panoptykon Foundation, Poland
16. Platform for International Cooperation on Undocumented Migrants (PICUM), Belgium
17. Inspectorate for Personal Data Protection, Slovenia
18. TNO, The Netherlands
19. Verbraucherzentrale Bundesverband, Germany
20. Unabhängiges Landes-Datenschutzzentrum Schleswig-Holstein (ULD), Germany
21. University of Amsterdam, The Netherlands
22. University of Kent, United Kingdom

B. Discussion points for the stakeholder workshops

Target: Identify what different stakeholders desire from the technology or what they fear. What are the requirements, what are the concerns?

Question 1 (Associations, before presentation of the scenario): Spontaneous associations with topic (short)

Question 2 (Comprehension, after the presentation of the scenario): Is there something that surprised you or that you find remarkable?

Question 3 (Positive Impact): What is perceived as positive, useful aspects of the technology?

- What are the criteria to define any possible positive impact? And, how can the positive impact be measured or compared to a previous situation?
- What other possible positive spill-over effects that do not emerge explicitly from the scenario?
- To what extend these positive features risk to jeopardize other important elements (rights, societal practices, security practices, etc.)?
- Which stakeholders categories are particularly in the position to take advantage from these positive impacts?

Question 4 (Negative Impact): What are negative developments, what are your concerns?

- What are the criteria to define any possible negative impact? And, how can the negative impact be measured or compared to a previous situation?
- Are the possible negative effects the resultant of the direct application of a new technology, or rather the way in which specific technologies are connected to other elements and practices? (Can you provide an example of both cases?)
- Which rights/values are particularly at stake in your opinion?
- To what extend and under which circumstances is the use of the technology acceptable? What are borderlines?
- Which stakeholders categories are particularly suffering from these negative impacts?

Question 5 (assessment): What is a desirable decision-making process, and who should be responsible for what?

- Are all the most relevant stakeholders present in the scenario? Who is missing (beyond the more classical institutions of political representativity), or who should be included?
- Is the described relationship between different stakeholders reflecting the real power relations?
- In particular, which specific aspects and (socio-)technological features should deserve specific attention in the decision-making process?
- How can a decision-making process be designed so to retain overview of the progressive deployment of these technologies? Is this necessary for specific technologies, or for all types of technologies?
- What is the added value of a preliminary (ethical/privacy) impact assessment? How can it effectively support the decision making process and contribute to mitigate the negative impacts?