FP7-SEC-2011-284725

SURVEILLE

Surveillance: Ethical Issues, Legal Limitations, and Efficiency
Collaborative Project

SURVEILLE Deliverable 3.3b Report on system effectiveness, efficiency and satisfaction assessment; Data Protection

Due date of deliverable: 30.09.2013
Actual submission date: 5.10.2013

Start date of project: 1.2.2012 Duration: 39 months

SURVEILLE WP 3: Dr. Coen van Gulijk, TU Delft

Author(s):
Erik Krempel, Fraunhofer IOSB
Dr. Coen van Gulijk ,TU Delft

1 Table of Contents

2 Position of the report in SURVEILLE

This report is entitled 'D3.3 b: Report on system effectiveness, efficiency and satisfaction assessment; Data Protection' and it is a deliverable in work package 3 of the SURVEILLE project. It contributes to the following objectives of work package 3:

O3.1 To assess the benefits and costs of surveillance technology. (By 'benefits' we mean the delivery of improved security; by 'costs' economic costs, negative public perceptions, negative effects on behaviour, and infringement of fundamental rights.) (project objective O2)

O3.2 To produce proposals for improving the effectiveness of security surveillance, while taking fully into account perceptions, economic costs, legal limitations and ethical issues.

With regard to O3.1 this report focuses on the delivery of data protection assessment. With regard to O3.2 it focuses on improving effectiveness by reducing the possible privacy impact of a surveillance task.

Note that other parts of these objectives are met in deliverables that are produced almost simultaneously with this report. They are:

D3.2: European level study on perceptions, including an overview of effects and side-effects of surveillance and their perceived effectiveness.

D3.3 (or D3.3a): Report on system effectiveness, efficiency and satisfaction assessment; User Satisfaction. The current report complements originally planned deliverable D3.3.

D3.4: Design of research methodology for assessing the effectiveness of selected surveillance systems

D3.5 Cost model for surveillance techniques.

These reports (and this work) focus on collecting prior knowledge in different fields (perception, financial cost, satisfaction, efficiency and effectiveness). The authors suggest reading those reports alongside this report because they demonstrate how difficult technology assessment is.

Further developments for surveillance technology assessment requires design decisions for the research apparatus that have to be based on these reports and on a discussion with all SURVEILLE partners.

3 Introduction

The SURVEILLE project systematically analyses the impact of surveillance technology for the pursuit of organized and serious crime from various positions. In contrast to many approaches focussing on one or few areas of expertise, SURVEILLE brings together social sciences, law, ethics, data security, human factor scientists and end users into a multidisciplinary research consortium. The SURVEILLE partners with a technical background make a survey in surveillance technologies (D2.3). These collected technologies then are rated from the different scientist in their field of expertise. Based on the results the overall goal of SURVEILLE is to enable an educated choice between different surveillance technologies considering the needs of stakeholders like law enforcement as well as social, legal and ethical requirements.

3.1 Taxonomy and scope

In the following document the terms privacy and data protection will be used multiple times. In a technological context the term data protection could mean the protection of collected data against corruption, unauthorized access and unintended deletion. In this context it is of no importance whether the data includes private information or the weather forecast from last month. In a legal context the same term 'data protection' is

often used as a shorthand expression for *the fundamental right of the protection of personal data* [1]which includes all kinds of data related to a person. The term privacy in a legal context would refer to one important dimension of the *fundamental right to respect for one's private and family life, home and communications*[2].
For the rest of this document we will use the term data protection as follows. The term data protection is used to describe how a given system protects data, against corruption, unauthorized access and unintended deletion. That includes features related to the collection, the processing and the access to the data. It will not include assessment whether the collection or processing of data is according to legal regulations.. As we rate the data protection of surveillance technologies it is unavoidably related the fundamental rights of the right to privacy and the right to the protection of personal data in their legal meaning. When we speak of a high privacy risk or a high privacy impact we want to point out that the measures of technical data protection are not sufficient.
The goal of this deliverable is to have a more detailed look at the Privacy by Design scores included in the technology assessment for deliverable D2.6 of SURVEILLE. It is not meant to replace or redo that work, but aims to achieve a broader understanding of how to rate the technical dimensions of data protection in surveillance technology.

4 System efficiency in the scope of data protection

The question how to rate if a surveillance system is effective and efficient gets analysed in detail in SURVEILLE deliverable D3.4.
When considering not only financial cost, but the overall cost for a society, privacy is an important factor. Most, if not all existing surveillance systems have a negative impact on privacy. Therefore it is not sufficient to asses if privacy is affected by a certain measure. To get meaningful results multiple dimensions of data protection and privacy impact, such as but not limited to, type of data acquisition, privacy impact and data processing, have to be measured.

4.1 Methods of privacy risk assessments

To measure the costs in term of privacy it is important to assess what privacy related data is processed by the system and which levels of data protection are in place.

Risk assessment and management are widely used methods in the field of IT to assess which risks are inherent in a project and which measures are in place to handle those risks. A risk is an event that, if the event occurs, has a negative impact on money, reputation or in the worst case health and life of people. The three most important standards for risk management are the baseline security standard[3] by the German Federal Office for Information Security (BSI), ISO 27005 by the International

[1] See, Article 8 of the EU Charter of Fundamental Rights, http://www.eucharter.org/home.php?page_id=15
[2] See, Article 7 of the EU Charter of Fundamental Rights, http://www.eucharter.org/home.php?page_id=14. It should also be noted that one of the main human rights treaties, the International Covenant on Civil and Political Rights uses, in its Article 17, explicitly the term "privacy" (instead of "private life").
[3] Bundesamt für Sicherheit in der Informationstechnik. BSI-Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz, Mai, 2008.

Standardisation Office (ISO)[4] and NIST 800-30 by the National Institute of Standards and Technology (NIST)[5] . As an example for a risk management system the ISO 27005, displayed in Figure 1, was chosen.

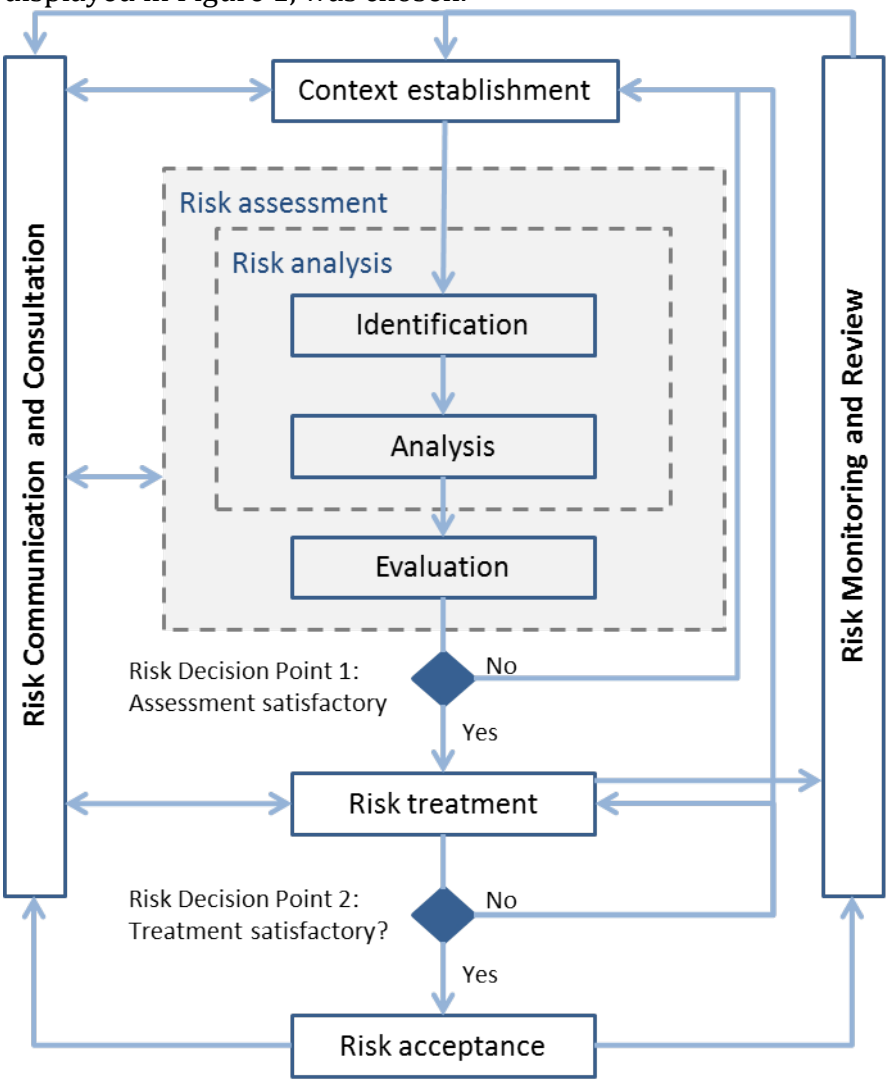


Figure 1: Risk management by ISO 27005

In the phase of context establishment, the different risks together with their probability of occurrence and the expected damage are listed. In the risk assessment phase the different risks are analysed and prioritised according to their importance. In the risk treatment phase it is decided how and if the risks are handled. It is important to state, that not every risk has to be handled by concrete measures. If an organisation comes to the result that the probability and estimated damage of a risk do not justify costly processes, a risk can stay unhandled.

4.2 Privacy risk assessments

Similar to risk management systems, specialised systems to assess data protection exist. Most of the time they are called privacy risk assessments, or privacy impact

[4] ISO/IEC. Information technology - Security techniques. Information security risk management (ISO/IEC 27005), June, 2008.

[5] National Institute of Standards and Technology. Guide for Applying the Risk Management Framework to Federal Information Systems (NIST SP 800-37), February, 2010

assessments, less common is the name data protection impact assessment. In this work we will use the name privacy impact assessment (PIA) from now on.
Unfortunately there are many concurrent PIA methods and so far none of them has become a standard. Table 1 tries to give an overview over the existing methods in different states and for what application they were designed for.

State	Title	Application
Germany	Privacy Impact Assessment Guideline (2011)	RFID, national
France	Methodology for Privacy Risk Management (2012)	National
UK	Privacy Impact Assessment Handbook (2009)	National
UK	Undertaking Privacy Impact Assessments (2010)	National
Ireland	Guidance on Privacy Impact Assessment in Health and Social Care (2010)	Health sector, national
EU	Privacy and Data Protection Impact Assessment (2011)	RFID, international
EU	A step-by-step guide to Privacy Impact Assessment(2012)	international
Canada	Privacy Impact Assessment: A User's Guide (2001)	State of Ontario, subnational
Canada	Core privacy impact assessment (2010)	Federal Agencies, national
Canada	Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada (2011)	Federal Agencies, national
USA	Managing Information Privacy and Security in Healthcare: Privacy Impact Assessment Guide (2001)	Health sector, national
USA	Privacy Impact Assessments: The Privacy Office Official Guidance (2010)	Privacy Office, subnational
USA	Guide to Implementing Privacy (2010)	Homeland Security, subnational
USA	Ohio Privacy Impact Statements and Assessments (2013)	State of Ohio, subnational
Australia	Privacy Impact Assessments - A guide for the Victorian public sector (2009)	State of Victoria, subnational
Australia	Data Matching In the Public Interest (2009)	Data matching, subnational
Australia	Privacy Impact Assessment Guide (2010)	national
New Zealand	Privacy Impact Assessment Handbook (2007)	national
Hong Kong	Privacy Impact Assessments (2010)	subnational

Table 1: Selected systems for privacy risk assessments

At the moment the Information Privacy Impact Assessment Handbook[6] by the British data protection agency ICO is handled as the best practice guideline[7]. Therefore it is introduced here as an example, as well as the Privacy Impact Assessment Framework by the EU.

4.2.1 Privacy Impact Assessment by ICO

The basic steps for performing a PIA according to the ICO rules are similar to a risk assessment and illustrated in Figure 2: StepsFigure 2. The method offers a general approach useable for all kinds of technology.

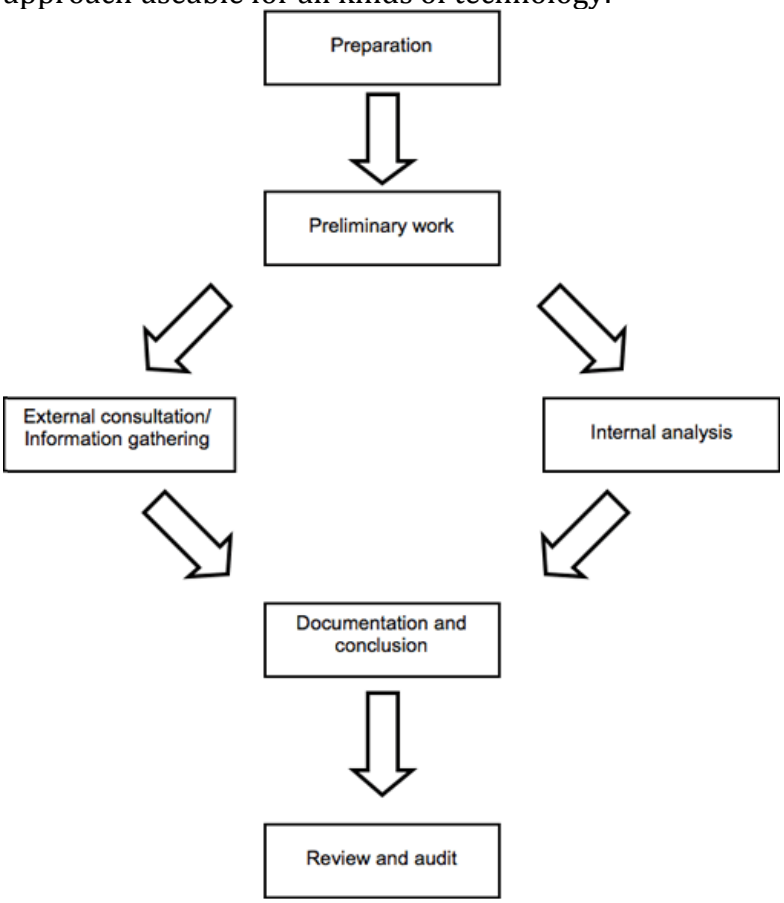


Figure 2: Steps of a PIA (ICO)

Screening

Before the actual PIA process starts, screening questions are used to decide which level of assessment should be done. The results could either be to perform a Full-Scale PIA, a Small-Scale PIA or an analysis of data protection laws.

Preparation

After the initial screening is done, the real PIA gets prepared where important project parameters are collected. Which are the important stakeholders and does the project have enough manpower to perform the PIA effectively and efficiently?

---

[6] Information Commissioner's Office (UK). Privacy Impact Assessment Handbook, June, 2009.

[7] M. C. Oetzel und S. Spiekermann. Privacy-by-Design through Systematic Privacy Impact Assessment - a Design Science Approach. In 20th European Conference on Information Systems, June, 2012, S. 160.

Preliminary work

This phase is used to establish a communication strategy and a PIA consultant group (PCG). The PCG consists of representatives of all important stakeholders of the project and enables them to influence the further project.

Consulting / Internal analysis

The consulting and analysis should be performed in parallel to the project development. Next to regular consulting with the PCG risks and problems should be identified. These should be worked on to find solutions early and integrate them into the design of the project. Therefore a register is created that collects problem descriptions, measures to mitigate or solve them as well as changes to the design.

Documentation and conclusion

In this step the results are documented and a PIA report is written and published to the PCG. In certain cases the result can be published to a wider group of people or be open to the public. The report consists of a description of the project, a collection of all data protection and privacy risks as well as the measures established to handle them.

Review and audit

Even after the PIA is completed it has to be ensured that the measures are effective and efficient. Therefore reviews are recommended not only at the end of a project but also during and at the end of the design phase.

4.2.2 Privacy Impact Assessment Framework by the EU

The PIAF[8] project (A Privacy Impact Assessment Framework for data protection and privacy rights) is a European research group founded in 2010. The goal is to develop a Privacy Risk Assessment framework for the EU on the basis of existing documents. PIAF does not define a concrete process on how to handle a PIA but rather shows how a framework for a company or technology should be created[9].

PIA as on-going process

The PIA must be an on-going process that is carried out over the full lifecycle of a project and not just one time to create a report.

Scalability

A PIA policy should allow a company to carry out a PIA appropriate to their own circumstances and needs.

All privacy types

A PIA should consider all sorts of privacy, not only data protection but also private life, private communication and privacy of the family.

Accountability

An organization should be able to prove that they carried out a PIA and handled privacy risk in an effective and efficient way.

Transparency

[8] http://www.piafproject.eu

[9] http://www.piafproject.eu/ref/PIAF_D3_final.pdf

A PIA should enjoy at least a minimal level of transparency. The assessor as well as all the stakeholders should get all information needed to understand the data protection results of the process. Only information that itself is critical should be kept secret.

Risk management and legal compliance check

Risk management and a legal compliance check are vital for the success of a PIA. Ideally a company already has processes to check for legal compliance of product, if not those processes have to be established.

Audit and review

To guarantee that the PIA is correct and complete, an external expert should perform a final audit and review.

4.3 Evaluation of PIA for surveillance technology

Privacy Impact Assessments are a powerful tool to describe, rate and improve the privacy protection of data processing systems. Many different approaches exist that all have a common process. First the system is described in detail to identify all relevant data flows. Those flows get rated by the change that data is lost and the possible harm resulting in the data loss. After that step the PIA process tries to solve or mitigate risk for the privacy. While this process is although possible and desirable for surveillance system two main requirements are not fulfilled. First PIAs are designed to rate specific implementations of a technology but not a technology concept. Second the PIA process itself is too time and resource demanding to be performed for a broad variety of technologies.

Therefore we decided to not use an existing PIA concept for the assessment but look for an alternative that will yield useful results for the project partners in the given time schedule.

5 Privacy by Design and surveillance technology

The assessment of available PIAs showed that a rating of the effectiveness relating to aspects of data protection is not feasible using PIA, as the process itself is too time consuming and has to be done for a complete system rather than components. As the final goal of SURVEILLE is to provide a decision which surveillance technology should be used for a given scenario, another approach of rating and improving privacy impact was developed.

PbD Privacy by Design[10] by Ann Cavoukian is a well-known concept for creating technology that has the least amount of impact on the users' privacy. PbD has 7 foundational principles that have to be fulfilled by a technology.

1. Proactive not Reactive
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality – Positive Sum, not Zero-Sum
5. End-to-End Security
6. Visibility and Transparency

[10] Cavoukian, Ann. "Privacy by design." *Take the Challenge. Information and Privacy Commissioner of Ontario, Canada* (2009).

7. Respect for User Privacy

This seems to be a good basis for a data protection assessment but in terms of surveillance some problems occur. First of all, PbD is meant to rate and improve technology that has a minimal impact on the users' privacy. In the case of surveillance the scope of the analysis is not the user, i.e., a police officer but the people under video surveillance.
Another problem occurs with the 4th principle. Full Functionality – Positive Sum, not Zero-Sum. The full principle states as follows:

"Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.[11]"

The application of this principle seems to be problematic, as in a surveillance system we have to intrude the privacy of a subject to enable law enforcements to collect evidence when needed. Therefore privacy and functionality is possible at the same time. In a newer document [12] Ann Cavoukian gives an example of what is meant by this statement. Although a privacy impact is needed, the technology must protect the privacy of all people at all times unless when needed for the functionality. A good example would be a video surveillance system that deploys a special Privacy Enhancing Technology (PET) to encrypt the video stream. The video stream is encrypted in a way that the scenery is recognizable, but the persons in the stream are encrypted and therefore cannot be identified. Only when law enforcement has evidence that a person in the stream committed a crime, e.g., there is violence, a judge can release the cryptographic key used to encrypt the persons.

5.1 Enhancing Privacy by Design from a Developer's Perspective

Before the newer work of Ann Cavoukian was available we published two papers analysing PbD and what it means for surveillance technology. In a short Paper[13] "How Is Positive-Sum Privacy Feasible?" at the Future Security Conference in 2012 we especially looked at the 4th principle (Full Functionality – Positive Sum, not Zero-Sum) that addresses the compatibility of privacy and functionality. In a second more detailed paper "Enhancing Privacy by Design from a Developer's Perspective"[14] we looked at all the 7 principles and explained them in a more developer friendly way.
It is important to state, that our work is not concurrent work to PbD by Ann Cavoukian but an extension that tries to clarify remaining questions.

---

[11] Cavoukian, Ann. "Privacy by design: The 7 foundational principles." *Office of the Information and Privacy Commissioner* (2011).

[12] Cavoukian, Ann. "Surveillance, Then and now: Securing Privacy in Public Spaces." (2013).

[13] Bier, C., Birnstill, P., Krempel, E., Vagts, H., & Beyerer, J. (2012). How Is Positive-Sum Privacy Feasible?. In *Future Security* (pp. 265-268). Springer Berlin Heidelberg.

[14] Bier, C., Birnstill, P., Krempel, E., Vagts, H., & Beyerer, J. (2012). Enhancing Privacy by Design from a Developer's Perspective. In 1st Annual Privacy Forum.

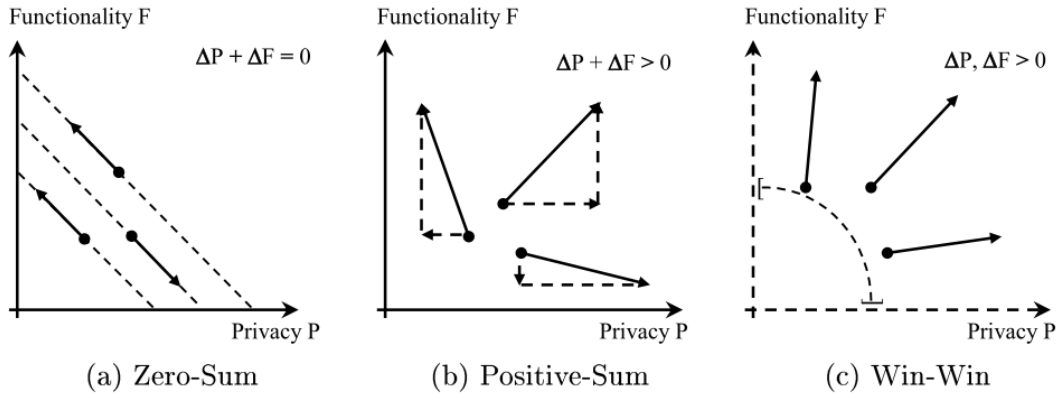


Figure 3: Comparing zero-sum, positive-sum and win-win

Figure 3 illustrates the three different concepts from game theory needed for understanding Cavoukian's definition as well as the revised version done by us. Depending on a starting point (dots in Figure 3), functionality F and privacy P can evolve. Changes are denoted with ΔP and ΔF respectively.

- Zero-sum: A concept in the field of game theory in which the sum of the outcomes is equal to zero (cf. Figure 3 a), i.e., a positive ΔP results in a negative ΔF with the same quantity and vice versa.
- Positive-sum: A concept in the field of game theory in which the sum of the outcomes is greater zero (cf. Figure 3 b), i.e., either ΔP or ΔF can be negative, but the sum is positive.
- Win-win: A special case of a positive-sum game where it is necessary that every participant has an outcome greater zero, i.e., privacy and functionality increases (cf. Figure 3 c).

We argue that, while the win-win is the best case and should be intended in a development process, especially for surveillance technology positive-sum should be allowed. This allows for a legitimate privacy invasion to achieve needed functionality. Generally speaking, there have to be trade-offs between functionality and privacy in some cases. In order to assess whether a new design results in a win-win, positive-sum or zero-sum situation, the degrees of privacy and functionality have to be measured. For this, privacy and functionality requirements have to be prioritized and weighed against each other. After determining to which fraction the requirements are actually fulfilled by a given design, the weighted sums over the fractions of privacy and functionality fulfilment can be calculated. With the approach applied in D2.6 SURVEILLE enables end users to rate the privacy and efficiency of a given system.
A design process does not necessarily start from scratch, i.e., privacy invasive features are often created by adding new functionality to an existing system.
Thus, the new definition also has to be applicable as a guideline for the evolution of a system.

Positive-Sum Privacy

Positive-Sum Privacy consists of a starting point (cf. Figure 3 b), an evolutionary step and an assessment of the method:

- Starting point of a comparative evaluation is an outdated predecessor with less than full functionality and less than full privacy, both greater than zero.
- In an evolutionary step, a change in the privacy score or functionality score is acceptable if and only if it results in a positive-sum of functionality and privacy.

- The positive-sum has to be clear and not based on biased evaluation methods. If there is reasonable doubt, Positive-Sum Privacy is not fulfilled.

It must be stressed that PbD cannot assure that a system is not privacy invasive. When adhering to all seven principles of PbD, however, one can come up with a design that is as little privacy invasive as possible given the purpose of the system. As a consequence, particularly for a system whose purpose is intrinsically privacy invasive, it makes perfect sense to establish a PbD compliant design process.

5.2 Example Positive-Sum for intelligent video surveillance

As starting point for this example assume an airport being monitored using a conventional video surveillance system, which is supposed to be replaced for efficiency reasons. The purpose of the video surveillance system is to observe critical infrastructures of the airport, i.e., regions of the airport that must not be accessed by unauthorized persons. The system is also used for manual tracking of intruders, thus its cameras do already cover the airport to a great extent. The security personnel are faced by a large number of live video screens.
Video surveillance is often criticized as an unselective measure putting people under general suspicion, i.e., a very high privacy impact is inherent to video surveillance. Nevertheless, modernizing video surveillance due to efficiency needs is an opportunity for carrying out a PbD compliant redesign.
The new system shall enable security personnel to observe critical regions more efficiently, i.e., intrusions have to be detected autonomously, so that an operator can concentrate on handling incidents. In the default setting the system performs rather non-invasive intrusion detection. Person detector algorithms are only running on specific cameras that cover critical regions and the cameras' video streams are not shown to the operator. Thus, no personal data is stored. If and only if an intruder is detected; the system is put into alert mode, which enables logging of the operator's interactions and tracking of the intruder.
By this means, system functionality is separated into a less privacy-invasive default operational mode, i.e., intrusion detection for critical regions, and a highly invasive alert mode, i.e., tracking or locating of intruders.

This design is compliant to Positive-Sum Privacy as in total the system is less privacy invasive. Only in certain cases in highly selective situations there is a legitimate interference with privacy for valuable functionality.

5.3 Evaluation of PbD for surveillance technology assessment

PbD has huge potential to develop new and to redesign existing technology to reduce privacy impact. Unfortunately it is not useable to rate existing technologies for its privacy impact. One of the most important criteria in PbD is the consent of the data subject, its control over the data as well as the transparency of the data collection. While it is important to search the content of the data subjects in classical ICT, in surveillance this is not the case. Therefore we argue that PbD cannot be used to rate surveillance technology but could be used to improve existing systems.

6 Measuring Data Protection

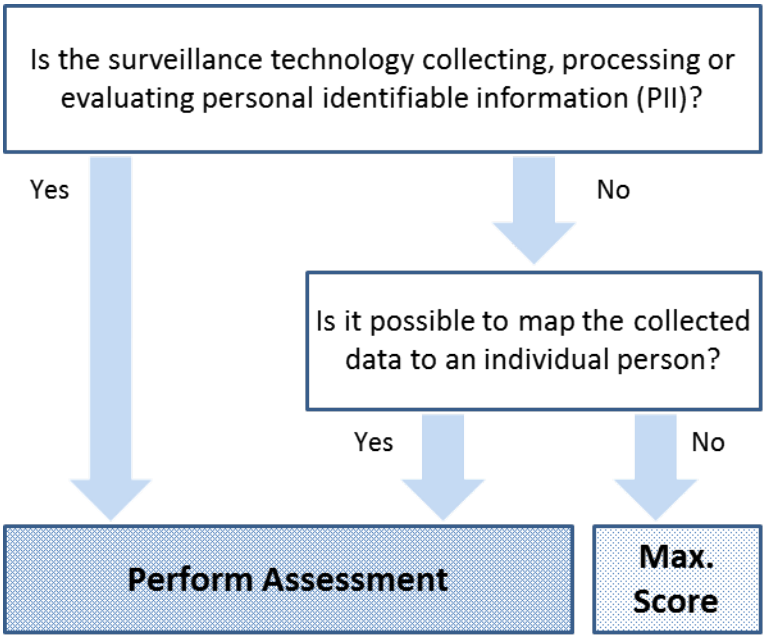
The new develop rating scale was designed to get a quick overview of privacy impact of existing technology. The analysis itself is not as detailed as performing a PIA (compare

chapter 4.2) but much faster and feasible for small groups or single persons. Compared with a PbD based analysis it is able to rate privacy risk, but not able to mitigate or solve them.

6.1 Pre-Assessment screening

Before the assessment starts an initial screening visualized in Figure 4 that is similar to a PIA screening (cp. 4.2) is done. This enables to skip the assessment when no personal information is collected or processed by the surveillance technology. In that case a technology gets the maximum score. The screening has two parts.

Figure 4: Pre-Assessment screening



First it is checked if a technology collects or processes or evaluates any personal identifiable information (PII). This includes any information that can be mapped to an individual person such as a name, a picture or a biometric template. When this is the case a full assessment has to be done. The second step asks if the data can be mapped to an individual person. This is important because certain technology could have a negative privacy impact while not directly processing PII. A good example is an AIS ship detection and localisation device. By itself it does not process PII, but when a ship is tracked and the people on board are known the collected data can be used to track the movement of individual persons. When the response to both questions is negative, a technology gets the maximum score.

6.2 Assessment questions

The scoring is done by answering multiple questions about a technology and its processing of data. The questions are selected elements from different privacy risk assessment and data protection assessment catalogues[15,16] described in 4.1. Every question is assigned with a score as well with a weight how important the criteria are. The assessment questions are separated into three different categories.

---

[15] T. B. of Canada Secretariat. Directive on Privacy Impact Assessment. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=18308

16 Commission Nationale de l'Informatique et des Libert´es. Measures for the Privacy Risk Treatment, Juni, 2012

6.2.1 Data collection

The assessment questions concerning with the topic of data collection shown in Table 2; important factors are the selectivity of the collection, data minimisation and transparency.

Q. No.	Question	Scoring range	Weight
C1	Is the collection of data selective?	0 = no, all person are affected; 1 = some selectivity ; 2 = only subject(s) are recorded	3
C2	Is the amount of collected data from the subject minimized?	0 = no 1 = yes, only needed data is collected	1
C3	Is the collection done overtly or covertly?	0 = covertly 1 = overtly	1

Table 2: Data collection

6.2.1.1 Category details

In terms of data collection the most important aspect is the selectivity of the surveillance measure. This is of course only valid, if we can assume that the selectivity is based on legitimate criteria. In an ideal case only the subject or subjects should be under surveillance. This is the case for a cell phone location tracking when the current position of a subject is collected. Even when many other people are around the subject their privacy is not affected. If the same cell phone tracking would be used to track all people in a certain area, this would be a non-selective use of the technology and would result in a bad scoring. Video surveillance is a technology for a surveillance measure that is not selective. The installed cameras will record every person in the area under video surveillance, but only when they enter such an area. No points are given for systems like the internet data retention where the internet history of every person is collected.
Data minimization concerns only the collected data of the subjects in the focus of the video surveillance not the selectivity. A system with high scoring, i.e., a cell phone location tracking, only collects the data of interest. Systems that collect data that is not needed score zero points here.
While it is not always feasible to collect data in a transparent way i.e. a covert observation will never be transparent for the subject, transparency of surveillance measures has a big impact on the scoring.

6.2.2 Data access and use

The assessment questions shown in Table 3 handle the topic of data access and use; important factors are the access control to the data and how data is protected against unlawful processing.

Q. No.	Question	Scoring range	Weight
A1	Who has access to the data?	0 = open access to data 1 = access is limited to reasonable stakeholders	2
A2	Is there a clear regulation who is allowed access under which circumstances?	0 = no 1 = organisational regulation exists 2 = regulation is enforced	1

		by technical measures	
A3	Is there a protection against function creep?	0 = no 1 = yes	3

Table 3: Data access and use

6.2.2.1 *Category details*

The first question is who has access to collected data. When collected data is accessible for a broad variety of people the surveillance measure has a strong negative privacy impact. This could be the case when the evaluation of a CCTV system becomes crowdsourced[17].
Even when data is processed by defined stakeholder the question remains how access to the data is regulated. In the best case there is a regulation on who is allowed to process the collected data that is enforced by technical measures. In a less strict version this regulation exists but is only guaranteed by an organisational measure.
A protection against function creep, i.e., collecting data for a defined purpose and processing is for another one, should have high priority for data protection.

6.2.3 Data protection

The assessment questions concerning the topic of data protection are shown in Table 4; important factors are the protection against theft and manipulation of data.
This category, while extremely important for the assessment cannot be rated for a technology in general but has to be evaluated for every concrete implementation of a surveillance technology. Therefore we performed the assessments in the Annex based on our experience how those systems are typically implemented. These ratings should be taken as examples and not as ratings of the technology in general.

Q. No.	Question	Scoring range	Weight
P1	Is the collected data encrypted or otherwise access protected?	0 = no access restrictions 1 = yes encryption or other access control in place	1
P2	Is the data protected against manipulation?	0 = no 1 = protected against external manipulation 2 = protected against external an internal manipulation	2
P3	Is the collection device secure against data theft?	0 = no 1 = yes or not applicable	1

Table 4: Data protection

6.2.3.1 *Category details*

When storing data some important questions about data protection have to been answered. As data from surveillance systems are critical to privacy the data should be encrypted or otherwise protected against unauthorised access.
Measures should be in place to protect the data against internal attackers, i.e. malicious employees, and external attackers, i.e., targeted attack against material that could become evidence.

[17] Burkhard Schafer. Crowdsourcing and cloudsourcing CCTV surveillance. In DuD, July, 2013.

When deploying mobile technology, like an audio bug or a hidden camera, that stores the data internal, this storage should be protected against attackers that try to extract the data.

6.3 Assessment result

In the next chapter we will give an overview over the assessment of different surveillance technologies mentioned in the MerPOL scenario that are also analysed in SURVEILLE deliverable D2.6. This was done as an example to demonstrate how to use the assessment tool not as an exhaustive assessment of every surveillance technology imaginable. The goal was to enable further analysis by the technology developers or for decision makers in law enforcement agencies.

6.3.1 Overview

Table 5 gives an overview of the assessment results. The different surveillance technologies and their weighted score in the different assessment questions are shown. For example the weighted score for data collection question 1 (SC1) = score (C1) x weight score (WC1). The last column of the table gives the sum of all weighted scores. When it was impossible to answer one or more questions in the assessment, no sum is given.

Technology	SC 1	SC 2	SC 3	SA 1	SA 2	SA 3	SP 1	SP 2	SP 3	∑
Closed-circuit television (CCTV); Public place – used overtly	3	0	1	2	1	0	1	2	1	11
Closed-circuit television (CCTV); Public place – used covertly	3	0	0	2	1	0	1	2	1	10
Covert photography in a public space	6	1	0	2	1	3	0	4	0	17
Sound recording bug at home	3	0	0	2	1	0	1	-	1	-
Sound recording bug in target's vehicle	3	0	0	2	1	0	1	-	1	-
Sound recording bugs on public transport used by target	0	0	0	2	1	0	1	-	1	-
Sound recording bugs in police vehicle transporting target following arrest	6	0	0	2	1	0	1	-	1	-
Sound recording bugs in target's prison cell	6	0	0	2	1	0	1	-	1	-
Platform Micro Helicopter	6	1	0	2	1	3	0	4	0	17
AIS ship location detection and identification	0	1	1	0	0	0	0	0	0	2
Explosives detector near harbour	-	-	-	-	-	-	-	-	-	21
Gas chromatography drugs detector	-	-	-	-	-	-	-	-	-	21
Luggage screening technology (X-ray)	-	-	-	-	-	-	-	-	-	21
Eqo security scanner ("full body scanner")	3	1	1	2	2	3	1	4	1	18
Anti-Money laundering (AML) technologies	0	0	0	2	1	3	1	-	1	-
HEMOLIA	-	-	-	-	-	-	-	-	-	-
Data crawler SCIIMS	-	-	-	-	-	-	-	-	-	-
Data crawler OMNIFIND	-	-	-	-	-	-	-	-	-	-
Cellular Phone Location Tracking	6	1	0	2	1	0	1	2	1	14
Mobile Phone Tapping	6	0	0	2	1	0	1	-	1	-

Table 5: Assessment results

6.4 Analysis of results

The results of the rating done above are interesting on different levels. The score of two technologies is especially surprising. First the Eqo security scanner often called full body scanner has a score of 18. Therefore it is one of the best technologies rated. At first glance this is surprising as a huge privacy debate started when full body scanners where introduced. After this public discussion many different measures were introduced to prevent and mitigate the privacy risks. The newly developed systems do not display an image of an identifiable person and therefore achieved good ratings. This is an excellent example how a given technology can be altered to protect privacy while still enabling the functionality.
The second surprising technology is the AIS system. Because it was never intended to use AIS to track individuals no access control are other protection measures exist. This once more shows the privacy risks of systems, which do not collect or process PII but can be mapped to individuals under certain conditions.
One clear drawback of the detailed assessment is that a final scoring is only available when every question can be answered. As soon as a single question remains unclear no result on the technology can be given.

7 Conclusion and Outlook

At the end of SURVEILLE project month 20 it is clear that rating the privacy risks of surveillance is an extremely complicated matter. All existing methods to rate the privacy risks of an existing technology are too complicated and typically will take months to perform on a single technology. A further restriction is that a rating is only feasible if enough details about the technology and the usage scenario are known.

To cope with these problems we developed a simplified rating system that can solve most of the existing problems. It will yield less detailed results than a conventional audit, but it is possible to rate a technology in hours and not in months. It is still complicated, in that a lot of details about a certain technology are needed to make a fair rating. The same surveillance technology, i.e., a video surveillance system, could be designed in different ways, altering the audit result. With the help of technology experts we were able to rate typical representatives of most of the surveillance technologies used in the MerPOL scenario that was produced for D2.6 and included there.

The next step of our work will be to rate existing Privacy Enhancing Technologies (PETs) that can be used to improve the audit results of the surveillance systems in multiple ways. On the one hand when it is known that a surveillance technology implements a certain PET it can become possible to rate a system. One example of this is the sound recording bugs. When it is known if the system uses a PET that encrypts the data stored on the device, it is possible to rate question P2. On the other hand deploying a PET might improve the score of a system. For example integrating a watermark technology into CCTV system can prevent data manipulation from an internal attacker and therefore improve the rating of the surveillance system.

8 Annex: Detailed Technology Assessment for the MerPOL Scenario

In this chapter all technologies found in the MerPOL scenario are listed and rated in detail. The detailed technology descriptions were taken from SURVEILLE D2.6.

8.1 Technology: Closed-circuit television (CCTV); (public place – used overtly)

8.1.1 Description (TU Delft)

Closed-circuit television (CCTV) is a setup of video cameras to transmit a signal from a specific place to a limited set of monitors. The signal is not openly transmitted though it may employ point to point (P2P), point to multipoint, or mesh wireless links. CCTV technology is most often used for surveillance in areas that may need monitoring to prevent or register crimes.

The images in a CCTV system are captured through the lens of the camera and projected onto a high resolution CCD chip that converts the image into a large collection of digital data that is stored and transmitted along the interconnects (wired or wireless) of the CCTV system to television monitors or a storage server.

Today's High-definition CCTV-cameras have many computer controlled technologies that allow them to identify, track, and categorize objects in their field of view.

The Video Content Analysis (VCA) technology enables the automatic analysis of video content that is not based on a single image, but detect and determine events as a function of time. A system using VCA can recognize changes in the environment and even identify and compare objects related to a database based on pre-defined classifiers. VCA analytics can also be used to detect unusual patterns in a videos environment, such as anomalies in a crowd of people.

CCTV technology as a Facial Recognition System is a computer application that is able to automatically identify a person from a video source. So far only facial recognition in relation to a facial database with a limited number of persons and facial features has been effective with a low number of false positives. Facial recognition systems based on the interpretation of facial expression to determine a person's intention have so far not been very effective. Computerized monitoring of CCTV images is under development, allowing CCTV operators to observe many CCTV cameras simultaneously. These systems do not observe people directly but analyze the image on the basis of certain pre-defined classifiers like body movement behavior or certain types of baggage.

The data obtained with CCTV cameras is often stored on a digital video recorder or on a computer server. In order to limit the amount of data, these images are compressed and are often kept for a preset amount of time before they become automatically archived. Closed-circuit digital photography (CCDP) is often combined with CCTV to capture and save high-resolution images for applications where a detailed image is required. Modern day CCTV cameras are able to take images in a digital still mode that has a much higher resolution than the images captured in the video mode.

A growing development in CCTV technology is the application of internet protocol (IP) cameras. These cameras are equipped with an IP interface, enabling the incorporation of the camera in a Local Area Network (LAN) to transmit digital video data across. Optionally, the CCTV digital video data can be transmitted via the public internet, enabling users to view their cameras through any internet connection available. For professional secure applications IP video is restricted to within a private network or is recorded onto a secured remote server. IP cameras can be wired (LAN) or wireless (WLAN).

8.1.2 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?

  Yes, the technology is used in a public place.

8.1.3 Assessment Results

Here the detailed assessment results of the technology are listed.

8.1.3.1 Data collection

Q. No.	Question	Points	Weight	Score
C1	Is the collection of data selective?	1	3	3
C2	Is the amount of collected data from the subject minimized?	0	1	0
C4	Is the collection done overtly or covertly?	1	1	1

8.1.3.2 Details to the scoring

As the whole area is under video surveillance, the data collection is not as selective as possible. As typical CCTV system does not minimize data collection we assume that this also is the case here.

8.1.3.3 Data access and use

Q. No.	Question	Points	Weight	Score
A1	Who has access to the data?	1	2	2
A2	Is there a clear regulation who is allowed access under which circumstances?	1	1	1
A3	Is there a protection against function creep?	0	3	0

8.1.3.4 Details to the scoring

In the scenario the video surveillance system operates in a public place. The data collected by typical systems is only available for a team of operators and in special cases, as in the scenario for law enforcements. Regulations what the operators are allowed to do with the collected data exist and are required by law in most member states of the EU. Nonetheless no technical measure protects the people under surveillance from an operator that uses the system to look at woman instead of monitoring the area for crime. This also shows the problem of function creep that exists with all video surveillance systems.

8.1.3.5 Data protection

The data protection assessment is done for the following typical explanation of the technology:

Typical CCTV systems store video footage in an archive, this archive is protected by access control. Special measures are in place to protect the archive from external attacks against the video archive. As some EU member states, e.g. Germany, have high requirements when video footage is used in court the material is often protected against internal manipulation. As this is not the case for all EU member states, we assume that no protection against internal manipulation is present.

Q. No.	Question	Points	Weight	Score
P1	Is the collected data encrypted or otherwise access protected?	1	1	1
P2	Is the data protected against manipulation?	1	2	2
P3	Is the collection device secure against data theft?	1	1	1

8.1.4 Conclusion

Video surveillance in public places is a highly discussed topic. Done correctly it has an acceptable privacy protection scoring. Critical is the insufficient protection against function creep and misuse by the operators. This is especially problematic because of the low level of transparency achieved by the systems.

8.2 Technology: Closed-circuit television (CCTV); (public place – used covertly)

8.2.1 Description (TU Delft)

Closed-circuit television (CCTV) is a setup of video cameras to transmit a signal from a specific place to a limited set of monitors. The signal is not openly transmitted though it may employ point to point (P2P), point to multipoint, or mesh wireless links. CCTV technology is most often used for surveillance in areas that may need monitoring to prevent or register crimes.
The images in a CCTV system are captured through the lens of the camera and projected onto a high resolution CCD chip that converts the image into a large collection of digital data that is stored and transmitted along the interconnects (wired or wireless) of the CCTV system to television monitors or a storage server.
Today's High-definition CCTV-cameras have many computer controlled technologies that allow them to identify, track, and categorize objects in their field of view.
The Video Content Analysis (VCA) technology enables the automatic analysis of video content that is not based on a single image, but detect and determine events as a function of time. A system using VCA can recognize changes in the environment and even identify and compare objects related to a database based on pre-defined classifiers. VCA analytics can also be used to detect unusual patterns in a videos environment, such as anomalies in a crowd of people.
CCTV technology as a Facial Recognition System is a computer application that is able to automatically identify a person from a video source. So far only facial recognition in relation to a facial database with a limited number of persons and facial features has been effective with a low number of false positives. Facial recognition systems based on the interpretation of facial expression to determine a person's intention have so far not been very effective. Computerized monitoring of CCTV images is under development, allowing CCTV operators to observe many CCTV cameras simultaneously. These systems do not observe people directly but analyze the image on the basis of certain pre-defined classifiers like body movement behavior or certain types of baggage.
The data obtained with CCTV cameras is often stored on a digital video recorder or on a computer server. In order to limit the amount of data, these images are compressed and are often kept for a preset amount of time before they become automatically archived.
Closed-circuit digital photography (CCDP) is often combined with CCTV to capture and save high-resolution images for applications where a detailed image is required. Modern day CCTV cameras are able to take images in a digital still mode that has a much higher resolution than the images captured in the video mode.
A growing development in CCTV technology is the application of internet protocol (IP) cameras. These cameras are equipped with an IP interface, enabling the incorporation of the camera in a Local Area Network (LAN) to transmit digital video data across.
Optionally, the CCTV digital video data can be transmitted via the public internet, enabling users to view their cameras through any internet connection available. For professional secure applications IP video is restricted to within a private network or is recorded onto a secured remote server. IP cameras can be wired (LAN) or wireless (WLAN).

8.2.2 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?

  Yes, the technology is used in a public place

8.2.3 Assessment Results

Here the detailed assessment results of the technology are listed.

8.2.3.1 Data collection

Q. No.	Question	Points	Weight	Score
C1	Is the collection of data selective?	1	3	3
C2	Is the amount of collected data from the subject minimized?	0	1	0
C4	Is the collection done overtly or covertly?	0	1	0

8.2.3.2 Details to the scoring

As the whole are is under video surveillance, the data collection is not as selective as possible. As typical CCTV system does not minimize data collection we assume that this also is the case here. As this system is used covertly no transparency is given to the people in the area under surveillance.

8.2.3.3 Data access and use

Q. No.	Question	Points	Weight	Score
A1	Who has access to the data?	1	2	2
A2	Is there a clear regulation who is allowed access under which circumstances?	1	1	1
A3	Is there a protection against function creep?	0	3	0

8.2.3.4 Details to the scoring

In the scenario the video surveillance system operates in a public place. The data collected by typical systems is only available for a team of operators and in special cases, as in the scenario for law enforcements. Regulations what the operators are allowed to do with the collected data exist and are required by law in most member states of the EU. Nonetheless no technical measure protects the people under surveillance from an operator that uses the system to look at woman instead of monitoring the area for crim. This also shows the problem of function creep that exists with all video surveillance systems.

8.2.3.5 Data protection

The data protection assessment is done for the following typical explanation of the technology:

Typical CCTV systems store video footage in an archive, this archive is protected by access control. Special measures are in place to protect the archive from external attacks against the video archive. As some EU member states, e.g. Germany, have high requirements when video footage is used in court the material is often protected against internal manipulation. As this is not the case for all EU member states, we assume that no protection against internal manipulation is present.

Q. No.	Question	Points	Weight	Score
P1	Is the collected data encrypted or otherwise access protected?	1	1	1
P2	Is the data protected against manipulation?	1	2	2
P3	Is the collection device secure against data theft?	1	1	1

8.2.4 Conclusion

Video surveillance in public places is a highly discussed topic. Done correctly it has an acceptable privacy protection scoring. Critical is the insufficient protection against

function creep and misuse by the operators. This is especially problematic because of the low level of transparency achieved by the systems, this gets even worse when the system is used in an covert mode.

8.3 Technology: Covert photography in a public space

8.3.1 Description (FHG)

When police officers take covert photos of the subject conventional digital cameras are used. Modern digital single lens reflex camera with zoom lenses can be used over long distances. In good weather conditions it is possible to identify persons over couple of hundred meters. This allows the officers to have a safe distance to the subject to not get spotted.

8.3.2 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?

  yes

8.3.3 Assessment Results

Here the detailed assessment results of the technology are listed.

8.3.3.1 Data collection

Q. No.	Question	Points	Weight	Score
C1	Is the collection of data selective?	2	3	6
C2	Is the amount of collected data from the subject minimized?	1	1	1
C4	Is the collection done overtly or covertly?	0	1	0

8.3.3.2 Details to the scoring

Manually taking photos of subject enables the officers or photograph to wait until no or limited amount of bystanders are present. This allows for a selective and minimized data collection of the subject. When to goal of the observation is to create photos of the subject X and his potential business partner Y, there is no need to take pictures of the subject and his family etc.

8.3.3.3 Data access and use

Q. No.	Question	Points	Weight	Score
A1	Who has access to the data?	1	2	2
A2	Is there a clear regulation who is allowed access under which circumstances?	1	1	1
A3	Is there a protection against function creep?	1	3	3

8.3.3.4 Details to the scoring

As there is no further clarification in the scenario it is unclear who will have access to the collected pictures but it seems safe to assume, that only relevant stakeholders will have access to covertly taken photographs. The same rule applies to the usage of the data; it will be restricted to the case the law enforcement is currently working on, but only by organizational measures not by technology. Protection against function creep should be inherent in by the processes of police work. This will prevent unlawful processing of the data under changed function.

8.3.3.5 Data protection

The data protection assessment is done for the following typical explanation of the technology:

Unfortunately the scenario gives no details over how the data is stored once collected and how the collection device is protected. Therefore we are going to describe and rate a typical system. DSLR cameras do not protect the data by encryption but high class models apply cryptographic signatures to ensure that the data is not manipulated after it was taken[18]. If the camera gets stolen the taken pictures could be used by anybody.

Q. No.	Question	Points	Weight	Score
P1	Is the collected data encrypted or otherwise access protected?	0	1	0
P2	Is the data protected against manipulation?	2	2	4
P3	Is the collection device secure against data theft?	0	1	1

8.3.4 Conclusion

In the context of data protection covert photos of subject achieve good results. The measure is highly selective and as most of the collected data is under the control of the police or other law enforcement teams only a limited risk of data loss or function creep is present.

[18] http://cpn.canon-europe.com/content/education/infobank/image_verification/canon_data_verification_system.do

8.4 Technology: Sound recording bug at home

8.4.1 Description (TU Delft)

Audio surveillance devices, like phone bugs, distant audio recorders or cell-phone audio bugs can be assembled into a very small device and incorporated into almost any object we use in our everyday life. Audio surveillance devices capture the audio with a microphone (audio sensor), which converts the audio signal to an electric signal. This analog electric signal is converted via an analogue to digital converter to binary data, which can be stored and distributed wired or wireless to a receiver, where the signal is converted from a digital into an analogue audio signal. Due to modern day chip technology, these audio surveillance devices consists of only a few electronic devices, assembled on a very small printed circuit board, enabling the incorporation of the device in almost any object available. Most of the present day audio chips that are used have also a DSP (Digital Signal Processor) incorporated, allowing onboard digital audio signal processing to enhance the quality of the sound.
The sound bugs can be hidden almost anywhere. Their vulnerability for detection is in the way the sound bugs communicate the received digital audio signal to the receiver. When the communication is wireless the sound bug transmits an electromagnetic wave within a certain frequency band, which can be detected with a device that can locate these electromagnetic sources.
Sound bugging is also done by measuring the vibrations of windows with the aid of a laser monitoring device or a sound bug hidden in an adhesive substance stuck on the window.

8.4.2 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?
  yes

8.4.3 Assessment Results

Here the detailed assessment results of the technology are listed.

8.4.3.1 Data collection

Q. No.	Question	Points	Weight	Score
C1	Is the collection of data selective?	1	3	3
C2	Is the amount of collected data from the subject minimized?	0	1	0
C4	Is the collection done overtly or covertly?	0	1	0

8.4.3.2 Details to the scoring

The selectivity of sound bugs in general is pretty bad as they will record the voice of every person in reach. The collected data is not minimized, as next to important conversations with subject also private conversation in the family or with layers or doctors could be overheard. Sound bugs are always used covertly.

8.4.3.3 Data access and use

Q. No.	Question	Points	Weight	Score
A1	Who has access to the data?	1	2	2
A2	Is there a clear regulation who is allowed access under which circumstances?	1	1	1

A3	Is there a protection against function creep?	0	3	0

8.4.3.4 Details to the scoring

When law enforcement uses sound bugs, only relevant stakeholders have access to the collected data. There will be an organizational regulation on how is allowed to process and handle the data, but no protection against function creep is present.

8.4.3.5 Data protection

The data protection assessment is done for the following typical explanation of the technology:

As audio bugs are custom hardware and no commercial of the self-product its data protection methods are even harder to measure. As its custom build it is reasonable to assume that the uncommon build will guarantee some protection against access by unauthorized parties. If a method is in place to protect the data from internal or external manipulation is unclear.

Q. No.	Question	Points	Weight	Score
P1	Is the collected data encrypted or otherwise access protected?	1	1	1
P2	Is the data protected against manipulation?	-	2	-
P3	Is the collection device secure against data theft?	1	1	1

8.4.4 Conclusion

Audio bugs have a huge potential impact on data protection. As the measure is costly and personal and time-consuming it will most likely only be used in special cases. The version where the home of the subject is bugged offers some protection against a broad surveillance of large parts of the population but still possesses a high risk for the privacy of unrelated third parties.

8.5 Technology: Sound recording bug in target's vehicle

8.5.1 Description (TU Delft)

Audio surveillance devices, like phone bugs, distant audio recorders or cell-phone audio bugs can be assembled into a very small device and incorporated into almost any object we use in our everyday life. Audio surveillance devices capture the audio with a microphone (audio sensor), which converts the audio signal to an electric signal. This analog electric signal is converted via an analogue to digital converter to binary data, which can be stored and distributed wired or wireless to a receiver, where the signal is converted from a digital into an analogue audio signal. Due to modern day chip technology, these audio surveillance devices consists of only a few electronic devices, assembled on a very small printed circuit board, enabling the incorporation of the device in almost any object available. Most of the present day audio chips that are used have also a DSP (Digital Signal Processor) incorporated, allowing onboard digital audio signal processing to enhance the quality of the sound.
The sound bugs can be hidden almost anywhere. Their vulnerability for detection is in the way the sound bugs communicate the received digital audio signal to the receiver. When the communication is wireless the sound bug transmits an electromagnetic wave within a certain frequency band, which can be detected with a device that can locate these electromagnetic sources.
Sound bugging is also done by measuring the vibrations of windows with the aid of a laser monitoring device or a sound bug hidden in an adhesive substance stuck on the window.

8.5.2 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?
  yes

8.5.3 Assessment Results

Here the detailed assessment results of the technology are listed.

8.5.3.1 Data collection

Q. No.	Question	Points	Weight	Score
C1	Is the collection of data selective?	1	3	3
C2	Is the amount of collected data from the subject minimized?	0	1	0
C4	Is the collection done overtly or covertly?	0	1	0

8.5.3.2 Details to the scoring

The selectivity of sound bugs in general is pretty bad as they will record the voice of every person in reach. The collected data is not minimized, as next to important conversations with subject also private conversation in the family or with layers or doctors could be overheard. Sound bugs are always used covertly.

8.5.3.3 Data access and use

Q. No.	Question	Points	Weight	Score
A1	Who has access to the data?	1	2	2
A2	Is there a clear regulation who is allowed access under which circumstances?	1	1	1

A3	Is there a protection against function creep?	0	3	0

8.5.3.4 Details to the scoring

When law enforcement uses sound bugs, only relevant stakeholders have access to the collected data. There will be an organizational regulation on how is allowed to process and handle the data, but no protection against function creep is present.

8.5.3.5 Data protection

The data protection assessment is done for the following typical explanation of the technology:

As audio bugs are custom hardware and no commercial of the self-product its data protection methods are even harder to measure. As its custom build it is reasonable to assume that the uncommon build will guarantee some protection against access by unauthorized parties. If a method is in place to protect the data from internal or external manipulation is unclear.

Q. No.	Question	Points	Weight	Score
P1	Is the collected data encrypted or otherwise access protected?	1	1	1
P2	Is the data protected against manipulation?	-	2	-
P3	Is the collection device secure against data theft?	1	1	1

8.5.4 Conclusion

Audio bugs have a huge potential impact on data protection. As the measure is costly and personal and time-consuming it will most likely only be used in special cases. The version where the car of the subject is bugged offers some selectiveness against a broad surveillance of large parts of the population.

8.6 Technology: Sound recording bugs on public transport used by target

8.6.1 Description (TU Delft)

Audio surveillance devices, like phone bugs, distant audio recorders or cell-phone audio bugs can be assembled into a very small device and incorporated into almost any object we use in our everyday life. Audio surveillance devices capture the audio with a microphone (audio sensor), which converts the audio signal to an electric signal. This analog electric signal is converted via an analogue to digital converter to binary data, which can be stored and distributed wired or wireless to a receiver, where the signal is converted from a digital into an analogue audio signal. Due to modern day chip technology, these audio surveillance devices consists of only a few electronic devices, assembled on a very small printed circuit board, enabling the incorporation of the device in almost any object available. Most of the present day audio chips that are used have also a DSP (Digital Signal Processor) incorporated, allowing onboard digital audio signal processing to enhance the quality of the sound.
The sound bugs can be hidden almost anywhere. Their vulnerability for detection is in the way the sound bugs communicate the received digital audio signal to the receiver. When the communication is wireless the sound bug transmits an electromagnetic wave within a certain frequency band, which can be detected with a device that can locate these electromagnetic sources.
Sound bugging is also done by measuring the vibrations of windows with the aid of a laser monitoring device or a sound bug hidden in an adhesive substance stuck on the window.

8.6.2 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?
  yes

8.6.3 Assessment Results

Here the detailed assessment results of the technology are listed.

8.6.3.1 Data collection

Q. No.	Question	Points	Weight	Score
C1	Is the collection of data selective?	0	3	0
C2	Is the amount of collected data from the subject minimized?	0	1	0
C4	Is the collection done overtly or covertly?	0	1	0

8.6.3.2 Details to the scoring

The selectivity of sound bugs in general is pretty bad as they will record the voice of every person in reach. Especially as the bug is in a public transport system this gets no points for selectivity. The collected data is not minimized, as next to important conversations with subject also private conversation in the family or with layers or doctors could be overheard. Sound bugs are always used covertly.

8.6.3.3 Data access and use

Q. No.	Question	Points	Weight	Score
A1	Who has access to the data?	1	2	2
A2	Is there a clear regulation who is allowed access	1	1	1

	under which circumstances?			
A3	Is there a protection against function creep?	0	3	0

8.6.3.4 Details to the scoring

When law enforcement uses sound bugs, only relevant stakeholders have access to the collected data. There will be an organizational regulation on how is allowed to process and handle the data, but no protection against function creep is present.

8.6.3.5 Data protection

The data protection assessment is done for the following typical explanation of the technology:

As audio bugs are custom hardware and no commercial of the self-product its data protection methods are even harder to measure. As its custom build it is reasonable to assume that the uncommon build will guarantee some protection against access by unauthorized parties. If a method is in place to protect the data from internal or external manipulation is unclear.

Q. No.	Question	Points	Weight	Score
P1	Is the collected data encrypted or otherwise access protected?	1	1	1
P2	Is the data protected against manipulation?	-	2	-
P3	Is the collection device secure against data theft?	1	1	0

8.6.4 Conclusion

Audio bugs have a huge potential impact on data protection. As the measure is costly and personal and time-consuming it will most likely only be used in special cases. The version where the car of the subject is bugged offers some selectiveness against a broad surveillance of large parts of the population.

8.7 Technology: Sound recording bugs in police vehicle transporting target following arrest

8.7.1 Description (TU Delft)

Audio surveillance devices, like phone bugs, distant audio recorders or cell-phone audio bugs can be assembled into a very small device and incorporated into almost any object we use in our everyday life. Audio surveillance devices capture the audio with a microphone (audio sensor), which converts the audio signal to an electric signal. This analog electric signal is converted via an analogue to digital converter to binary data, which can be stored and distributed wired or wireless to a receiver, where the signal is converted from a digital into an analogue audio signal. Due to modern day chip technology, these audio surveillance devices consists of only a few electronic devices, assembled on a very small printed circuit board, enabling the incorporation of the device in almost any object available. Most of the present day audio chips that are used have also a DSP (Digital Signal Processor) incorporated, allowing onboard digital audio signal processing to enhance the quality of the sound.
The sound bugs can be hidden almost anywhere. Their vulnerability for detection is in the way the sound bugs communicate the received digital audio signal to the receiver. When the communication is wireless the sound bug transmits an electromagnetic wave within a certain frequency band, which can be detected with a device that can locate these electromagnetic sources.
Sound bugging is also done by measuring the vibrations of windows with the aid of a laser monitoring device or a sound bug hidden in an adhesive substance stuck on the window.

8.7.2 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?
  yes

8.7.3 Assessment Results

Here the detailed assessment results of the technology are listed.

8.7.3.1 Data collection

Q. No.	Question	Points	Weight	Score
C1	Is the collection of data selective?	2	3	6
C2	Is the amount of collected data from the subject minimized?	0	1	0
C4	Is the collection done overtly or covertly?	0	1	0

8.7.3.2 Details to the scoring

The selectivity of sound bugs in general is pretty bad as they will record the voice of every person in reach. When a bug is only present in the police vehicle after the subject was arrested the selectivity is good. The collected data is not minimized, as next to important conversations with subject also private conversation in the family or with layers or doctors could be overheard. Sound bugs are always used covertly.

8.7.3.3 Data access and use

Q. No.	Question	Points	Weight	Score
A1	Who has access to the data?	1	2	2

A2	Is there a clear regulation who is allowed access under which circumstances?	1	1	1
A3	Is there a protection against function creep?	0	3	0

8.7.3.4 Details to the scoring

When law enforcement uses sound bugs, only relevant stakeholders have access to the collected data. There will be an organizational regulation on how is allowed to process and handle the data, but no protection against function creep is present.

8.7.3.5 Data protection

The data protection assessment is done for the following typical explanation of the technology:

As audio bugs are custom hardware and no commercial of the self-product its data protection methods are even harder to measure. As its custom build it is reasonable to assume that the uncommon build will guarantee some protection against access by unauthorized parties. If a method is in place to protect the data from internal or external manipulation is unclear.

Q. No.	Question	Points	Weight	Score
P1	Is the collected data encrypted or otherwise access protected?	1	1	1
P2	Is the data protected against manipulation?	-	2	-
P3	Is the collection device secure against data theft?	1	1	0

8.7.4 Conclusion

Audio bugs have a huge potential impact on data protection. As the measure is costly and personal and time-consuming it will most likely only be used in special cases. The version where the car of the subject is bugged offers some selectiveness against a broad surveillance of large parts of the population.

8.8 Technology: Sound recording bugs in target's prison cell

8.8.1 Description (TU Delft)

Audio surveillance devices, like phone bugs, distant audio recorders or cell-phone audio bugs can be assembled into a very small device and incorporated into almost any object we use in our everyday life. Audio surveillance devices capture the audio with a microphone (audio sensor), which converts the audio signal to an electric signal. This analog electric signal is converted via an analogue to digital converter to binary data, which can be stored and distributed wired or wireless to a receiver, where the signal is converted from a digital into an analogue audio signal. Due to modern day chip technology, these audio surveillance devices consists of only a few electronic devices, assembled on a very small printed circuit board, enabling the incorporation of the device in almost any object available. Most of the present day audio chips that are used have also a DSP (Digital Signal Processor) incorporated, allowing onboard digital audio signal processing to enhance the quality of the sound.
The sound bugs can be hidden almost anywhere. Their vulnerability for detection is in the way the sound bugs communicate the received digital audio signal to the receiver. When the communication is wireless the sound bug transmits an electromagnetic wave within a certain frequency band, which can be detected with a device that can locate these electromagnetic sources.
Sound bugging is also done by measuring the vibrations of windows with the aid of a laser monitoring device or a sound bug hidden in an adhesive substance stuck on the window.

8.8.2 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?
  yes

8.8.3 Assessment Results

Here the detailed assessment results of the technology are listed.

8.8.3.1 Data collection

Q. No.	Question	Points	Weight	Score
C1	Is the collection of data selective?	2	3	6
C2	Is the amount of collected data from the subject minimized?	0	1	0
C4	Is the collection done overtly or covertly?	0	1	0

8.8.3.2 Details to the scoring

The selectivity of sound bugs in general is pretty bad as they will record the voice of every person in reach. When a bug is only present in the subject's prison cell the selectivity is good as only a minimal change exists that an unrelated third party is recorded. The collected data is not minimized, as next to important conversations with subject also private conversation in the family or with layers or doctors could be overheard. Sound bugs are always used covertly.

8.8.3.3 Data access and use

Q. No.	Question	Points	Weight	Score
A1	Who has access to the data?	1	2	2

A2	Is there a clear regulation who is allowed access under which circumstances?	1	1	1
A3	Is there a protection against function creep?	0	3	0

8.8.3.4 Details to the scoring

When law enforcement uses sound bugs, only relevant stakeholders have access to the collected data. There will be an organizational regulation on how is allowed to process and handle the data, but no protection against function creep is present.

8.8.3.5 Data protection

The data protection assessment is done for the following typical explanation of the technology:

As audio bugs are custom hardware and no commercial of the self-product its data protection methods are even harder to measure. As its custom build it is reasonable to assume that the uncommon build will guarantee some protection against access by unauthorized parties. If a method is in place to protect the data from internal or external manipulation is unclear.

Q. No.	Question	Points	Weight	Score
P1	Is the collected data encrypted or otherwise access protected?	1	1	1
P2	Is the data protected against manipulation?	-	2	-
P3	Is the collection device secure against data theft?	1	1	0

8.8.4 Conclusion

Audio bugs have a huge potential impact on data protection. As the measure is costly and personal and time-consuming it will most likely only be used in special cases. The version where the car of the subject is bugged offers some selectiveness against a broad surveillance of large parts of the population.

8.9 Technology: Platform Micro Helicopter

8.9.1 Description (TU Delft)

A micro-helicopter is the smallest type of UAV or unmanned aerial vehicle, a micro-UAV. Micro-helicopters are usually quadrocopters (with 4 rotors). The payload is usually one small camera. Its operating range is small; typically an operator is in close proximity of the quadrocopter. Relevant for the scenario is that range and payload capabilities of UAV's vary. Note that the UAV itself is not a surveillance instrument but a platform for carrying surveillance instrumentation.
For the purposes of this assessment the review considers a platform micro helicopter equipped with a camera sensing device that captures stills and motion video in the visible light spectrum, rather than other possible configurations that include sensing and scanning capabilities such as radar, infra-red and terahertz (terahertz waves - the portion of the electromagnetic spectrum between infrared and microwave light) sensing. Furthermore, this review assumes that images are captured, transmitted and recorded for the purposes of surveillance. Audio is not, however, assumed to be subject to monitoring in this instance (though such a capability does exist).

8.9.2 Scenario Details

The home address for Z is in a rural location making general surveillance by a team and the deployment of covert CCTV extremely difficult. As such, law enforcement officers may consider the deployment of a platform micro helicopter fitted with standard image capture functionality to record images of activity in the location. The scenario envisages the device being used in a covert surveillance operation, which infers that the monitoring is conducted discretely so as to avoid detection.

8.9.3 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?
  Yes, photos/video footage of the subject is made

8.9.4 Assessment Results

Here the detailed assessment results of the technology are listed. As described in the scenario details the drone is used as a measure to take photos or video of the subject in a covert mode. Therefore the results are similar to the results of the covert photo team.

8.9.4.1 Data collection

Q. No.	Question	Points	Weight	Score
C1	Is the collection of data selective?	2	3	6
C2	Is the amount of collected data from the subject minimized?	1	1	1
C4	Is the collection done overtly or covertly?	0	1	0

8.9.4.2 Details to the scoring

Making photos of the subject allows the officers or photograph in general to wait until no or limited amount of bystanders are present. This although allows for a selective and minimized data collection of the subject. When to goal of the observation is to create photos of the subject X and his potential business partner Y, there is no need to take pictures of the subject and his family etc.

8.9.4.3 Data access and use

Q. No.	Question	Points	Weight	Score
A1	Who has access to the data?	1	2	2
A2	Is there a clear regulation who is allowed access under which circumstances?	1	1	1
A3	Is there a protection against function creep?	1	3	3

8.9.4.4 Details to the scoring

As there is no further clarification in the scenario it is unclear who will have access to the collected pictures but it seems safe to assume, that only relevant stakeholders will have access to covertly taken photographs. The same rule applies to the usage of the data; it will be restricted to the case the law enforcement is currently working on, but only by organizational measures not by technology. Protection against function creep should be inherited by the processes of police work. This will prevent unlawful processing of the data under changed function.

8.9.4.5 Data protection

The data protection assessment is done for the following typical explanation of the technology:

Unfortunately the scenario gives no details over how the data is stored once collected and how the collection device is protected. Therefore we are going to describe and rate a typical system. In contrast to the covert photo team we do assume that due to weight limits no high end DSLR camera will be used. Therefore no protection against image manipulation will be present. If the camera gets stolen the taken pictures could be used by anybody.

Q. No.	Question	Points	Weight	Score
P1	Is the collected data encrypted or otherwise access protected?	0	1	0
P2	Is the data protected against manipulation?	0	2	0
P3	Is the collection device secure against data theft?	0	1	0

8.9.5 Conclusion

In the context of data protection covert photos of subject achieve good results. The measure is highly selective and as most of the collected data is under the control of the police or other law enforcement teams only a limited risk of data loss or function creep is present.

8.10 Technology: AIS ship location detection and identification

8.10.1 Description (TU Delft)

AIS stands for Automatic Identification System. This system is designed to provide information about the ship to other ships and to coastal authorities automatically (IMO). In 2000, IMO adopted a new requirement for all ships to carry automatic identification systems (AISs) capable of providing information about the ship to other ships and to coastal authorities. Ships fitted with AIS shall maintain AIS in operation at all times except where international agreements, rules or standards provide for the protection of navigational information.
AIS provides:

1. transmitting the ship's identity, type, position, course, speed, navigational status and other safety-related information;
2. receiving automatically such information from similarly fitted ships; monitoring and tracking ships;
3. exchanging data with shore-based facilities

All ships can be seen on the internet at url http://www.marinetraffic.com/ais/nl/

8.10.2 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?
  No, only data about ships is collected.
- Is it possible to map the collected data to an individual person?
  As it is the case in the scenario the police use the AIS to track the subjects' position. Therefore PII is collected.

8.10.3 Assessment Results

Here the detailed assessment results of the technology are listed.

8.10.3.1 Data collection

Q. No.	Question	Points	Weight	Score
C1	Is the collection of data selective?	0	3	0
C2	Is the amount of collected data from the subject minimized?	1	1	1
C4	Is the collection done overtly or covertly?	1	1	1

8.10.3.2 Details to the scoring

As every ship over a certain weight has to have an AIS system the measure is not selective. Only a strictly limited amount of data about the ships is collected which gives a high minimization score as well as the fact that the AIS system is an overt system.

8.10.3.3 Data access and use

Q. No.	Question	Points	Weight	Score
A1	Who has access to the data?	0	2	0
A2	Is there a clear regulation who is allowed access under which circumstances?	0	1	0
A3	Is there a protection against function creep?	0	3	0

8.10.3.4 Details to the scoring

The data of the AIS system open to everybody. On http://www.marinetraffic.com/ais/ the current position of every ship with an AIT system is visible. There are no regulations on the usage of the data, at least no regulations what will prevent any misuse. Function creep as well is not prevented at all. In fact it is arguable is the policy using the system to track subjects is a case of function creep.

8.10.3.5 Data protection

As AIT is a finished project and documented the data protection can easily evaluated. Unfortunately the system offers no protection for the data. This could be to the reason that the collected data itself is neither critical nor private. Only the combination of the AIT system with the knowledge which persons are onboard makes the case critical.

Q. No.	Question	Points	Weight	Score
P1	Is the collected data encrypted or otherwise access protected?	0	1	0
P2	Is the data protected against manipulation?	0	2	0
P3	Is the collection device secure against data theft?	0	1	0

8.10.4 Conclusion

The AIT system itself is an open system to monitor the movement of larger ships. As it was never intended or understood that is could be used to track individual persons , no protection for that data exists.

8.11 Technology: Explosives detector near harbor

8.11.1 Description (TU Delft)

This technology was developed recently in a EU research project called UNCOSS: Underwater Coastal Sea Surveyor (UNCOSS: Final Report UNCOSS, 2012). An explosive detector is mounted on an ROV. Remotely Operated Vehicle is an unmanned submarine that operates in close proximity of a ship to which it remains connected. The detector can scan the bottom of the sea for suspect objects and then remotely analyse the contents of the object. Thereby it can detect explosives without touching the object. The UNCOSS ROV is deployed in an area where suspicious objects are located. Typically these can are WWII bombs, torpedoes or IED's. The ROV searches the sea floor for anomalies by optical detectors (cameras) or magnetic detectors that detect metals, in the latter case, hidden devices can be found as well. If a suspect material is found, the ROV is brought into close proximity of the material and it is bombarded with neutron radiation (nuclear radiation with uncharged atomic particles: neutrons). This radiation induces gamma radiation from the object (nuclear radiation in the form of photons, similar to x-ray but with higher energy content). The gamma radiation that is returned to the detector shows what atoms are present in the object. Carbon, oxygen, hydrogen and nitrogen atoms are detected. The relative amount of the number of atoms is a clue to which explosive is present in the object.

8.11.2 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?
  No.
- Is it possible to map the collected data to an individual person?
  No.

8.11.3 Conclusion

As the system does not process any PII there is no need for a data protection assessment and the system will get the highest score for data protection.

8.12 Technology: Gas chromatography drugs detector

8.12.1 Description (TU Delft)

Gas chromatography mass spectrometry (GC/MS) is an important technique in the detection and identification of both bulk drugs and trace level drugs in biological samples. Gas chromatography–mass spectrometry (GC-MS) is a method that combines the features of gas-liquid chromatography and mass spectrometry to identify different substances within a test sample. GC-MS has been widely heralded as a "gold standard" for forensic substance identification because it is used to perform a specific test. A specific test positively identifies the actual presence of a particular substance in a given sample. A non-specific test merely indicates that a substance falls into a category of substances. Although a non-specific test could statistically suggest the identity of the substance, this could lead to false positive identification. A mass spectrometer is typically utilized in one of two ways: full scan or selected ion monitoring (SIM). The typical GC-MS instrument is capable of performing both functions either individually or concomitantly, depending on the setup of the particular instrument.
The primary goal of instrument analysis is to quantify an amount of substance. This is done by comparing the relative concentrations among the atomic masses in the generated spectrum. Two kinds of analysis are possible, comparative and original. Comparative analysis essentially compares the given spectrum to a spectrum library to see if its characteristics are present for some sample in the library. This is best performed by a computer because there are a myriad of visual distortions that can take place due to variations in scale. Computers can also simultaneously correlate more data (such as the retention times identified by GC), to more accurately relate certain data.

8.12.2 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?
  No.
- Is it possible to map the collected data to an individual person?
  No.

8.12.3 Conclusion

As the system does not process any PII there is no need for a data protection assessment and the system will get the highest score for data protection.

8.13 Technology: Luggage screening technology (X-ray)

8.13.1 Description (FHG)

Luggage scanners consist of an X-Ray generator and a detector as well as a signal processing unit. Typical systems deploy two different energetic levels of radiation to distinguish between organic and inorganic material.

8.13.2 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?
  No.
- Is it possible to map the collected data to an individual person?
  No.

8.13.3 Conclusion

As the system does not process any PII there is no need for a data protection assessment and the system will get the highest score for data protection.

8.14 Technology: Eqo security scanner (“full body scanner”)

8.14.1 Description (Smiths Detection + TU Delft)

Smiths’ eqo security scanner ("body scanner") is a millimetre-wave body imaging scanner which provides a rapid means of detecting concealed threat objects. The automated detection capability dispenses with the need for operators to review a millimetre-wave image. A generic graphical representation of the person is presented to the operator. The system software detects concealed objects and indicates their location with a marker on the appropriate part of the graphical display.
This type of scanner operates like a sonar or radar device, hence the product's eqo name referring to the system's technological approach of sending out and analyzing the signal information as reflected by the human body. Using non-ionizing energy, eqo scans the passenger's body. Reflections from any concealed objects are different to those from a person's body and this variation is detected by eqo's sensors.
Those reflected signals are sent into a high-speed image processing computer which produces privacy filtered, three-dimensional image data models in real-time. These video-style images can be displayed as rotatable images or can be further analyzed electronically.

8.14.2 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?
  Yes.

8.14.3 Assessment Results

Here the detailed assessment results of the technology are listed.

8.14.3.1 Data collection

Q. No.	Question	Points	Weight	Score
C1	Is the collection of data selective?	1	3	3
C2	Is the amount of collected data from the subject minimized?	1	1	1
C4	Is the collection done overtly or covertly?	1	1	1

8.14.3.2 Details to the scoring

As most airports use full body scanners to evaluate random and conspicuous passengers they are a selective measure. As the data is privacy filtered before it is displayed the data is minimized to a level that allows the concrete security task but protects the privacy of affected people. The surveillance measure is always done overtly.

8.14.3.3 Data access and use

Q. No.	Question	Points	Weight	Score
A1	Who has access to the data?	1	2	2
A2	Is there a clear regulation who is allowed access under which circumstances?	2	1	2
A3	Is there a protection against function creep?	1	3	3

8.14.3.4 Details to the scoring

The collected data is either processed by an operator right next to the body scanner or by a third person in a remote location. In both cases it is ensured that the results are

only handled by security personal. To further protect the passengers' privacy modern body scanners have special security measures that prevent that any data is extracted from the system.

8.14.3.5 Data protection

The data protection assessment is done for the following typical explanation of the technology:

Modern body scanners have a high level of data protection. The results get deleted after they are taken or are stored in a secure way for a limited amount of time. As the system offers no mean of editing the collected data no internal or external manipulating of the data is possible.

Q. No.	Question	Points	Weight	Score
P1	Is the collected data encrypted or otherwise access protected?	1	1	1
P2	Is the data protected against manipulation?	2	2	4
P3	Is the collection device secure against data theft?	1	1	1

8.14.4 Conclusion

In terms of data protection new generation body scanners can achieve a high score.

8.15 Technology: Anti-Money laundering (AML) technologies

8.15.1 Description (TU Delft)

Anti-Money laundering (AML) technology is used as part of a normal financial crime investigation to prevent concealing illicit sources of money. Some anti-money laundering technologies rely upon techniques developed in the field of artificial intelligence (AI), others involve computer graphics and statistical computing. There are at least four categories of technologies that may be useful in the analysis of wire transfers. These technologies can be classified by the task they are designed to accomplish:

- Knowledge acquisition to construct new profiles of money laundering activities;
- Data transformation to produce data that can be easily screened and analyzed.
- Wire transfer screening to determine the focus of investigations, based on profiles;
- Knowledge sharing to disseminate profiles quickly, reliably, and in a useful form.

Anti-Money laundering tools are 'data crawlers' and, in some respects, maybe not so different from a Google search engine. They search for financial anomalies. Anomalies may include: uncharacteristically large financial deposits, organizations or banks that were already associated with money laundering in earlier investigations, suspect gambling operators, connections between known criminals and financial flows.

8.15.2 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?
  Yes

8.15.3 Assessment Results

Here the detailed assessment results of the technology are listed.

8.15.3.1 Data collection

Q. No.	Question	Points	Weight	Score
C1	Is the collection of data selective?	0	3	0
C2	Is the amount of collected data from the subject minimized?	0	1	0
C4	Is the collection done overtly or covertly?	0	1	0

8.15.3.2 Details to the scoring

As the crawlers have to analyze all available money flows, or at least all flows in foreign countries it is an unselective measure. In the description no minimization of the collected data could be identified as the results are not filtered by conditions as certain countries of high money flows.

8.15.3.3 Data access and use

Q. No.	Question	Points	Weight	Score
A1	Who has access to the data?	1	2	2
A2	Is there a clear regulation who is allowed access under which circumstances?	1	1	1
A3	Is there a protection against function creep?	1	3	3

8.15.3.4 Details to the scoring

It is not clear who has access to the collected data. As the systems operate inside legal regulations it is reasonable that data is only used inside regulated groups and that the usage and processing circumstances are regulated. As the analysis of the data is specifically designed for money laundering there should be an inherit protection against function creep.

8.15.3.5 Data protection

The data protection assessment is done for the following typical explanation of the technology:

As not further documentation about the systems exist the rating of the data protection measures are difficult. Access restrictions will prevent unauthorized access to the data. But how the data is protected against internal or external manipulation is unclear. As data is neither stored nor collected by a mobile device, no risk for data extraction exists.

Q. No.	Question	Points	Weight	Score
P1	Is the collected data encrypted or otherwise access protected?	1	1	1
P2	Is the data protected against manipulation?	-	2	-
P3	Is the collection device secure against data theft?	1	1	1

8.15.4 Conclusion

As only little public information about such money laundering detection exists, it is hard to rate how they cope with data protection. As the systems are under the control of legal entities it is reasonable to assume that the collected data is sufficient protected, but without further data that cannot be guaranteed.

8.16 Technology: HEMOLIA

8.16.1 Description (TU Delft + EUI)

HeMOLIA, which stands for Hybrid Enhanced Money Laundering Intelligence, Investigation, Incrimination and Alerts, is an Anti-Money laundering tool under development in the context of an FP7 project that seems to innovate with respect to the above categories. It is an alert and investigation system that combines traditional financial data with telecom data source. It will "hybridize and correlate the Financial and Telecom Planes in order to create richer and more accurate alerts, intelligence and investigation tools, as well as information sharing, both nationally and internationally."
HEMOLIA seems multi-agent, involving Money Laundering fighters (Financial Inspection Unit, LEAs) and Financial Institutes (Banks, Insurance Companies, etc.). It is unclear who will have control of the system.
HEMOLIA tries to mitigate the privacy and data protection concerns that Anti-Money laundering technology raises by bringing "a new model of Push Privacy Preserving Alerts where all FIUs and FIs are pushed with alerts that mark a transaction or customer with a money laundering / fraud risk level or risk probability, yet without disclosing any private data. This model may have outstanding impact on Anti-Money laundering tools because it means that FIs will be alerted based on data of all other FIs and based on Telecom service providers at the national and international level, opening up a new era of Money Laundering and financial crime reporting by FIs to FIUs.

8.16.2 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?
  Yes.

8.16.3 Conclusion

HEMOLIA seems to have high chances to reduce the data protection risk of money laundery protection. Expect the project website http://www.hemolia.eu/ no further information is available to rate the system.

8.17 Technology: Data crawler SCIIMS

8.17.1 Description (TU Delft)

SCIIMS is the acronym for an EU research project on 'smart' data gathering, where test cases include people smuggling and human trafficking. There are several components to this work.
I. A 'smart' search engine is built for crawling through the Internet (*open data or data in transit?*);
II. A data-crawler for databases that are not open to the public;
III. Algorithms are developed that enable automatic data-fusion. That is to say, data coming from different databases or web-sources are compared and matched to create an agglomerate database. This is useful when a particular crime occurs in several databases: the algorithms recognize the fact that they are one and the same crime, associated person or victim;
IV. The programming is user-friendly, the user being an investigator. A key feature is that data-points, or relevant facts, are represented graphically as sets of connected dots (as is sometimes used by policing-analysis tools).
V. An ontology database is used. That is to say that terms are specified in some way (such as specific natural language) in order to create an agreed-upon vocabulary for exchanging information. This makes it easier to match search terms, nomenclature from different databases and establishes a vocabulary between different professions relevant in the crime search.
The exact functioning of SCIIMS is unknown. However, it seems it is a computer program that utilizes advanced programming algorithms for searching, analysing and presenting findings. The information available to us is insufficient to determine how difficult it would be to execute a search. At this stage, it seems reasonable to assume that if individuals leave a digital trail, which is somehow connected to the events that are investigated or the search terms used in the program, the data relating to that individual will be analysed, even when they have no real relationship to the crime. How often this happens and how intrusive the method is, are not clear at this point.

8.17.2 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?
  Unknown.
- Is it possible to map the collected data to an individual person?
  Unknown.

8.17.3 Conclusion

Not enough information about SCIIMS is available to allow a data protection rating. It is likely that the system will process PII but no further details about selectivity, usage and storage are known.

8.18 Technology: Data crawler OMNIFIND

8.18.1 Description (TU Delft)

OMNIFIND is big data-gathering and analysis tool for business purposes. It searches the entire Web for relevant data related to a certain (legitimate) business or product. Similar to SCIIMS, it combines different functionalities, such as sophisticated natural language processing capabilities, search engine, data navigator, and a sentiment analyser. It is a computer program that utilizes advanced programming algorithms for searching, analysing and presenting findings. It is different from SCIIMS in that it is predominantly oriented toward business support and business decisions. Also, it only searches publicly available information. The information available is insufficient to evaluate the complexity of executing a search. People that are connected to products, businesses or clients are probably part of the data-reservoir that the program builds. How often this happens, and how intrusive the method is, is unclear at this point. However, customers' opinions about products are analysed.

8.18.2 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?
  Unknown.
- Is it possible to map the collected data to an individual person?
  Unknown.

8.18.3 Conclusion

OMNIFIND is not developed as a surveillance technology but as a big business search engine. It is reasonable that it processes PII next to enterprise data. Its potential usage as surveillance system is not likely.

8.19 Technology: Cellular Phone Location Tracking

8.19.1 Description (EUI)

To send and receive calls, text messages, or e-mail, cell phones communicate with radio towers, known as cell towers. The cell towers are distributed throughout a coverage area; cell phone users are often in range of more than one. By comparing the phone signal's time and angle of arrival at several cell towers, the location of the broadcast can be figured out. This is known as radio triangulation. The more densely placed the phone towers, the more accurate the location data will be. This location information, originating as it does from the physical cell towers, is often called "cell site information." For the purposes of this assessment the review considers the use of the aforementioned technology (cell tower triangulation), rather than a wider scope that might also cover smartphone devices and the capabilities therein whereby applications can determine their location by, inter alia, means of GPS or proximity to Wi-Fi routers. It is to be noted that while the location tracking of a smartphone using GPS may be more accurate than traditional cell tower triangulation, the user has more control of the situation as location tracking can be turned off without losing the functionality of the phone itself. Hence, traditional cell tower triangulation may be more intrusive than GPS location tracking.

8.19.2 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?
  No.
- Is it possible to map the collected data to an individual person?
  Yes, when identity of phone owner is known, effective tracking is possible

8.19.3 Assessment Results

Here the detailed assessment results of the technology are listed.

8.19.3.1 Data collection

Q. No.	Question	Points	Weight	Score
C1	Is the collection of data selective?	2	3	6
C2	Is the amount of collected data from the subject minimized?	1	1	1
C4	Is the collection done overtly or covertly?	0	1	0

8.19.3.2 Details to the scoring

The legitimate and typical use of phone tracking is the tracking of single subjects. In this scenario the measure is highly selective what results in good scores. As mentioned earlier using the technology to track large number of people would result in other scores. Only the location of the phone is recorded so the data is minimized to the specific need but completely covert.

8.19.3.3 Data access and use

Q. No.	Question	Points	Weight	Score
A1	Who has access to the data?	1	2	2
A2	Is there a clear regulation who is allowed access under which circumstances?	1	1	1
A3	Is there a protection against function creep?	0	3	0

8.19.3.4 Details to the scoring

Only a limited amount of people have access to the data as it is not publicly available. Inside law enforcement agency organizational measures will regulate which employee is allowed to access the data and limit the usage to specific task. Most likely no protection against function creep will be present.

8.19.3.5 Data protection

The data protection assessment is done for the following typical explanation of the technology:

A typical system to evaluate phone tracking will have an access control system to prevent unauthorized people from using it. As the data is stored at an law enforcement agency and not on the phone itself, no risk for data extraction on the capture device exists and the data is reasonable protected against external manipulation.

Q. No.	Question	Points	Weight	Score
P1	Is the collected data encrypted or otherwise access protected?	1	1	1
P2	Is the data protected against manipulation?	1	2	2
P3	Is the collection device secure against data theft?	1	1	1

8.19.4 Conclusion

In the term of data protection mobile phone location gets a good score. One potential danger is function creep and a broad usage of a measure that should only be used in a highly selective manner.

8.20 Technology: Mobile Phone Tapping

8.20.1 Description (EUI)

It is assumed that 'mobile phone data tap' pertains to the metadata relating to calls made and received available to cellular service providers that provide a record of a customer's phone calls: the number dialed, the duration of the call. Data relating to the locality of the handset would also be available, but is otherwise covered in the analysis 'Location tracking of cellular phones' elsewhere. In the present context 'phone data' does not refer to other information available by directly accessing the device itself (providing access, for example, to contact data held on either on the SIM card or the hardware device itself). Actual interception of the phone calls (content data) is not addressed in this assessment.
A wider scope for this assessment might necessitate a review of conducting a 'tap' of more complex cellular phones – devices able to run a plethora of different applications (i.e. smartphones); the capabilities of which would warrant a much broader analysis of the data made accessible by the surveillance.

8.20.2 Pre-Assessment screening result

- Is the surveillance technology collecting, processing or evaluating personal identifiable information (PII)?
  Yes.

8.20.3 Assessment Results

Here the detailed assessment results of the technology are listed.

8.20.3.1 Data collection

Q. No.	Question	Points	Weight	Score
C1	Is the collection of data selective?	2	3	6
C2	Is the amount of collected data from the subject minimized?	0	1	0
C4	Is the collection done overtly or covertly?	0	1	0

8.20.3.2 Details to the scoring

As the surveillance measure of phone tapping is done for specific subjects it is highly selective. The collected data is not minimized. The phone company delivers only a limited amount of data, i.e., who was called for how long. To achieve minimization it would be desirable to filter the data for specific numbers or countries of origin. As the measure is completely covert, there is no transparency for the affected person.

8.20.3.3 Data access and use

Q. No.	Question	Points	Weight	Score
A1	Who has access to the data?	1	2	2
A2	Is there a clear regulation who is allowed access under which circumstances?	1	1	1
A3	Is there a protection against function creep?	0	3	0

8.20.3.4 Details to the scoring

Only a limited amount of people gets access to the data as it is not public available. Inside law enforcement agency organizational measures will regulate which employee is allowed to access the data and limit the usage to specific task. Most likely no protection against function creep will be present.

8.20.3.5 Data protection

The data protection assessment is done for the following typical explanation of the technology:

A typical system to evaluate phone tapping will have an access control system to prevent unauthorized people from using it. As the data is stored at a law enforcement agency and not on the phone itself, no risk for data extraction on the capture device exists and the data is reasonable protected against external manipulation.

Q. No.	Question	Points	Weight	Score
P1	Is the collected data encrypted or otherwise access protected?	1	1	1
P2	Is the data protected against manipulation?	1	2	2
P3	Is the collection device secure against data theft?	1	1	1

8.20.4 Conclusion

In the term of data protection mobile tapping gets a good score. One potential danger is function creep and a broad usage of a measure that should only be used in a highly selective manner.