FP7-SEC-2011-284725

SURVEILLE

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

SURVEILLE Deliverable 2.6 Matrix of Surveillance Technologies

Due date of deliverable: 31.07.2013
Actual submission date: 31.07.2013

Start date of project: 1.2.2012 Duration: 39 months

SURVEILLE Work Package number and lead: WP02 Prof. Tom Sorell (University of Warwick)

Author(s):

The UW team: John Guelke, Tom Sorell and Katerina Hadjimatheou
The EUI team: Martin Scheinin, Jonathan Andrew, Juha Lavapuro, Tuomas Ojanen, Maria Grazia Porcedda and Mathias Vermeulen
The MERPOL team: Brian McNeill
The TU Delft team: Coen van Gulijk, Simone Sillem, Pei-Hui Lin and Bert Kooij

Matrix of Surveillance Technologies

Table of contents

1. Introduction

In this paper we present a survey of surveillance technologies through the development of a multidimensional matrix. The matrix reflects (a) usability, understood in terms of effectiveness, cost, privacy-by-design features and overall excellence, (b) ethics, and (c) intrusiveness into fundamental legal rights.

Although assessments of one of these different aspects will sometimes have implications for assessment of another, they are conceptually distinct. A technology can be useful and usable towards a surveillance goal, but its use can nevertheless be morally problematic or intrude on fundamental rights. Furthermore, technologies can raise substantial ethical concerns not covered by law, and uses of technology that are prima facie morally justifiable can nevertheless be inconsistent with a state's human rights commitments or constitution.

The assessment in this deliverable is organised around a fictional but realistic scenario describing a police investigation. This scenario was constructed by the police partner in the SURVEILLE project, MERPOL. The scenario tracks the developments in a serious crime investigation where the deployment of various surveillance technologies is contemplated across 15 stages.

The technological assessment builds on previous SURVEILLE work in Deliverable D2.1, which surveyed 43 technologies and introduced a range of considerations relevant to technological assessment. D2.6 narrows down this wider range to focus on 14 technologies used in a typical serious crime investigation, and demonstrates how technological assessment can be summarised and related to normative assessment of actual dilemmas facing investigators and policy makers.

The ethical assessment builds on previous SURVEILLE work in Deliverable D2.2, and in particular its analysis of what features of crime justify what we term 'morally risky' investigatory methods. Morally risky action is action that ought not to be done under normal circumstances – action that is prima facie morally objectionable. For example the use of coercive force is usually objectionable – it is prima facie wrong to push someone to the ground. However, the risk of harm incurred by this action is justifiable if this is the only to prevent a person from being hit by oncoming traffic. Certain surveillance technologies are so intrusive that their use is overwhelmingly reserved for policing authorities alone. Even then there is a presumption against the taking of moral risk unless the seriousness of the crime investigated merits it. In section 3, these considerations, outlined in Deliverable D2.2, are related to particular technologies and a realistic police investigation.

The legal analysis builds upon previous SURVEILLE work in Deliverable D2.4 that outlined the way in which surveillance technologies intrude on fundamental rights. Deliverable D2.6 applies this work to specified uses of the selected technologies in the context of the policing scenario.

In section 2.1 the technologies surveyed in the matrix are briefly described. In section 2.2 the matrix is presented, with its assessment of usability, ethics and fundamental rights. This section also includes the main conclusions from the three assessments. Section 2.3 explains the methodologies for the three modes of assessment; section 2.4 includes further discussion of the scoring in the matrix, highlighting technologies that score well in one or more categories, but badly in another. The ethics section of the matrix reflects principled considerations that weigh in assessing a technology as more or less morally objectionable, coding dangers as moderate (green), intermediate (amber) or severe (red). The ethical considerations are relevant to the use of the technologies as specified in the scenario but they concern the use of the selected technologies in general and not only in the context of the scenario. The fundamental rights considerations calculate scores out of 16 for the intrusion into different fundamental rights represented by the use of the technology as proposed in the scenario. Usability assessments of the technologies are scored out of 10, summarising an assessment of the technology's performance in terms of effectiveness, cost and privacy by design.

Section 3 introduces an illustrative scenario for a serious crime investigation where a number of technologies surveyed in the matrix might be used for specific purposes. In 3.1 there is a detailed commentary on the ethical and fundamental right considerations facing investigators at each stage of the investigation – here we see how the ethical principles identified in relation to the technologies restrict their permissible use in practice, and how these compare to the legal analysis of the intrusions on fundamental rights, the rationale for which is explained and justified.

2. A Matrix of Surveillance Technologies

2.1 Description of technologies (TU Delft)

A wide variety of technologies have been listed for examination in SURVEILLE Deliverable 2.1. The following technologies — a subset of those mentioned in D2.1 – are included in the matrix. They have been chosen for their perceived relevance to counter-terrorism and serious and organized crime operations by the police, in accordance with the policing scenario outlined by MERPOL. The following sub-sections summarize in layman's terms the most important defining technological elements of the technologies analysed.

2.1.1-3 CCTV and digital photography

Closed-circuit television (CCTV) is a setup of video cameras that transmit a signal from a specific place to a limited set of monitors. Today's high-definition 'smart' CCTV-cameras have many computer-controlled technologies that allow them to identify, track, and categorize objects in their field of view. Video Content Analytics (VCA) can also be used to detect unusual patterns in an environment, such as anomalies in a crowd of people.

CCTV technology can also be paired with a Facial Recognition System: a computer application that is able to automatically identify a person from a video source.

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. CCTV images and video can be transmitted via the internet or a private network.

2.1.4-8 Audio surveillance devices

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 analogue 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 consist of only a few electronic elements, 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 on-board digital audio signal processing to enhance the quality of the sound.

Cell-phone audio surveillance makes use of an ordinary cell phone, equipping it with a device that enables an external connection and tracking of all conversations made over that cell phone. Together with the installed GPS system, the location of the caller can be monitored.

2.1.9. Video Camera Mounted on Platform Micro-Helicopter

A micro-helicopter is the smallest type of UAV or unmanned aerial vehicle. A micro-UAV can be combined with one small video camera. Its operating range is small; typically an operator is in close proximity of the vehicle. The range and payload capabilities of UAV's vary. The UAV itself is not a surveillance instrument but a platform for carrying surveillance instrumentation.

2.1.10 AIS system (Automatic Identification System) for ships

The AIS system (Automatic Identification System) is a complex system to support safe transport on waterways. Seagoing ships are obliged to transmit their type (general cargo, tanker, coaster, etc.), GPS-position, heading, speed, destination, together with a time stamp of the transmission and a unique identification number (MMSI, Maritime Mobile Service Identity) via VHF radio frequencies. Often additional information is transmitted such as ship length, draught and sometimes the type of cargo. Typically, this information is transmitted every 3 seconds. The information can be received by other ships in the vicinity or by coastal receivers.

2.1.11 Explosives detection near harbour

An explosives detector is mounted on an ROV (Remotely Operated Vehicle). In this context, an ROV 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 suspicious objects and then remotely analyse the contents of the object.

2.1.12 Gas chromatography mass spectrometry (GC/MS)

This is an important technique in the detection and identification of both bulk drugs and trace levels of drugs in biological samples. GC-MS has been widely heralded as a "gold standard" for forensic substance identification because it 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.

2.1.13. Eqo security scanner ("full body scanner")

Smiths' eqo security scanner ("body scanner") is a millimetre-wave body imaging scanner that 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 a 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. These video-style images can be displayed as rotatable images or can be further analysed electronically.

2.1.14 Luggage Screening

Security screening of luggage or cargo is a standard practice, in particular when such items travel through air but also more generally. Traditionally, X-ray machines using radioactive emissions have been used to locate and identify metal items. They remain in use together with other equipment, for instance Explosive Detection Systems (EDS) and Explosives Trace Detection (ETD) for explosives detection, and bottled liquids scanner (BLS) screening systems. New generation bottled liquids scanner systems have the ability to detect a wider range of explosive materials and use light waves to screen sealed containers for explosive liquids. If a bag or other item requires additional screening, it may be automatically diverted to a resolution room where security officers will inspect it to ensure it doesn't contain a threat item.

2.1.15. Money laundering technology

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:

- Wire transfer screening to determine where to target further investigations,
- Knowledge sharing to disseminate profiles of money laundering activities quickly, reliably, and in a useful form,
- Knowledge acquisition to construct new profiles for use during screening,
- Data transformation to produce data that can be easily screened and analyzed.

2.1.16-17 Data Analysis Tools

Data analysis tools to examine large data sets on the internet or in data communication to find certain pre-defined classifiers are widely used in crime fighting and anti-terrorism surveillance. In general uncertain intelligence information from the Internet or from other data communication has to be interpreted, integrated, analyzed, and evaluated to provide situational awareness, using situational and threat assessment methods.[1]

Social Network Analysis (SNA) is a method of statistical investigation of the patterns of communication within groups. The basic concept of the method is the hypothesis that the way members of a group communicate with each other and members of other groups reveals important information about the group itself.

[1] Recent revelations over the US NSA's collection of telecommunications metadata have also highlighted the central role of this kind of technology. So much data is collected that it can only be made use of via data analysis tools – see for example http://www.nytimes.com/2013/06/09/us/revelations-give-look-at-spy-agencys-wider-reach.html?pagewanted=all&_r=0

2.1.18-19 Mobile phone tap

Phone tapping or wire tapping is the monitoring of telephone calls and Internet access by covert means. Mobile phone tapping usually requires phone-tapping software that needs to be installed as an invisible application on a 'smartphone' (which usually requires manual installation on the phone itself). Once such software is installed nearly all information on the phone can be accessed, including but not limited to: tracing calls, receiving copies of text messages, access to the contact list, view Internet sites that were visited, receiving copies of photos, GPS tracking, listening to both sides of a telephone conversation and recording sounds in the environment when the telephone is not operated. The software can be bought from the Internet and can be as cheap as 60 dollars.

2.2 Combined Matrix

Heretofore there follows (on page 8) a matrix of surveillance technologies that reflects assessments of usability and of the risks of violating both ethical standards and fundamental rights. This is represented by way of numerical scores awarded in the usability and fundamental rights assessments and by a red-green-amber colour code in the ethics assessment. Although the matrix may provide a basis for a general, all-things-considered assessment of surveillance technologies covered by it, it should be emphasized that this first version assesses the use of specific surveillance technologies in the context of a fictional but realistic and complex crime investigation, developed by MERPOL. The police investigation scenario will be presented and discussed in Section 3 that follows. In total, 14 technologies are surveyed, all drawn from the initial survey of surveillance technologies carried out in SURVEILLE deliverable D2.1 by TU DELFT. These technologies feature as options for use by police in the scenario.

MATRIX							
		HUMAN RIGHTS AND ETHICAL ISSUES					
		Moral risk of error leading to significant sanction	Fundamental right to protection of personal data	Fundamental right to privacy or private and family life (not including data protection)	Fundamental right to freedom of thought, conscience and religion	Freedom of movement and residence	Moral risk of damage to trust and chilling effect
TECHNOLOGY AND USE	USABILITY			Moral risk of Intrusion			
1. Visual spectrum dome– zoom, tilt, rotate (public place – used overtly)	6		2	1			
2. Visual spectrum dome– zoom, tilt, rotate (public place – used covertly)	7		8*	2			
3. Covert photography in public place	9		8*	2			
4. Sound recording bug in target's home address.	8		16*	16*			
5. Sound recording bug in target's vehicle.	8		8	6-12			
6. Sound recording bug on public transport used by target.	3		8*	¾*			
7. Sound recording bug in police vehicle transporting target following arrest.	4		8	2			
8. Sound recording bug in target's prison cell.	5		8	4-8			
9. Video camera mounted on platform micro helicopter	6		¾	4-8*		3	
10. AIS ship location detection and identification	5		0	0			
11. Explosives detection near harbor	4			0-¾			
12. Gas chromatography drugs detector	8			0-¾			
13. Whole body scanner eqo	6		0	3			
14. Luggage screening technology	7			0-¾			
15. Money laundering technology	7		8	8	1 ½		
16. Networked data analysis	7		3	2			
17. Data transfer analysis (name recognition) technology	6		8	8	1 ½		

18. Location tracking of cellular phones	7		6	6		2	
19. Mobile phone tap	8		3	8*			

Scores for **usability** run from 0-10, 0 representing the least usable, and 10 the most usable technology. Fundamental rights intrusion scores run from ¾-16, ¾ representing the least problematic interference with fundamental rights, 16 representing the most problematic intrusion. The addition of an asterisk* to the fundamental rights scores indicates that significant third-party intrusion is identified, resulting in a need to justify the surveillance not only as proportionate in relation to the target but also as justified in relation to third parties. Ethical risk assessments are expressed via a colour coding system. No colour is used where the ethics assessment found no risk at all (or a negligible ethical risk). Green indicates a moderate ethical risk, amber an intermediate, and red a severe one.

The main conclusions that in the context of the scenario and the matrix can be drawn from the combination of usability (technology), fundamental rights (law) and moral risk (ethics) assessments of the 19 usage situations of the 14 surveillance technologies can be formulated as follows.

Firstly, there are 7 situations where the surveillance appears as *justified* in respect of a combination of the three different assessments. They are the overt use of CCTV, AIS ship location detection, explosives detection, drug detection by chromatography, body scanners that do not present an image of the actual person, luggage screening, and analysis of open (publicly available) internet data. The security benefit obtained by these methods, represented by the usability score, varies from 4 to 8 (on the scale of maximum 10) with no major fundamental rights intrusion or major ethical risks. One caveat that has to be made also in relation to this category of surveillance technologies is that it must nevertheless be verified that a proper legal basis exists for their use, i.e. that the authority to use these surveillance methods is based on precise and publicly available law. The same caveat will of course apply also in relation to the other categories to be discussed below. A second caveat is specific to the use of open data. While the collection of individual, discrete pieces about a person may not have a strong fundamental rights impact, the aggregation of various types of (unrelated) open sources (from different contexts) in order to build a profile of a person can have a serious fundamental rights impact.

A second group consists of 3 situations where the combination of the three assessments in the form of a matrix gives the outcome that the use of the particular surveillance method in the context of the scenario would be *suspect,* even if one cannot come to a definite conclusion that it cannot be justified. These are covert photography in public space, money laundering detection technology and analysis of Internet data by data crawlers. The usability score varies from 6 to 9, signifying a somewhat higher average security benefit than in the case of the 7 unproblematic technologies. However, the significant risk of intrusion into fundamental rights of third parties appears to outweigh the security benefit of covert photography in a public place. As to the two other technologies in this group, it is the degree of intrusion into the fundamental rights (privacy and data protection) of the actual target that makes them suspect. As the fundamental rights score and the usability score in all three cases are quite close to each other, and as the ethical risks are not particularly high, it can nevertheless be concluded that judicial authorization would make the surveillance justified in these three cases.

A third group of surveillance technology usage situations includes 4 cases where the comparison between usability (security benefit) and fundamental rights intrusion is similar than in the second category, making the surveillance suspect and potentially legitimate if judicial authorization is given. The difference compared to the second group, however, is the identification of significant ethical risk. The four cases are the placement of a sound recording bug in the suspect's vehicle, the use of a micro helicopter for aerial surveillance, location tracking of cellular phones and tapping of mobile phones for retrieving metadata, including a register of the calls or text messages placed or received. The usability score in all four cases is relatively high (from 6 to 8) but so is the fundamental rights intrusion (from 6 to 8 or even 12 when the most deeply affected fundamental right is looked into). Due to the high level of third-party intrusion in two of the cases (micro helicopter and mobile phone metadata tap) and high moral risk in all four cases, here identified as a *highly suspect* category, it is questionable whether even judicial authorization could make the surveillance acceptable. Another way to formulate this conclusion is that the judiciary should be hesitant to authorize these measures if requested, due to the fundamental rights intrusion, third party effect, and moral risk. In some cases it may be possible to mitigate the adverse consequences to reach a solution where judicial authorization would make the surveillance legitimate. Restrictions in time and place in the use of the surveillance, privacy by design features built into the technology for instance to avoid third-party intrusion, or proper representation of the interests of the targeted person in the judicial authorization process may be among the solutions.

The remaining 5 usage situations of surveillance technologies can be identified as legally *impermissible* for various reasons. In the case of covert use of CCTV the outcome flows from the fundamental rights intrusion score (8) narrowly outweighing the clear security benefit (7), but combined with a high level of third-party intrusion. It can be noted that covert photography in a public place fell in the second, suspect, category above, simply because of its higher usability score. The outcome is the same for the placement of a sound recording bug in the suspect's home. The security benefit is quite high (8) but here the level of fundamental rights intrusion is even higher (16), coupled with significant risk of third-party intrusion and also high moral risk. This is a clear case where the matrix suggests that even judicial authorisation cannot justify the surveillance measure and should therefore be denied. As for the placing of a sound recording bug in either public transport (a bus), or in a police car, or in the suspect's prison cell - all three represent a clearly lower level of intrusion into fundamental rights. As, however, also the security benefit is dramatically lower (between 3 and 5), it is with a clear margin outweighed by the fundamental rights intrusion score (8). In all five cases also intermediate or high moral risk was identified. It is suggested that in the case of these 5 situations even judicial authorization could not make the surveillance justified, either due to third-party intrusion, the intensity of the intrusion into the suspect's rights, or the limited security benefit obtained through the measure. Quite often the conclusion to be drawn would be to look for an alternative surveillance method that would yield either a higher usability score or a lower fundamental rights intrusion score (or ideally both), and in addition would not raise a flag of significant moral risk. The placing of the 5 situations in the category of impermissible surveillance, in the context of the scenario, does not mean that the use of the same technologies would by definition always be legally impermissible.

It is to be noted that the assessment was made in the context of a crime prevention/investigation scenario that was neutral in relation to the applicable legal system and the characteristics of the targets, and did not include identifiable third parties. Minor adjustments may be needed to take into account these additional factors. That said, the multidimensional matrix developed here by the

SURVEILLE consortium is a promising step towards developing a methodological tool to assess the all-things-considered costs and benefits of various surveillance technologies to be used for combating crime.

The methodology for arriving at these scores is outlined in section 2.3, immediately below. Then, in 2.4, the matrix is discussed in greater detail, identifying a number of cases where technologies score well on one dimension, but poorly on others.

2.3 Methodologies

2.3.1 Scoring usability

The scoring methodology developed by TU Delft assesses usability on the basis of four factors: effectiveness, cost, privacy by design and excellence. The assessment of the first three of these, effectiveness, cost and privacy by design, in turn relies on three further factors, to give ten factors in total, each receiving a mark of 1 or 0, to give the score for usability from 0-10, 0 representing the least usable, and 10 the most usable technology.

'Effectiveness' in the TU Delft scoring system refers to the technology's ability to increase security by carrying out a specified function within the relevant context.[2] The assessment of effectiveness relies on the three further factors of delivery, simplicity and sensitivity.

'Delivery' refers to whether or not the equipment yields a useful outcome when used correctly. Surveillance technologies vary considerably in their function – sometimes the useful function can be defined narrowly in terms of the detection of a specific prohibited object, such as a weapon, or a contraband substance. Sometimes the useful outcome will refer to gaining access to a private space to assist with ongoing intelligence gathering. On other occasions it may simply refer to providing useful leads for further investigation. Delivering a useful outcome, however, does not imply that the technology is not susceptible to error (an issue addressed by the factor of 'sensitivity', discussed below). Furthermore, a technology may 'deliver' successfully in one context, but fail to do so in another (for example the listening equipment is judged to 'deliver' planted in the suspect's home, but not when placed on public transport).

Simplicity refers to structure and ease of operation. Other things being equal, simpler technologies are more effective. The involvement of more than one external expert or stakeholder is an example of something that might make a technology too complex to score for simplicity. In both the case of 'delivery' and 'simplicity', the criteria for scoring '1' is either evidence of past success, or the fact that that it is reasonable to expect that success is achievable. In the absence of either, the technology scores '0'.

Sensitivity refers to the likelihood of error. Technologies that are awarded a '1' in this category provide information that is clear as well as accurate, and that is not susceptible of multiple interpretations. Where there is evidence that a technology is prone to error it scores a '0', and if there is no evidence available of its clear outputs it also scores '0'. Only if there is evidence of its

[2] "*Effective*: the technology has the technical capacity to deliver increased security, and when employed for a defined goal within the necessary context (good location, trained operators, a larger security system, etc.) achieves the intended outcome." Annex 2.

precise and accurate output does it score '1'. The three scores for 'delivery', 'simplicity' and 'sensitivity' are added to give a score for 'effectiveness' out of three.

The second category contributing to the overall score for usability is cost. This refers to the different ways in which the financial costs of surveillance technology vary. The score for 'cost' is also determined on the basis of three factors: 'purchase cost', 'personnel requirements' and 'additional resources'. Purchase cost is the upfront price of the equipment and associated systems needed to run it. Both identifying prices and selecting a criteria for costliness are problematic. Prices for the same technology will vary for one thing. And more substantially budgets available to policing authorities will vary by jurisdiction. Necessarily a nominal scoring system such as that used for the matrix can only provide limited insight into this issue. Technologies costing €50,000 or more, score a '0', and technologies costing less score a '1'. Personnel requirements refers to the number of people who are needed to operate the equipment within the organisation carrying out the surveillance. Two or less scores a '1', three or more scores a '0'. 'Additional resources' refers to whether personnel external to the organisation are required for operation – whether commercial partners or vendors, which represents a further source of financial expense. If a third party is involved, a '0' is scored. If not, it scores '1'. The score for these three factors are added together to give a score for cost out of three.

The third category contributing to the overall score for usability is privacy by design. The score for this category relies on scores for three further factors: 'observation of persons', 'collateral intrusion' and 'hardware and software protection'. 'Observation of persons' refers to whether the surveillance technology is used to observe people, as opposed to simple objects or substances. Other things being equal, technologies that observe objects or substances are better than those that observe people. Technologies count as observing people when they monitor or record images of individuals, their behaviour or their voices, resulting in a score of '0'. Technologies that record or otherwise surveille either objects, substances, or data score '1'. 'Collateral intrusion' refers to the likelihood of surveilling people beyond the intended target. Technologies that monitor or record only the intended person(s) score '1', technologies that surveille more than the intended target score '0'. 'Hardware and software protection' refers to the difficulty of building in 'privacy by design' features. If it is difficult to do so, it scores a '0'; if it can be done easily it scores a '1'. The score for these three factors are then added to give a score for 'privacy by design' out of three.

One final factor unrelated to the others is 'excellence'. The criteria for excellence is that the technology has proven its usefulness beyond all reasonable doubt, such as is the case with iris-scans and DNA sampling for personal identification. Technologies qualifying as 'excellent' have been proven their usefulness both scientifically and in application to actual crime prevention and investigation. If the technology's excellence has been proven in this way, it scores a '1'. If it has not, it scores a '0'. This score is then added to the composite scores for 'effectiveness', 'cost' and 'privacy by design' to give the overall usability score out of 10.

2.3.2 Scoring Ethics

The colour coding for the moral risks is derived from the tables visualising moral risk developed in the DETECTER project's 10 Detection Technology Quarterly Updates,[3] based on analysis in DETECTER Deliverable D5.2 and discussed in SURVEILLE Deliverable D2.2.

[3] See for example DETECTER Deliverable D12.2.10 available at www.detecter.bham.ac.uk/pdfs/D12_2_10_QuarterlyUpdateonTechnology_10__1_.doc

Invasion of privacy on this view involves penetration of one of three distinct 'zones' of privacy, discussed in SURVEILLE deliverable D2.2, and DETECTER deliverable D5.2.[4] These are bodily privacy, penetrated by close contact, touching or visual access to the naked body; privacy of home spaces, penetrated by uninvited observation in the home or spaces being temporarily used as such, like a hotel room; and private life, penetrated by inappropriate scrutiny of associational life and matters of conscience. Also relevant is the question of whether information uncovered by the initial intrusion is made available to further people, as intrusion is usually made worse by sharing information. Technologies that delete information upon initial use, or do not store information for further viewing preserve the privacy of the surveilled. Cases where the UW team judge technology not to invade privacy at all, or to do so only to a negligible extent, are left blank; moderate intrusions are coded green; intermediate invasions amber; and severe invasions red.

The moral risk of error may derive from any of a number of sources. Firstly, if the information acquired by the technology is susceptible to false positives this will contribute to errors: some information targeted by surveillance technologies is inherently ambiguous and potentially misleading. For example, a private conversation targeted by means of listening devices can easily be misinterpreted.[5] This is distinct from the technology itself producing/generating, or revealing information which may be highly error prone. For example, data mining technologies often involve profiling algorithms that are susceptible to false positives. Some technologies require extensive training and may be vulnerable to errors because of mistakes by the user or viewer. Finally, storage may lead to repeated risks of error as well, either because of risks of data corruption, or simply because a later viewer does not have all the information to put the intelligence stored in its proper context. However the multiple possible sources of error must be considered in the light of whether the person surveilled is subjected to sanction as a result. It is not error in itself that represents a moral problem here. Rather, it is only error that leads to intrusive searches or arrests that is of concern. No risk of error leading to sanction, or a negligible one, results in the category being left blank. A moderate risk of errors leading to sanction is coded green, an intermediate risk amber, and a severe risk red.

The moral risk of damage to valuable relations of trust refers to two categories of social trust eroded by uses of technology. The first category is the trust in policing authorities that may be damaged by what is perceived as excessive, ethically problematic uses of technology.[6] The second category is, interpersonal social trust among the population – damage to this social trust is sometimes referred to as the 'chilling effect'.[7] Damage to both of these kinds of trust result from the perception of at least four morally problematic possibilities on the part of the general public. One, the perception of the intrusiveness of the technology. Two, the perception of error resulting from the technology –

[4] See DETECTER Deliverables D5.2. especially pp. 7-18 www.detecter.bham.ac.uk/pdfs/D05.2.The_Relative_Moral_Risks_of_Detection_Technology.doc and D12.2.1 – D12.2.10 available at http://detecter.eu/index.php?option=com_content&view=section&layout=blog&id=7&Itemid=9

[5] See for example DETECTER Deliverable D5.2., which refers to range of empirical studies on the interpretation of recorded conversations such as (Graham McGregor, in Alan Thomas,1987) and (Graham McGregor, 1990) and (Dore and McDermott, 1982) on the essential role of context in interpreting conversation – which in the case of technologically enabled eavesdropping may not be available.

[6] See, for example: Paddy Hillyard, 1993, *Suspect Community*; Pantazis and Pemberton, 2009; Spalek, El Awa and McDonald, 2008 and Richard English. 2009. *Terrorism: How to Respond* p 141

[7] See, for example: DeCew, 1997, 64 on weakening of associational bonds, contributing to "wariness, self-consciousness, suspicion, tentativeness in relations with others".

that the error-proneness of technology poses risks of the individual being wrongly suspected. Three, the perception that the technology poses risks of discrimination – either that the technology is disproportionately likely to be used against particular groups, or even that application of the technology may be more likely to cast suspicion on particular groups, as is the case for example with data mining technologies which make use of crude profiling techniques.[8] Four, the perception of function creep also contributes to this damage to social trust. No risk of damage, or negligible damage to relations of trust result in the category being left blank, moderate risk of damage is coded green, an intermediate risk amber, and a severe risk red.

2.3.3 Scoring Fundamental Rights

The scores for fundamental rights, given by the EUI team in SURVEILLE, are closely connected to the use of the technologies in the context of the investigatory scenario from MERPOL. EUI provides assessments of the intrusions the proposed uses of the technologies in the scenario cause to fundamental rights. The assessment relies upon a multitude of approaches, including Robert Alexy's theory of fundamental rights,[9] identification of attributes within a fundamental right in order to assess the weight of the rights in context,[10] and analysis of existing case law, both by the European Court of Human Rights and the Court of Justice of the European Union.

Scores are offered for a number of different fundamental rights, with emphasis on the right to the protection of private life (or privacy), on the one hand, and the right to the protection of personal data, on the other hand. Although these two rights are closely interlinked, the protection of personal data is increasingly conceived of as an autonomous fundamental right in the current state of evolution of European law, related to but distinct from the right to respect for private life. This is neatly illustrated by the EU Charter of Fundamental Rights in which data protection has been enshrined as an autonomous fundamental right in Article 8, alongside the protection of private and family life under Article 7.

The concept of private life is a very broad one in accordance with the case law by the European Court of Human Rights, whereas the right to the protection of personal data largely, albeit not exclusively, constitutes one of the aspects or dimensions of the right to respect for private life.[11]

The concept of private life covers the physical and psychological integrity of a person; it embraces aspects of an individual's physical and social identity. Elements such as gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8 of the ECHR. Moreover, Article 8 protects a right to personal development, and the right to establish and develop relationships with other human beings and the outside world. Although Article 8 does not establish as such any right to self-determination, the European Court of Human Rights has considered the notion of personal autonomy to be an important principle underlying the

[8] See for example Moeckli and Thurman DETECTER Deliverable D8.1. especially on the German Rasterfahndung: www.detecter.bham.ac.uk/pdfs/D8.1CounterTerrorismDataMining.doc

[9] Robert Alexy, (2002) *Theory of Constitutional Rights*

[10] For earlier SURVEILLE work, see Porcedda, Maria Grazia (2013), 'Paper Establishing Classification of Technologies on the Basis of their Intrusiveness into Fundamental Rights': SURVEILLE deliverable D2.4, Florence, European University Institute).

[11] See Maria Tzanou, The Added Value of Data Protection as a Fundamental Right in the EU Legal Order in the Context of Law Enforcement. PhD Thesis European University Institute, 2012.

interpretation of its guarantees.[12]

Data protection, in turn, is usually understood as referring to a set of rules and principles that aim to protect the rights, freedoms and interests of individuals, when information related to them ("personal data") is being processed (e.g. collected, stored, exchanged, altered or deleted).

The difference between privacy and data protection is also indicated by the fact that not all personal data necessarily fall within the concept of private life. *A fortiori*, not all personal data are by their nature capable of undermining the right to private life.[13]

Aside from the right to privacy and the right to the protection of personal data, several other fundamental rights may also be affected in many cases by the use of surveillance technologies, including freedom of movement, freedom of thought, conscience and religion, freedom of expression, freedom of association or the right to non-discrimination. As the assessments were made in relation to the crime investigation scenario, a consideration of the impact on other fundamental rights beyond privacy and data protection was necessary only in a few cases. In many other cases a remark was nevertheless made in respect of the right to non-discrimination.

Where a technology (or rather the application of a technology) engages a fundamental right, a score is given from 0 to 16 where the value 0 would signify no intrusion whatsoever. In practice, the lowest given score was ¾ representing the best case or the least interference. In one case the maximum score of 16 was the outcome, representing the worst case or the greatest intrusion. Any score above 10 represents an impermissible interference with fundamental rights – one that cannot be justified by any increase in security that may result from the use. This is because the maximum usability score was 10, and no usability score could outweigh or counterbalance a fundamental rights intrusion above the score 10.

The scores generated for each technology are primarily a result of two factors: first the weight, or importance of the particular fundamental right affected in the context of the scenario, and second, an assessment of the degree of intrusion into that right. Each of these two factors is marked as 1, 2 or 4. A score of '1' represents a low, '2' a medium and '4' a high relative weighting of the fundamental right. A score of '1' represents a low, '2' a medium and '4' a high (or serious) level of intrusion into that right. These two scores are then multiplied to give a score from 1 to 16.

The scored variables (weight of a right and the degree of an intrusion), as well as the individual scores given to them, stem from classifications and concepts used in everyday legal practice and argumentation. For instance, the ECtHR has often held that the actual significance of a right and the respective margin of appreciation it allows for member states, depends on a number of factors including the nature of the Convention right in issue, its importance for the individual, the nature of the interference and the object pursued by the interference.[14] These aspects have been addressed in the scoring. Similarly, the differentiation between rights that have weak, medium, or high weight as well as between low, medium and serious intrusions have analogous counterparts in concrete legal argumentation. To give an example, in *Peck v. the United Kingdom*[15], the ECtHR held that the

[12] Pretty v. the UK (Application no. 2346/02), judgment of 29 April 2002, Reports of Judgments and Decisions 2002–III.
[13] See e.g. Case T-194/04 *Bavarian Lager,* judgment of the Court of First Instance of 8 November 2007, paras 118-119.
[14] See for example, S. and Marper v. The United Kingdom (December 4, 2008), § 102
[15] Peck v. The United Kingdom (January 29, 2003), § 63.

disclosure to the media for broadcast use of video footage of the applicant whose suicide attempt was caught on close circuit television cameras constituted a “serious interference” with the applicant's right to respect for his private life. For the purposes of the matrix, this legal outcome is represented in the matrix assessment by assigning the score of 4 to the assessment of the degree of intrusion.

The two scores provided by the assessment of both the weight of the right and the degree of intrusion are then multiplied to give a score from 1 to 16. This score from 1 to 16 may be reduced by the two multipliers. The first is the reliability of the judgements of the weighting and intrusiveness generating the 1-4 scores. The most reliable assessment has a solid grounding in authoritative case law. In this case there is a scoring of ‘1’, and no consequent reduction of the 1-16 score. Where there was not a solid basis of case law to draw upon, the next reliable basis was a consensus among the EUI team of legal experts. In this case a score of ‘¾’ was awarded. This factor was then multiplied by the 1-16 score, thus reducing the final score by a quarter. The least reliable basis was that of a layman’s opinion, which would result in a score of ‘½’, reducing the raw score by a half. In practice each assessment could be made on the basis of solid case law or expert consensus.

The second multiplier that can reduce the 1-16 scoring is judicial authorisation. This reflects the fact that judicial authorisation mitigates the intrusion. However, certain interferences with fundamental rights are so intrusive that even with judicial authorisation they remain unacceptable. In the scoring, judicial authorisation results in a score of ‘¾’, which is multiplied by the raw, 1-16 score, reducing it by a quarter. In the absence of judicial authorisation a ‘1’ is scored for this category, retaining the original assessment. For example, in the case of the maximum original score of ‘16’, even with judicial authorisation this is reduced to 12 – still above the maximum score of 10 that could be counterbalanced by maximum security benefit. As the analysis is carried out in relation to an unspecified jurisdiction, it could not be assessed whether the law would in each case require judicial authorization. Hence, the question of judicial authorization was left open. In assessing real life cases both the existence of appropriate judicial mechanisms and their effective operation would stand in need of verification.

One important precondition for an interference in a fundamental right being permissible is that it was ‘prescribed by law’, i.e. that there was a proper legal basis for it in the applicable legal framework, typically national legislation regulating the investigation of crime and the powers various authorities possess for it. The requirement of any interference being prescribed by law does not merely relate to the existence of law but also to the quality of the law, including its degree of precision and foreseeability. The absence of proper legal basis would turn otherwise permissible surveillance into impermissible surveillance, whenever there is an interference with fundamental rights, including the right to privacy. As the assessment was not made in respect of a particular jurisdiction, the existence of a legal basis for each use of surveillance technologies could not be determined. Instead, it was assumed that legal basis existed and a score was given under such an assumption. In real life situations, the validity of the assumption would need to be verified.

In the scoring as applied, the maximum score of ‘16’ was the result of a combination of the highest level of intrusion into a fundamental right that was of highest weight in the context under analysis (4 x 4 = 16). Although not applied in practice when assessing the scenario, the maximum score of 16 could also be awarded directly under the construction that the surveillance under assessment intruded into the inviolable or essential ‘core’ of a fundamental right. This is because it is one of the analytically distinct preconditions of the permissibility of any interference with a fundamental right

that the restriction in question leaves unaffected the essential core of the right. Further, as some fundamental rights, such as the prohibition against torture, are absolute in the meaning that they do not allow for any restrictions, the maximum score of 16 could also be awarded directly when an intrusion into an absolute right is identified.[16] However, in this deliverable neither of these cases was identified in any of the situations analysed but the scoring could always be given through the two-step separate assessment of the weight of the right and the intensity of the intrusion.

Finally, the scenario as described contains instances where there is potential for 'third-party' or 'collateral' intrusion of individuals beyond the intended target. Therefore these cases would require further and separate legal analysis as to their permissibility, and/or how such third-party intrusion could be prevented. This analysis would require detail beyond the scope of the original scenario. Those cases where a significant risk for third party analysis has been identified are marked with an asterisk (*).

2.4 Discussion of the Matrix

The fundamental rights and ethics analyses should be understood as serving complementary but distinct purposes in the matrix. The former is a legal assessment of uses of the technologies by police forces in the context of an investigation. This analysis is therefore necessarily more tightly bound to the context of the police investigation scenario given below. Both assessments reflect the uses of technologies specified in the scenario. However the ethics analyses technology descriptions in the abstract and not just their uses in the scenario. In part this is due to the difference between the approaches of ethics and law to the technologies.

Ethical and legal analysis overlap to an extent – the legal right to privacy and the moral interest in privacy, for example, share certain features and arguably protect some of the same values: especially that of having an unobserved sphere to develop independent and autonomous thought. This overlap is reflected in the matrix by their sharing a column. The two other moral risks mentioned overlap with human rights not analysed in the matrix. The moral risk of error is related to the fundamental right to non-discrimination. Error-prone technologies can contribute to discrimination when they disproportionately target particular groups. Discrimination can also contribute to error if prejudiced users decide to deploy technologies, or report suspicions without justification. Some human rights have no overlap with any single moral risk, such as the right to data protection. To the extent that data protection can be cashed out in terms of a moral duty, it is likely to be covered by duties to respect others' privacy, or to stop preventable harm resulting from information sharing.[17]

It is important that surveillance technologies are not used in ways that either violate law or violate ethical norms. Taking only the law into account is not enough, because there are a wide range of possible uses of surveillance technologies that most people would agree are wrong, even if there are reasons why they should not be made illegal. An example of this can be seen in the response to revelations about mass surveillance of Internet data on the part of the American NSA and British GCHQ in 2013 where one argument has been that the surveillance might have been legal under domestic law but was nevertheless unethical (and arguably also in violation of international human rights law). Likewise, ethical assessment is by itself insufficient, because some things that are not

[16] For a discussion of the 'core' of fundamental rights and of absolute rights, see SURVEILLE Deliverable D2.4 and the sources identified there.

[17] In some cases this duty might correspond to the moral risk of error.

obviously or at first glance questionable morally are in fact illegal, and the potential developers and users of the technologies discussed here need to know whether their activities are in accordance with the law.

However, ethical standards and legal standards are distinct. Although law will often be guided by ethical standards, it is widely recognised that laws can be inconsistent with moral standards. In these circumstances it is usual to talk about an immoral or unjust law. This demonstrates that ethics represents a broader normative perspective than law, one from which law itself may be subjected to criticism. Ethical standards also operate over a much wider range of conduct than law. Ethical standards operate in everyday life as well as in our professional capacities. While legal standards will rightly be silent on whether or not we are permitted to tell lies in everyday life, there are always ethical reasons not to lie, even if in the end those reasons are outweighed by other reasons. Law may prohibit lying in particular rarefied circumstances – such as in contracts, for example – but will not provide a general, principled prohibition. Ethics provides principles justifying certain actions and condemning others to equip us for the many dilemmas we face in both everyday and professional life. Law fulfils a different, more directly practical objective. For example, law will be crucial to what kind of response is possible, as it determines what the individual is entitled to in the way of redress, specifically what claims for redress will be underwritten by the state.

However, not all criticism will rely on the claim that laws have been broken. Beyond the issue of law, criticisms may be made on the basis of an ethical claim: that a particular action breached a moral norm and that people ought not to do it, whether the law is silent on the matter or not. Ethical claims may also be used to highlight gaps in the law as it stands, and as the basis for suggestion for law reform – that because a particular action is immoral that this is a good reason for the state to prevent it. It is generally recognised that by itself, the fact that conduct is morally questionable is not always a good reason for the state to be involved, but sometimes it will be, and so ethical analysis will be relevant to questions of law reform.

The question of what is legal is determined state by state, and in democratic institutions on the basis of the deliberation of national legislatures whose members are selected by its citizens, but this is not the whole story. A national constitution or international human rights instruments to which a state is a party exist as a framework for the acceptability of proposed or existing legislation. Laws that are inconsistent with the constitution or human rights treaties must be amended or scrapped. In many jurisdictions the judiciary can also refuse to apply a law that is in conflict with the constitution or with international or European norms. National constitutions or human rights instruments lay down duties to respect rights. Usually these correspond to fundamental interests – in survival and bodily security, or freedom from fear or hunger, and are realized through the institutions of the state for education, the distribution of health care and courts. If an individual's legal rights are infringed, she may turn to the state for redress. However, laws passed democratically are still criticisable from the perspective of regional or international law, and on the basis of human and fundamental rights norms. Furthermore, human and fundamental rights are considered to be of such widely acknowledged importance as to have universal application, independent of the laws of the state. These rights include those typically threatened by technologies considered in SURVEILLE: the rights to privacy, data protection, freedom of thought, and freedom of association.

In an ideal world the technologies with the highest scores for usability would pose neither ethical risks nor problems for fundamental rights. This is the case with the use of the gas chromatography drugs detector in the scenario, primarily because this is a technology that detects things rather than

people, and thus exposes no individual to harm.[18] However, a number of the most usable technologies score high for both ethical and human rights risk. State authorities claim they need to use surveillance technologies to investigate and prevent serious and organised crime. Uses of technology that invade people's privacy or are susceptible to false positives might be ethically justified in such cases, but there is nevertheless a moral cost. The colour coding offered in the matrix is intended to indicate this moral cost. And the greater the moral cost, the rarer and more demanding the circumstances in which it can be ethically justified.

Among the most intrusive surveillance technologies from the point of view of both ethics and human rights is bugging equipment designed for use in cars, homes or hotel rooms. These kinds of listening devices intrude into the space where one is at greatest liberty to act without regard for convention and do as one likes. They may well intrude upon the most intimate details of home life, and conversations with friends and family. Nevertheless, in the right circumstances they can be ethically justified. In a case where there is good evidence to suggest that the target is using the privacy of the home to further life-threatening criminal plans, the high standards for ethical justification of the intrusion are met. Indeed, on most formulations of liberal theory,[19] the state has an obligation to protect the individual from threats to life. The technology in question is likely to be the best, and most effective way of acquiring the intelligence needed to prevent the crime, and its suitability for the task is reflected in the high score it receives under the category of 'usability'. However the human rights law perspective is that this severe intrusion may encroach on the core of the right to privacy, and that at the core of fundamental rights even the highest security benefit cannot justify such an incursion.

Deployment of bugging equipment on public transport is regarded as less objectionable from the perspective of both human rights and ethics. But to say that it is less objectionable is not to say that it is not objectionable at all. Both perspectives register risks, particularly with regard to the right to data protection (where it scores a high '8'), and moral risks of error, intrusion and damage to trust (all rated as 'intermediate'). However, such deployment is much less likely to yield useful intelligence. This is reflected by its poor score of '3' for usability – the lowest score for all the technologies assessed. This moral cost is unlikely to be worth paying given such a poor return.

The difference of approach of ethics and law is revealed in divergent assessments for another highly effective technology: mobile phone tapping equipment. This receives a high score for its usability, scoring maximum points for its efficiency, and also performing well in terms of cost and privacy by design features. However, while a low cost is good from the point of view of usability, it is also a problem ethically. Because ethics takes individual actions into account, technologies that are readily exploitable by private actors raise ethical concerns. While low cost is a virtue from the point of view of the usability of technologies, the fact that, for example, mobile phone tapping technology is commercially available for as little as 60 dollars (see annex 1), makes it substantially more likely that these technologies will be abused by private individuals for their own voyeuristic purposes. Furthermore, the software installed for these purposes on mobile phones are easily adaptable to additional severe intrusions, such as the interception of text messages, and even remotely activating

[18] DETECTER Deliverable D5.2, p.7, advises as to the principle that technologies that do this are, all things being equal, less objectionable. See: www.detecter.bham.ac.uk/pdfs/D05.2.The_Relative_Moral_Risks_of_Detection_Technology.doc.
[19] This is so both in the tradition of Kant, who like Hobbes identifies preservation of order as a primary obligation of the state, and in that of Locke for whom the obligation is a consequence of the primary obligation of upholding individual rights.

the microphone, essentially turning the mobile phone into a listening device that the target is likely to keep on their person wherever they go. Thus aspects of a technology that make it more usable may in some cases also make it more problematic ethically.

The fundamental rights analysis of the mobile phone tap in this deliverable refers to a much narrower aspect of the interception: the call metadata, revealing for instance the number dialled and duration of call, but not the content. It finds that even tapping this information is highly intrusive, but that its use could be justified by a sufficient security benefit.[20] This conclusion is confirmed by the approach of the ethical analysis which considers the much more expansive (and intrusive) applications. Ethical analysis treats this technology as an even greater threat to privacy than bugging devices, reflecting both the great potential for intrusion and the easy availability of this technology for abuse by private citizens.

One of the possible capacities of mobile phone taps is location tracking, which is treated as a separate technology in the matrix. This technology scores well for usability (if not quite as well as for mobile phone taps) but for that reason the ethics analysis finds it significantly problematic, because of the profound intrusion into private life that it represents, and the possibility – given its wide availability – that it can be used by individuals as well as the authorities. The fundamental rights analysis, similarly finds the nature of the surveillance highly intrusive: indeed more so, as it awards the highest possible score for its intrusiveness with the right to privacy, but this is qualified both by a medium score for the abstract weighting of the right and a less reliable basis in case law than is available in the case of listening devices, for example.[21]

[20] - With respect to the right to privacy, the use of a cellular phone tap can be considered to be an intrusion on a high level, where the monitoring activity may disclose to law enforcement a large volume of information pertaining to a person's private life.
- Access to the records of the use of a cellular phone also provides a party with detailed insight into the individual's patterns of association with others, constituting therefore a further interference in the right to privacy. Thus, the interference as a whole with regard to the right to privacy may be qualified as of a 'high' weighting.
- The protection of personal data in accordance with the guarantees furnished by Article 8 of the ECHR has been considered pivotal to an individual's enjoyment of their private life (*See*: Peck v. the United Kingdom [2003] 35 EHRR, §59). Collecting and analysing the data provided by a cellular phone tap inheres a capacity to furnish information pertaining to many facets of an individual's private life. Elements of the phone tap procedure will constitute automated processing and, as such, the ECtHR has stated that the need for safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes (S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, 4 December 2008, § 105).
- Considering the high level of intrusiveness of a cellular phone tap, the reader should consider that where an interference caused by a surveillance activity may be justified as being necessary in a democratic society it must correspond to a pressing social need and, furthermore, must be proportionate to the legitimate aim pursued Uzun v. Germany (no. 35623/05, 2 September 2010), §78). Thus, in assessing the proportionality of the use of a cellular phone tap one must duly consider whether other comparatively less intrusive methods of investigation could prove sufficient while constituting a lesser interference in the fundamental rights of the individual. (Annex 3.19)

[21] - With respect to the right to privacy, the level of intrusiveness of the use of location tracking can be considered to be significant where the monitoring activity can provide authorities with detailed information not just to movement, but also in respect of daily interactions and choices that can build a detailed pattern of behaviour. Locality therefore reflects more than simply one's physical location, but also a broader range of attributes that provide a high level of granularity pertaining to, for example, an individual's associations with others. Where cellular phones are frequently carried by an individual their tracking may provide the party conducting the monitoring with a extremely nuanced understanding of an individual's daily routine in both in public and notionally private areas (such as the home). Thus the interference may be qualified as of a 'high' weighting.
- The protection of personal data in accordance with the guarantees furnished by Article 8 of the ECHR has been considered pivotal to an individual's enjoyment of their private life: "[T]he Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which

There is another point of divergence in scores for networked data analysis, because the legal analysis focuses on the use in the scenario while the ethics analysis considers a wider range of possibilities. The legal analysis considers the possible use of such a tool in relation to open source information that could be found about a person online. The ethical analysis highlights this as a riskier technology than that application might suggest because it is a tool which frequently makes use of much more intrusive data – such as telecommunications metadata. The coding of this technology as an intermediate risk reflects this possibility.

Notwithstanding these disagreements, the assessments of human rights and ethics overlap substantially – much more than either correlates with usability. The ethics and human rights assessments agree that technologies detecting objects or substances rather than people are less objectionable than technologies detecting or surveilling people. Thus the least objectionable technology on both approaches in the AIS ship detector. The next best technologies from the perspective of human rights and ethics are the two substance detectors. The gas spectrometer drugs detector and the harbour scanner register low marks for their human rights intrusiveness and are assessed as posing negligible moral risks. After this the luggage scanner, which also detects things, is assessed as a similarly low threat.

The body scanner also receives low scores and is assessed as only a moderate intrusion. This might seem surprising given the degree of controversy the issue of body scanners provoked on introduction to airports. However the body scanner considered does not produce an intimate image of the subject's naked body, but rather an outline of a generic human person to highlight areas of the body for further search – reducing the extent to which it surveilles the human body and increasing the extent to which it detects objects or substances.

The next step up in intrusiveness is represented by the variety of different applications of cameras. While the overt use of CCTV is taken to be only moderately invasive, and scores low marks for its intrusiveness into fundamental rights, some other applications are more so. Covert use of CCTV and covert photography in public places both get high scores of 8 for their intrusion into the right to data protection, and the platform micro helicopter mounted camera is a greater intrusion into privacy, scoring between 4 and 8. Both covert use of photography and the use of the camera mounted on a platform helicopter are assessed as intermediate ethical risks.

---

these records are used and processed and the results that may be obtained" (*See*: Peck v. the United Kingdom [2003] 35 EHRR, §59). As has been already been noted, the collation and analysis of location tracking data carries particular risks pertaining to its capacity to furnish highly nuanced inferences – it might thus be constituted to fall within the ambit of 'Special categories of data' where, specifically, data pertaining to time and location of an individual provides a public authority with information of a highly sensitive nature. Furthermore, the ECtHR has stated that the need for such safeguards is all the more necessary where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes (S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, 4 December 2008, § 105).

- The ECtHR case law has affirmed that the notion of being "necessary in a democratic society" in respect of a surveillance activity must be considered to infer that the interference corresponds to a pressing social need and is proportionate to the legitimate aim pursued (Uzun v. Germany (no. 35623/05, 2 September 2010), §78). Thus, in assessing the proportionality of the use of location tracking one must consider whether other methods of investigation that are comparatively less intrusive could prove to sufficiently effective while constituting a lesser interference in the fundamental rights of the individual. (Annex 3.18)

The next most intrusive set of technologies is the range of data analysis technologies. However, the intrusiveness of these techniques varies greatly depending on what information is analysed and on what information is revealed. It should also be noted that there are applications of data mining not considered in the policing scenario, which would score differently. Some techniques, such as 'crime mapping' to identify hotspots for a particular offense, will violate no individual rights and be very unobjectionable, and thus might score better than the data mining techniques considered here. And some that make use of more intrusive information to begin with, such as how often a person emails or telephones particular associates, and do so to profile a person's likelihood of involvement in serious crime, might be more objectionable.

The next most serious intrusion according to ethics is the use of location tracking, which the ethics assessment rates as severely intrusive, and a severe risk of error. As discussed above, the human rights analysis regards it as less of a threat, closer to the level of more intrusive data mining programmes and the use of the camera mounted on a platform helicopter, scoring a '6', a '6' and a '2' for its threat to the right to data protection, privacy and to freedom of movement.

There is more agreement on the intrusiveness of bugging equipment, in particular when it comes to its use in the home, where there is consensus that this is the worst threat to privacy, coded as a severe ethical risk of intrusion, and scoring the maximum '16' for data protection and privacy. Use of such equipment in a vehicle is less intrusive, but still coded as a severe moral risks and meriting high scores of '8' for its risk to data protection and '6-12' for its risk to privacy. Uses of bugging equipment in other, less private contexts, such as public transport, or police custody, still pose risks to privacy and data protection, but to a much lesser extent.

3. Serious crime police investigation scenario

This section describes a selected serious crime (drugs and firearms) investigation, of intelligence received and decisions that have to be made, at different points. The scenario was designed to reflect the increasing complexity over time of an investigation – complexity in numbers of suspects, jurisdictions and resources deployed – and also the pauses and intermissions, which in themselves pose further challenges. The central purpose of this scenario is to contextualize the use of surveillance technologies and to introduce the perspective of a long-term investigation.

Information / Intelligence/ Evidence		Potential Law Enforcement Activity
Intelligence (low grade) suggests that nominal X is engaged in the large scale importation of drugs		**Decide** – Commence research and analysis including open source research on X? **Consideration** – Does this action by Law Enforcement require authorisation(*) or not?

Intelligence suggests association between nominal X with nominals Y and Z and provides detail of their intention to import controlled drugs.		**Decide** – Commence research and analysis including open source research on Y and Z? **Consideration** – Does this action by Law Enforcement require authorisation(*) or not? **Decide** - Consider development of the intelligence through a covert internet investigation? **Consideration** – Does this additional action by Law Enforcement require authorisation(*) or not?
Intelligence regarding nominal Z suggests that they are linked to a firearms supplier in another EU member state		**Decide** - Conduct further and more in-depth research and analysis including open source research on nominal Z? **Consideration** – Does this action by Law Enforcement require authorisation(*) or not? **Decide** - Commence liaison with other EU member state regarding potential firearms supplier? **Consideration** – Is an ILOR required as yet, is this a formal request for intelligence / evidence at this stage, is law enforcement action sought by other member state at this stage? **Decide** – Should law enforcement 'Friend Request' nominals on open source to develop intelligence relating to X, Y, Z and unknown foreign national? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not?

Further intelligence suggests the intention of X, Y and Z is to bring a firearm into the country with the future drugs consignment but no further details as yet regarding date.		**Decide** – Should law enforcement place X, Y and Z under physical observation by Surveillance Team? **Consideration** - What surveillance technology could be deployed? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not? **Decide** - Should the surveillance include the covert use of use of public place (overt) CCTV and photography etc.? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not? **Decide** – Should law enforcement commence financial background enquiries and development of financial profiles on all nominals?
		Consideration - Does this additional action by Law Enforcement require authorisation(*) or not?
For approximately 3 months there is no development in the intelligence or information being received, nor any intelligence or evidence being obtained from the surveillance operation		**Decide** - Should the law enforcement operation continue? **Consideration** - An issue for consideration by the Authorising Officer and investigation team regarding the proportionality, justification and necessity of maintaining covert surveillance.
Surveillance identifies a male believed to be a foreign national who is regularly visiting the home address of Z and appears to be staying overnight. It is suspected that this may be the firearms supplier.		**Decide** - Should law enforcement intensify observations / surveillance on the home address of Z to identify the foreign national? **Consideration** - What surveillance technology could be deployed?

		Consideration - Does this additional action by Law Enforcement require authorisation(*) or not? **Decide** - Should law enforcement consider deployment of covert CCTV and to maintain general surveillance? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not? **Decide** - Should enquiries be progressed / escalated with other EU member state to request specific intelligence and any relevant evidence on the as yet unidentified foreign national? **Consideration** – Is an ILOR required at this stage?
The home address for Z is in a rural location making general surveillance by a team and the deployment of covert CCTV extremely difficult.		**Decide** - Should law enforcement require surveillance to be maintained? **Consideration** - What surveillance technology could be deployed? **Decide** – Consider covert use of drone and / or other air surveillance in order to maintain observations. **Consideration** – Does this additional action by law enforcement require authorisation (*) or not?
Further intelligence is received that the drugs / firearm importation is imminent but there are no further details as to the route to be taken. The source is not likely to be able to assist any further.		**Decide -** Consider use of covert listening device at home address and / or vehicle of Z? **Consideration** - What surveillance technology could be deployed? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not?

		Decide - Should law enforcement start to consider interception of communications? **Consideration** - What surveillance technology could be deployed? **Consideration** – If progressed, on which nominals in this scenario? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not?
Through surveillance it has been ascertained that whilst travelling with the visiting foreign national that nominal Z quite often uses public transport?		Is this action by nominal Z and the unknown foreign national deliberate, in order to maintain anti-surveillance activity? **Decide -** Consider use of covert listening device on public transport? **Consideration** - What surveillance technology could be deployed? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not?
Open source research suggests a link between nominal Z and a crime group engaged in gun crime including armed robbery and a gang dispute involving previous shootings.		**Decide** – does this intelligence justify more intrusive surveillance? **Decide -** Should there be research conducted on the intended recipients of the gun? **Decide -** Does this intelligence create a credible threat to life? **Decide -** When should law enforcement move into taking overt enforcement action? **Consideration** - Does any additional action by Law Enforcement require authorisation(*) or not?

Intelligence determines the planned route for importation and an expected date.		**Decide -** Consider liaison with relevant member states regarding surveillance / possible enforcement activity? **Consideration** - Is an ILOR now required requesting specific activity by foreign law enforcement, deployment of investigating officers from another member state and / or introduction of evidence from one country into another's Courts? **Consideration** - Should there be surveillance by law enforcement in another member state? **Consideration** - What surveillance technology could be deployed? **Consideration** - Does any additional action by law enforcement abroad require authorisation(*) or not?
Intelligence suggests that members of the crime group that are to take ownership of the gun are intending to shoot a named person.		**Decide -** Is there now a credible threat to life situation? **Decide –** Should law enforcement now consider: - Formal warning to intended victim? - Formal warning to possible offenders? - Use of surveillance technology in dealing with this aspect of the operation?

		Consideration - What surveillance technology could be deployed? **Consideration** - Does any additional action by law enforcement abroad require authorisation(*) or not?
The intelligence now in possession of law enforcement provides detail of: • The importation of a consignment of drugs and a firearm. • The known route of the importation. • The date of the importation. • The intended recipients of the gun and their intentions.		**Decide –** - Should law enforcement take action at the border / port when the consignment and gun are leaving the originating country? - Should law enforcement take action at the border / port on entering intended country? - Should law enforcement allow the consignment to progress to exchange between couriers and ultimate recipient of drugs / guns / both? **Risks:** - Will the intelligence and surveillance operation allow for certainty as to when the drugs / gun are present? - Will early action lead to no result - Will delayed action result in the gun / drugs being missed? - Is there a risk of losing control of the nominals involved and thereby the gun and drugs? - Will action by law enforcement at any stage compromise intelligence sources? - What impact will the decision to take action / not take action have on the threat to life situation?

Z and the unidentified foreign national to frequently use air travel on the lead up to the intended date of the import.		**Decide -** Should law enforcement make targeted use of body scanners at airports against nominal Z and the foreign national? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not? **Decide -** Should law enforcement make targeted use of x-ray / scanning machines against any luggage belonging to nominal Z and the foreign national? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not?
Intelligence suggests that the intended method of importation for the drugs and guns via sea		**Decide -** Should law enforcement make targeted and proactive use of ship tracking equipment and harbour scanning devices? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not?
Arrests		**Decide –** Should law enforcement consider the use of listening devices in cells / police transport? **Consideration** - What surveillance technology could be deployed? **Consideration** - Does any additional action by law enforcement abroad require authorisation(*) or not? **Additional consideration** – prisoners rights / legal privilege issues.

3.1 Discussion of serious crime police investigation scenario

The following section discusses the use of the surveillance technologies in the context of the scenario, taking into account separately the ethical and the fundamental rights considerations that arise at each stage of the investigation. The scenario describes an investigation that could have taken place in any jurisdiction. Many of the investigatory steps contemplated entail moral and fundamental rights risks. Identifying risks does not entail any judgment about how probable the dangers are. Most if not all jurisdictions will have in place instruments of oversight aimed precisely at mitigating these risks. Furthermore, some moral risks we identify will on balance be risks worth taking, given the priority of intelligence gathering at that stage. We do not comment in this deliverable on the mechanisms of oversight in place in particular jurisdictions, or assess their effectiveness. We do comment on some of the considerations that lessen or deepen the seriousness of risks at each stage, and that may add to or weigh against the justification of taking these risks.

3.1.1. Background to ethical considerations

The ethics parts of this section identify and discuss the considerations relevant to determining whether the uses of the technologies in the context of the scenario are justified ethically. As indicated in 2.4 above, these considerations are both more numerous and varied than those relevant to determining consistency with human rights law. The information included in the scenario is sufficient to allow a legal assessment to be made (albeit with some assumptions and caveats). The ethical assessments are not always so cut and dried. None of the uses of technologies proposed in the scenario is absolutely impermissible ethically. But this should not be taken to suggest that they are all justified despite the risks. On the contrary, there is a presumption in ethics against taking these risks, unless and until sufficient justification is provided.

Over the various stages of the investigation, the moral justification to engage in morally risky activity varies with regard to three aspects:

1. The seriousness of the crime.[22]
2. The strength of the evidence for believing that criminal activity is taking place.
3. The imminence of the crime.

Evidence is essential to justified moral risk taking. The decision to use force or intrude on privacy cannot be taken on an entirely speculative basis, for example. However, the epistemic standard for taking such moral risks cannot be too stringent.

[22] SURVEILLE deliverable D2.2. 'Paper with input from end users'. See in particular sections 3 and; for example "There are at least five factors which may lead to more intrusive methods being appropriate. These are significant financial loss; use of violence; threat to public order; organisation; and significant financial gain. Each of these five possible features of crime can elevate it to a level where intrusion and other risks would be appropriate" p 13.

For example, the extreme stringency of the courtroom's requirement for guilt to be established 'beyond reasonable doubt' would be entirely inappropriate. And in the case of preventing serious crime from being carried out by organised crime groups, relevant evidence will be hard to come by: criminals will try to keep their plans and communications secret and intelligence, particularly of secret conspiracies to commit crime,[23] will typically be weak, yet little else may be available to the authorities

'Imminence', a feature only of future crimes, is a matter of how close a threat is to taking place. This is a matter both of time and readiness. If police have good reason to believe suspect *P* is plotting a (significantly welfare-threatening) crime *C*, but do not know when, they are justified in taking certain moral risks. However, the reason for the lack of knowledge when the crime is due to take place is crucial. If there is no evidence to suggest that *P* is ready to carry out *C* or that *P* intends to carry it out now, morally risky methods may need to wait for more evidence of imminence. Whereas if police do have reason to believe *P* is ready to carry out *C*, and that *P* intends to carry out *C*, even if they do not know the precise time or place that *P* will act, they may be justified in taking further moral risk aimed at preventing *C* taking place or catching *P* in the act.

3.1.2. Background to fundamental rights considerations

The fundamental rights affected by the use of surveillance technologies in the scenario are, in order of the frequency and severity with which they are intruded upon: the right to protection of personal data; the right to privacy (or to private and family life); and only in some cases also the right to freedom of thought, conscience and religion; and freedom of movement and residence.

The rights affected are not absolute, in the sense that they permit restrictions or limitations that: serve a legitimate aim, are prescribed by the law in a precise and foreseeable manner, and are both necessary and proportionate in nature.

The permissibility of each intrusion at each stage of the investigation depends on an assessment of the legal basis, necessity and proportionality. Establishing whether the intrusion at each stage of the investigation is "in accordance with the law" within the meaning of article 8.2 ECHR or "provided for by the law" (article 52.1 EUFCR) is not possible here, due to the fact that the scenario is jurisdiction-neutral. The discussion of fundamental rights considerations is based on the assumption that proper legal basis exists for each surveillance measure.

From the perspective of a fundamental rights analysis, the legitimacy of the intrusion ultimately depends on the relationship between the level of intrusion and the contribution towards the aim of that intrusion. The greater the degree of non-satisfaction of, or detriment to, a fundamental right, the greater must be the importance of satisfying the other legitimate aim.(Annex 2.1-3)

[23] See Adam Roberts, 1989, 60 on analogous problems in counter-terrorism.

3.2 Stage-by-stage ethical, legal and technological assessment

Stage 1. The reception of low grade intelligence.

Ethics considerations

The motivation for surveillance throughout the scenario derives from the seriousness of the suspected criminal activity. At stage (1) this is large scale importation of drugs. This crime is serious in itself, because of the harmfulness of a range of illegal drugs. As different drugs vary widely in their harmfulness the seriousness of the crime will vary considerably as well. See for example the *Lancet* study (Nutt et al, 2007, 1051), which attempts to rank the harmfulness of different kinds of drugs, considering measures of physical harm, addiction, and likeliness to lead to social problems like violence, or those resulting from intoxication. These considerations contribute to the ethical justification of moral risks taken to prevent the shipment: where the shipment contains heroin, for example, greater risks will be justifiable than for marijuana, other things being equal. However, the considerations cannot be the last word on the harmfulness of the drug shipment. As well as the harmfulness of the drugs to users, one must also take into consideration the significant financial gain this shipment may represent to criminal organisations.[24] These organisations may engage in violent conflict over territory in which drugs will be sold, or violence against drug users to extract payments. Criminal organisations could also threaten welfare indirectly, by way of money laundering through ostensibly legal activities like construction, which will threaten welfare if it involves abusive exploitation of workers or unsafe building practices. However, it is much more difficult to pronounce generally on these kinds of harms as they will vary from region to region on the basis of which drugs are most profitable to which groups.

However, although the suspected offense is serious from the beginning, the evidential basis for belief that an offense is taking place is weak. The 'low grade intelligence' which is the basis for the initial suspicion may be understood as an unverified report of someone not an eye witness, but rather who have themselves received the information at least at second hand or a further remove. Such 'low grade intelligence' may be partial, inaccurate (identifying the wrong individual), or motivated by a malicious agenda: casting suspicion on the innocent to settle some score. This does not mean that 'low grade intelligence' should not be acted upon, but it does limit the means that would be proportionate for investigating further. Taking severe moral risks, or expending significant resources of police time or costly investigative techniques could not be justified at this stage. For example, keeping a suspect under surveillance, in the sense of deploying people to follow the suspect 24 hours a day, would in practice require something like three shifts of six police officers deployed each day (with police cars), further static surveillance stationed in houses to alert the mobile surveillance team that the suspect was about to leave his

[24] See also this statement of the EU Internal Security Strategy on the priority of combating organised criminal organisations as a security priority: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/internal-security/internal-security-strategy/index_en.htm.

home, officers working in a control centre and a desk officer.[25] Even if this level of intrusion could be ethically justified at this early stage when so little evidence exists about the suspects, the expense of this deployment could not.

Even research based on open data can uncover quite revealing information about an individual, due to the recklessness with which people publish information about themselves and others online. (This reckless conduct, although it affects the individuals uploading information more than it does anyone else, is itself morally criticisable).[26] Furthermore, in general, the law-abiding public are the most likely to have revealing information about themselves exposed online – while those deeply involved in organised criminal activity may be forensically aware,[27] and far more careful about managing their online presence. In such circumstances the absence of any online presence may itself be notable, while obviously susceptible of many innocent explanations. At the same time, the fact that open source information is already in the public domain means it is much less intrusive for the police to access it than if they were to uncover such information by other means.

As with low-grade evidential reports, evidence from social networking will vary wildly in its partiality, accuracy and motivation, and inappropriate reliance on weak information could result in needless further, morally risky surveillance. Police must recognise the possibility that evidence that has appeared to be indicative of criminal involvement could in fact be misleading.

Fundamental rights considerations

Data crawlers and data analysis tools carrying out social network analysis (e.g. Networked Data Analysis and Data Transfer Analysis) may appear in steps one to four of the scenario. Based on low-grade intelligence, the police consider performing research and analysis (including on open data) on X, and, after discovering association with Y and Z, a covert Internet investigation (steps 3 and 4), including 'friending' the suspects on social media. 'Open data' are data posted on the Web and freely available and accessible to any users browsing.

Two operations could be identified from the scenario:

- The use of tools to analyse *open data*, akin to the police patrolling the roads.
- 'Following' specific individuals covertly based on evidence of a potential crime.

It appears that the use of data analysis tools is *covert* in both phases, since it is invisible and unannounced. It is unclear whether the analysis is performed on personal communications inaccessible to the wider public. The latter would require

[25] Stella Rimington on 'More or Less', broadcast 31st May 2013, Radio 4, UK. Available at http://www.bbc.co.uk/programmes/b01snyk3

[26] See for example Anita Allen (2013).

[27] See for example Beauregard and Bouchard, 2010 'Cleaning up your act: forensic awareness as a detection avoidance strategy'.

higher thresholds of justification, necessity and proportionality and has relevant implications for the fundamental rights analysis. (Annex 3.16)

The scenario describes operations based on officers' lawful conduct and *bona fides*. At this stage, we must assume that the code is written in such a way that the software:

- Is not used for fishing operations, by which may be understood speculative inquiries made without a clear idea of what information is being sought, in that its use needs to be authorised;
- Does not retain (or it automatically deletes) irrelevant data sieved in the process, that is data relating to innocent 'bystanders' or the private life of the suspect (i.e. family and private relations etc.);[28]
- Is controlled by police officers, so that any risks of automation are eliminated;
- No databases containing biometrics are consulted (as suggested in the scenario);
- No monitoring (as understood in EU law) or interception of data in transit occurs.

The rights affected by crawlers are data protection and privacy. However, indiscriminate collection may affect some attributes of freedom of thought, conscience and religion, namely:

- Data protection: sensitive data; data minimization; data quality (open data);
- Privacy: confidential communications (if at least metadata); social identity and relations (if information about social network); and autonomy and participation (if information about one's activities).(Annex 3.17)

In the context of the scenario where only the information of the suspects is obtained and where proper safeguards are in place, the intensity of the intrusion by data-crawlers is not as such as to impede the enjoyment of the right.

The rights affected by generic data analysis tools are

- Data protection: data quality (which cannot be verified by data subjects and is in turn relevant for the correct identification of suspects)
- Privacy: Social identity and relations. Since individuals X, Y and Z are aware about the possibility of some third-party access when developing one's social life in social media, the intrusion presented is relatively low. (Annex 3.16)

[28] See the case Robathin v. Austria, (Application no. 30457/06) JUDGMENT STRASBOURG 3 July 2012, on data minimization (proportionality) in case of search and seizure of electronic data.

Technology considerations

Data analysis techniques give a crime-fighting unit an idea about the crime network and a profile for the associated partners relatively cheaply (though the training level of operatives might have to be high). These facts will probably enable justification for the use of additional surveillance but it is unknown whether they can be used as evidence in courtrooms. With data traffic, it is relatively easy to implement privacy-by-design rules because data can be targeted and stored selectively. (Annex 2)

Stage 2. Intelligence of association between X, Y and Z

Ethics considerations

At stage (2) the evidence of involvement in an organised plan to import illegal drugs is strengthened. As outlined in the discussion of stage (1), the crime is one of sufficient seriousness to justify morally risky surveillance, given a strong enough basis for suspicion. However, with the increasingly detailed evidence there are further details that may be inaccurate or partial. The main additional evidence implicating X at stage (2) involves evidence of an association between the original suspect and others. This could take many different forms, and vary widely in its reliability. At the weaker end of the range, it could be reliable evidence of them being in the same café at the same time, in which case it is open to question whether their meeting was mere coincidence. Also weakly it could be a matter of an unverified report from a source of dubious reliability. Stronger might be a reliable report or photographic evidence that the two had met a number of times. Stronger still will be evidence of them explicitly making arrangements to meet in the future, or other correspondence indicating an ongoing relationship.

As well as the intelligence about the association itself being wrong or misleading, there is an additional element to consider: namely that the association could be of a non-criminal nature. Evidence of association with criminals is not necessarily evidence of criminal conspiracy. Association with criminals is not a crime – evidence of an association with criminals is a kind of 'evidence of evidence', or second order evidence. Thus police must treat it with appropriate care and caution. That said, it might still be useful intelligence of a sort that should be followed up on, but only with the less morally risky methods proportionate to the evidence available at this stage.

Stage 3. Evidence suggesting Z is linked to firearms supplier in another jurisdiction.

Ethics considerations

As well as questions with regard to the strength of evidence, the investigatory techniques may be morally risky in other ways. Presumably 'friend requests', and accessing certain more detailed social networking information will require a minimal level of deception. This seems fairly easy to justify up to a point, since a mere 'friend request' involves little in the way of an explicit claim about who one is – but what if further deception is necessary to maintain this source of information? This will still

be justifiable if directed against a person known to be engaged in significantly welfare-threatening activity, and where the deception is part of a plausible plan for acquiring information to prevent that activity. By contrast if the only evidence to suggest the connection to Z is 'low grade' or corresponds to the weaker indications of association then elaborate deception at this stage seems disproportionate, as the evidence of involvement is still relatively weak. But this may change at more advanced stages of the scenario.

Stage 4. Discovery of intention to bring in firearms with drug shipment.

Ethics considerations

The addition of evidence of firearms shipment increases the seriousness of the suspected criminal activity considerably. Firearms not only represent a potent means for criminal organisations to pursue further welfare-threatening activity such as armed robbery, but also ultimately threaten life – the condition of any welfare at all. However, although the seriousness of the suspected activity has been increased considerably, evidence is still minimal.

Deploying surveillance teams shifts from making use of information already existing in the public domain (often voluntarily disclosed by the suspect) to actively gathering information on them. Most of this will involve some kind of watching in public space – that is space outside the home, where everyone has an equal right of access. This intrudes on privacy,[29] as it involves sustained scrutiny of an individual, but only to a moderate and acceptable extent, as we understand that public spaces are places where we may be seen and it is plausible to argue that we consent to being seen by choosing to appear in public space.[30]

There are further practical considerations that may also weigh against the deployment of physical surveillance at this point. If suspects are placed under physical surveillance does this risk alerting the suspects that they are under scrutiny? This sets up a further dilemma: if it becomes apparent that the present plans have been abandoned as a result of surveillance alerting them that they are under scrutiny, do they remain objects of attention and thus (potential) surveillance?

Deepening the level of surveillance will inevitably reveal much information that is tangential, if not irrelevant, to the original purpose of investigation. In some cases this will include evidence of irrelevant criminal activity, perhaps not even on the part of any of the suspects targeted by surveillance (one could discover criminal activity by another associate, or a spouse). Should this information be followed up? Again, as a practical matter, following up may alert the surveilled that they are under scrutiny. And pursuing lower level criminality may negatively impact on the perceived legitimacy of police in certain communities as it could give the impression

[29] See SURVEILLE deliverable D2.2., p 4 on the privacy of public spaces.
[30] See for example Ryberg, 2007 'Privacy rights, crime prevention, CCTV and the life of Mrs. Aramac.

of unfairness.[31] This is because only serious crime justifies the use of intrusive or otherwise risky methods, but it might appear that risky methods were being systematically used to target the low level crime of that community. Likewise prosecuting activity that not all agree should be illegal (such as immigration offenses) on the basis of 'collateral surveillance' might also damage trust in the police by identifying them with the illegitimate prosecution of offenses that should not be treated as criminal matters.

Also under consideration at this point may be the use of data fusion and mining systems. These may make use of intelligence held by or accessible to law enforcement to reveal additional insight. One contemporary study distinguishes between three kinds of data mining used in criminal investigation according to what it calls "a crime perspective, an offender or victim perspective".[32] What is meant by 'the crime perspective' here is profiling on the basis of features of the crime. One example is given by algorithms for predicting future sites of gun crime on the basis of previous sites of gun crime.[33] Whereas what is meant by the 'offender', or 'victim' perspectives, by contrast, are features of individuals to develop a profile by which thus far unidentified victims or offenders might be discovered. For example one might develop a profile of victims of burglary.[34] To develop a profile of an offender one might make use of financial information, examining patterns of payments to reach conclusions about certain kinds of relationships between the suspect and other individuals. This kind of information can indicate a person's role in an organisational structure as a 'broker' or 'gatekeeper' that relates some individuals to others.[35] This kind of social network analysis can also be carried out on the basis of communications data. Another kind of data mining from an offender perspective involves profiling likely suspects for particular crimes on the basis of features like modus operandi (MO).[36]

Some data fusion and mining systems that target offenders are morally risky.[37] Some may be risky because they are intrusive,[38] if they draw on highly sensitive information, or if they reveal highly revealing information. Financial information or telecommunications data might fall into these categories. The same is true of criminal records. Financial background profiling usually refers to less intrusive techniques of checking records in a variety of publically held datasets on matters such as property purchases, criminal history, bankruptcies, and employment history. The use of data fusion and mining technologies to profile offenders can also be

[31] For the importance of maintaining social trust between policing forces and wider community see SURVEILLE deliverable D2.2. p 6-7
[32] Oatley, Ewart and Zeleznikow, 2006, 52.
[33] See for example McCue, 2007.
[34] See for example Oatley, Ewart and Zeleznikow, 2006, 48.
[35] Oatley et al ibid, 68-70
[36] See Oatley et al ibid, 75 for an example of identifying suspects for burglaries in the West Midlands area of the UK.
[37] On the moral risks of data fusion and data mining technologies see SURVEILLE deliverable D2.2. p 5-6.
[38] See, for example: Tavani, 1999.

morally risky because they are often prone to error, whether because algorithms used themselves output many 'false positives,[39] or because errors in name matching across diverse datasets are common.[40] However, error in itself is not a wrong: it is when errors lead to bad consequences that a wrong has been done: if arrests are made on its basis, for example.[41] All three kinds of profiling – of the circumstances of crime, of victims and of offenders – can lead to errors. But only profiling of offenders indicates an individual's guilt, which is much more likely than any other error to lead to injustice. This is why profiling offenders poses distinct moral risks of error. Continuing, or deepening surveillance on the basis of these technologies involves moral risk, but one that is justified in the circumstances. Police must bear in mind the possibility that these technologies cast suspicion falsely.

Fundamental rights considerations

The use of CCTV and photography by police officers does not, as such, necessarily give rise to privacy considerations. However, both the *covert* and *overt* use of CCTV, and the use of photography in public places can be seen as constituting an interference with private life under Article 8 of the ECHR at this stage of the investigation, because

- Material obtained from the covert or overt use of CCTV in public place is used by the police or other (law enforcement) authorities in an unforeseen or intrusive manner;
- The covert or overt use of CCTV material involves processing of personal data whenever an individual is identified.

The severity of fundamental rights intrusion created by the covert use of CCTV in public places depends on number of different aspects.

First of all, it should be kept in mind that the mere monitoring of the actions of an individual in a public place by the use of CCTV does not, as such, necessarily give rise to an interference with the individual's private life.

Private life considerations may arise, however, once any systematic or permanent recording of the CCTV material occurs or when such material is analysed or otherwise "processed" by the police or other authorities. On such occasions, the covert use of CCTV in public places can be seen as clearly interfering with the individuals' rights both to privacy and to the protection of personal data. It can, furthermore, be assessed that whereas the level of intrusion remains low with regard the right to private life, a medium level of intrusion can be established with regard to the protection of personal data.

[39] For example on a range of counter-terrorism data mining programmes see DETECTER Deliverable D8.1. www.detecter.bham.ac.uk/pdfs/D8.1CounterTerrorismDataMining.doc

[40] See for example DETECTER Deliverable D5.2 and and Branting, L. Karl. 2005, 'Name Matching in Law Enforcement and Counter-Terrorism'

[41] On moral risk of error see SURVEILLE deliverable D2.2., p 4-6.

If the CCTV material is used to associate the individual with racial or ethnic origin or other categories of sensitive data, the level of intrusion into the right to personal data can be regarded as being high. Restrictions on the use of technologies are dawn from the following principles:

- An individual's liberty right of being able to decide what information to share and with whom may as such be considered to fall close to the core of the right to private life and hence to be of significant (medium or high) weight. However, the weight of this right is usually weaker in public contexts. The covert use of CCTV increases the level of intrusion.
- The protection of personal data has been understood to have fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the ECHR.[42]
- The need for data protection safeguards is all the greater where such data are used for police purposes.[43]

Regarding the intensity of these restrictions, at least following considerations must be taken into account:

- Although the right to private life is also applicable in public contexts, the capture of images in public places can usually be understood as intruding at the outer border of the right to private life and to the protection personal data. After all, a person in a public place will inevitably be seen by some member of the public who is also present. Monitoring by such technological means of the same public scene is of a similar character.
- However, the covert capture of images entails that the individual cannot be aware of being recorded. In terms of the right to privacy in general, this kind of intrusion can be regarded as medium.
- With regard to the right to protection of personal data, the intrusion can also be assessed to be medium, except in cases in which CCTV or photographic material reveals sensitive data. The strict requirements set forth for the processing of sensitive data reflect the severity of intrusion, the intensity of which can be regarded as being high.[44]

The use of Anti-Money laundering technology is proposed in phase 4 of the scenario in relation to the investigation of drug and firearms smuggling (*ex ante facto*): Law enforcement agents ponder the initiation of "financial background enquiries and developments of the financial profiles on all nominal suspects." How anti-money laundering software could be used in this situation is unclear. In the absence of further detail, we assume that the police obtain 'pushes' of financial transactions for all relevant individuals, coupled with telecom information.

[42] See, S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, 4 December 2008.
[43] Ibid.
[44] See, M.M. v. United Kingdon, judgment of 13 November 2012.

The principal rights affected are data protection and privacy. Freedom of thought, conscience, and religion may also be affected. These rights are affected in the following ways:

1. EUCFR Article 8 (data protection): sensitive data; data minimization: the fusion of data from different sources is likely to infringe upon data minimization: the principle that such data *are relevant* and *not excessive in relation to the purposes* for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored

2. EUCFR Article 7 (privacy): confidential communications, social identity and relations; and autonomy and participation.
3. EUCFR Article 10 (thought, conscience and religion): *forum internum.*

Since suspects X, Y and Z are 'neutral' individuals, that is not identified by any features exposing them to discrimination, and no coercive action is imposed upon them, the following rights are not affected: non-discrimination, freedom of expression and information, and freedom of movement. However, while banking data and telecom data are not considered sensitive data *per se*, they can *reveal* sensitive information about the data subject pursuant to article 8 of Directive 95/46 and 6 of Council Framework Decision 2008/977/JHA (which would ideally apply to the present case, where information about individuals from different member states are requested). Processing information revealing sensitive data that relate to X, Y and Z's participation in society (autonomy and participation, social identity and relations), could also affect the right to freedom of thought, conscience and religion (article 10 EUCFR). The fused data may reveal one's religion or political preferences (*forum internum*). Insufficient knowledge of the collection is an important factor in appraisals of the existence of an interference with one's private life (Article 8.1 ECHR).[45] A person has a reasonable expectation of privacy if there is no warning about the monitoring of 'correspondence'.[46] The fusion of private and open data intrudes upon the following attributes: confidential communications; autonomy and participation; and social relations and identity (Annex 3.17)

Neither data protection nor privacy nor freedom of thought, conscience and religion are configured as absolute rights in the sense of not allowing for any limitations (see D2.4 for more details). The attributes of privacy analysed have different weights. Since the confidentiality of personal communications is very close to the core of the right to privacy, the weight given to the attribute is high. The attributes autonomy and participation, and social relations and identity, are not close to the core, and should be given a low weighting.

[45] *Copland v. United Kingdom*, § 44.
[46] *Copland v. United Kingdom*, § 42.

As for data protection, since sensitive data are very close to the core, the weight given to the attribute is high. Data minimization in the context of police operations should have a medium weight.

As for freedom of thought, conscience and religion, the forum internum is very close to the core (thus would weigh high in other circumstances), but since the scenario is based on the assumption of non-discrimination, it weighs medium.

Technology considerations

CCTV systems can be expected to yield results at a relatively low cost but it is hard to protect privacy. Results could include: identification of associates, proof of illegal activities, or proof of association. Some of these facts may be used in court cases. Photography scores higher than the CCTV since it does not indiscriminately record all persons in an area, also, photos that do not provide relevant facts can easily be omitted from the investigation which makes photos less privacy sensitive.

Data analysis techniques give a crime-fighting unit an idea about the crime network and a profile for the associated partners relatively cheaply (though the training level of operatives might have to be high). These facts will probably enable justification for the use of additional surveillance but it is unknown whether they can be used as evidence in courtrooms. With data traffic, it is relatively easy to implement privacy-by-design rules because data can be targeted and stored selectively. (Annex 2)

Stage 5. Three months without new information.

Ethics considerations

At this point the investigation continues to involve intrusion, without any breakthrough. The decision to continue at this point will be difficult. It will be much easier to justify the continuance of lower risk activity, such as monitoring of locations in public space, rather than e.g. tracking suspects' movements.

Stage 6. Identification of regular foreign visitor

Ethics considerations

The sudden appearance of an unknown, regular visitor to Z fits the theory that he is there because he is supplying a firearm to Z, based on the partial evidence gathered so far of a plan to bring a firearm into the country, but this is one among many possible explanations. At this point the only evidence against the foreign national is his association with Z. Even if there were strong evidence implicating Z in serious criminality, it would be morally unjust and legally disproportionate to deploy the most intrusive surveillance against the foreign national at this stage. As it is, even the evidence against Z at this stage is moderate. However, using surveillance of public space – targeted use of CCTV, for example – in an attempt to identify him, seems proportionate, especially given that such surveillance is aimed at verifying a specific, narrow matter: whether the repeat visitor is the identified foreign dealer.

While there is a presumption against watching a person, circumstances affect the strength of the presumption: public space by definition is space where we accept that others may be watching us. As well as making use of already existing CCTV, deploying individuals covertly to photograph the specified caller also seems easier to justify ethically – the photography is not more intrusive for being carried out by an individual in public space rather than a machine.

More intrusive than taking photographs will be tracking a person's movements, as he travels around public space – if the same photographer, or a team of photographers is deployed to follow the foreign visitor. Likewise (were such an action practical) using facial recognition to search all the foreign visitor's appearances on CCTV footage for a particular day, would seem disproportionate at this stage. This is because this would be far more revealing of the details of a person's day-to-day life, and at this stage all that is known if that he visits Z. If the photography enables him to be identified as a suspected trafficker of drugs or guns, at that point more intrusive following will be ethically justified.

Stage 7. Home address of Z in rural location.

Ethics considerations

The evidence of Z's involvement in criminal conspiracy was sufficient to justify the use of cameras to try to identify an associate who keeps calling at the house. The surveillance capacity of a camera placed on a drone is only different insofar as it captures more superfluous information. In a remote area, where any neighbour is likely to be a long way off, this may not be an issue.

The deployment of a drone may differ from deploying human photographers or CCTV in other ways, however. For one thing it may be costlier, and there may be places a drone could photograph a person from above where they high fences or hedges would lead a person to expect a larger degree of privacy.

Fundamental rights considerations

The fundamental rights affected by the use of a camera mounted on a helicopter drone are:

- Fundamental right to privacy or private and family life
- Fundamental right to the protection of personal data
- Freedom of movement and residence

The manner in which the platform micro helicopter is deployed and operated may influence the assessment of interference. The case of *Perry v. the United Kingdom* might provide guidance in this respect but must also be distinguished from the current issue: "As stated above, the normal use of security cameras per se whether in the public street or on premises, such as shopping centres or police stations where they serve a legitimate and foreseeable purpose, do not raise issues under Article 8 §

1 of the Convention." [47] Thus monitoring of this nature can be construed to represent a legitimate aim. The Court's guidance does not refer to areas of a notionally different nature, such as that of the home or workplace: and it refers to fixed security cameras that usually are indicated by proper warning signs whereas the use of a moving aerial camera may constitute an unexpected new type of an interference: it may be concluded therefore that the use of a platform micro helicopter in these locations may be evaluated differently. The purpose for which surveillance is conducted by a public authority, and the use made by the party of the data obtained are the significant factors in determining whether an interference has occurred in the right to privacy.

With respect to the right to privacy, the level of intrusiveness of the use of aerial surveillance in a public setting can be considerable regardless of whether the device can be readily detected (overt) or not (covert). Thus the interference may be qualified as of a 'medium' weighting. In specific contexts, such as in areas considered generally as outwith the ambit of a public space (such as in a private dwelling), the interference could be considered 'high'.

Surveillance conducted through the use of a platform micro helicopter may engage the fundamental right to freedom of movement as the technology allows for spatial and temporal information pertaining to an individual's whereabouts to be monitored and collected. This procedure may inhibit a person's enjoyment of free movement where they feel the liberty is restricted by the knowledge that others are aware of their location.

The rights that may be affected by the use of a platform micro helicopter by law enforcement for the purposes of monitoring a suspect are not absolute; the provisions within the ECHR, ECUCFR and ICCPR pertaining to the rights to privacy, the protection of personal data, freedom of expression and liberty of movement are all qualified by the permissibility of limitations placed upon them where such restrictions serve a legitimate aim, are necessary and proportionate.

Technology considerations

The micro-helicopter, in this application, is related to the CCTV surveillance instruments discussed earlier and has a similar usability score. (Annex 2)

Stage 8. Evidence drugs/firearms shipment is imminent

Ethics considerations

The discovery of evidence of a specific plan by X, Y and Z to import drugs and firearms considerably strengthens the justification for intrusion and other moral

[47] Perry v. the United Kingdom, no. 63737/00, § 40

risks, as there is now more evidence of the plan to commit this serious crime, and more evidence of its readiness, and imminence.

The use of listening devices is very intrusive, and likely to uncover very personal information not relevant to the investigation. At what point will use be abandoned if it is not uncovering anything relevant? If after a week the device has uncovered nothing except X's intimate exchanges with a partner, will police continue to use the device? Such a deep intrusion is only justifiable as a means to uncover evidence of serious criminality. Even if, say, Z is using the privacy of his home for purposes of criminal conspiracy (which at this stage is not known), if he lives with a spouse, or has visitors in his home or car their privacy will also be intruded upon.

Will police use the devices also to listen to the partner's conversation with visiting friends? This seems unjust unless there is a good reason to think that this is likely to yield relevant information – i.e. either that she is herself complicit or has relevant information she might disclose in conversation (about X's intended travel, for example).

Fundamental rights considerations

The placement of a sound recording bug in a person's home has a severe impact on the right to respect for private life and significant weight with regard to the right to personal data. This is based on following key points.

- An individual's liberty right of being able to decide what information to share and with whom may as such be considered to fall close to the core of the right to private life.
- The weight of this right is very strong in a person's home – or another analogously intimate non-public space.
- The protection of personal data has been understood to have fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the ECHR.[48]
- The need for data protection safeguards is all the greater where such data are used for police purposes.[49]

As to the intensity of the restrictions on the rights, at least following considerations must be taken into account:

- Based on case law of the ECtHR, the intrusion caused by sound recording bugs is more susceptible of interfering with a person's right to respect for private life than for instance GPS surveillance, because it discloses more information on a person's conduct, opinions or feelings. According to our assessment, the intensity of intrusion is severe.
- As regards the right to protection of personal data, the intrusion may be especially severe if organized in a systematic fashion. In the context of

[48] See, S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, 4 December 2008.
[49] Ibid.

> the recording and communication of criminal record data as in telephone tapping, secret surveillance and covert intelligence-gathering, the ECtHR has emphasized it to be essential, to have clear, detailed rules that provide sufficient guarantees against the risk of abuse and arbitrariness. The strict requirements set forth for processing of personal data in criminal investigation reflect the severity of the intrusion.[50]

The above considerations result in the highest possible intrusion just as if the conclusion had been drawn directly on the basis of positioning the situation within the inviolable core of privacy and data protection rights. (Annex 3.04)

While the same issues are raised by sound recording bugs in a target's vehicle, such bugs do not intrude into the core of those rights. This being the case, intrusions may be legitimate in principle, depending on the satisfaction of proportionality and necessity constraints. Nevertheless, the intrusion into privacy remains severe and the intrusion into data protection high. (Annex 3.05)

Technology considerations

Depending on the conditions in which they are used, sound recordings can be very targeted and useful. (Annex 2)

Stage 9. Ascertained that Z travels with foreign national on public transport.

Ethics considerations

Again some of the same, familiar problems of surveillance recur. The placement of a listening device on public transport may uncover information and evidence of criminal activity that is irrelevant to investigation, which may need to be acted upon, depending on its seriousness.

The intrusion caused by listening equipment is less severe on public transport than in the home or the suspect's vehicle, because our entitlement to privacy is less in public places. However, the likelihood of success is lower – it is unlikely that investigators can know in advance where the targets are likely to sit, and thus collateral intrusion seems inevitable, as any listening device likely to pick up the conversation of the suspects is just as likely to pick up the conversation of innocent travellers.

If the decision to bug public transport goes ahead nevertheless, it may be the case that the surveillance of public yields no useful results simply because the suspects do not talk about the topic of interest. Certainly use should be abandoned if it becomes known that Z and the foreign national do not say anything relevant while on public transport, but this is very unlikely to ever be known – it will only be known that Z and the foreign national have said nothing so far. But continuing surveillance with such inevitable 'collateral intrusion' seems hard to justify in the absence of results.

[50] See, M.M. v. United Kingdon, judgment of 13 November 2012.

Fundamental rights considerations

The bugging of public transport shares similarities with the covert use of CCTV in public places and with the use of audio bugs in targeted cars.

The severity of fundamental rights intrusion created by sound recording bugs on public transport used by the target depends on number of different aspects.

Sound recording bugs in public transport endanger rights or attributes of rights that have a low weight in regard the right to private life and medium weight with regard to the protection of personal data.

- As above, an individual's liberty right of being able to decide what information to share and with whom may as such be considered to fall close to the core of the right to private life and hence to be of significant (medium or high) weight. However, the weight of this right is usually weaker in public contexts.
- As above, the protection of personal data has been understood to have fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the ECHR.[51]
- The need for data protection safeguards is all the greater where such data are used for police purposes.[52]

As to the intensity of these restrictions, at least the following considerations must be taken into account:

- Although the right to private life is also applicable in public contexts, in typical cases, the recording of sounds in public transport can be understood as intruding at the outer border of privacy rights. A person talking on public transport will inevitably be heard by other members of the public present. Technological monitoring of the same public spaces will be similar. In terms of the right to privacy in general, this kind of intrusion is low.
- With regard the right to protection of personal data, the intrusion may be significant. (Annex 3.05)

Technology considerations

Sound recording in public places makes any form of privacy by design useless since many people may be overheard and it may be hard to use as evidence in court since the identity of the individual has to be proven beyond doubt. (Annex 2)

Stage 10. Suggestion of link between Z and crime group involved in violent dispute.

[51] See, S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, 4 December 2008.
[52] Ibid.

Ethics considerations

This stage again introduces evidence that raises the seriousness of the suspected crime. The evidence in question is of an association between Z and a violent crime gang. It raises the seriousness of the suspected crime because it provides good reason to fear the likely consequences of the successful importation of the illicit materials. These likely to further welfare-threatening criminal activities of the organisation: guns in particular may be being sought to escalate an already violent dispute, with risks that any new incident may trigger additional cycles of violence.

It is now a policing priority to find the intended recipient for the gun. The immediately available evidence in question is again associational and past criminality. The easiest way to justify surveillance of one of the gang members is if there is specific evidence naming them as the likely destination. However, specific evidence of an intention to acquire a gun may not be discoverable in the available window.

Intrusive scrutiny of all possible recipients would seem to entail the intrusive scrutiny of some innocent people. One might argue that if all likely recipients are gang members, they are therefore already known suspects in criminal activity (or short of this, that there is good reason to believe that they are participating in a criminal enterprise). But simple involvement may still be too weak a basis if the previous involvement is nothing to do with violence or other serious crime. And if the evidence of criminal association lies merely on the basis of associations with known criminals, this is likely to be too weak to sustain intrusive measures against all of these suspects. At this point very intrusive measures are justifiable against Z or the foreign national, but directing these measures against the gang members seems disproportionate unless there is specific evidence of their participation.

Stage 11. Intelligence of intended date and route of importation.

Ethics considerations

Further specification of the intended date and route strengthens the basis for confidence that the shipment is being plotted. And the specificity of date will mean that action directed towards preventing, disrupting or intercepting the shipment is justified by its imminence.

Sharing intelligence poses moral risks other than that of intrusion. In particular, there is a danger that mistakes will be made on the basis of the shared intelligence. This is especially a problem with jurisdictions with a poor record of respecting human rights. The risk of human rights abuse is not limited to the foreign national suspected of arranging the importation for Z – a jurisdiction with poor human rights practises might arrest or charge suspects not identified by the original jurisdiction on the basis of a weak association with the suspect. This is an extreme example, and does not reflect the reality of intelligence sharing risks with most EU member state jurisdictions. However, the home jurisdiction in the scenario do need to consider the likely consequences of sharing the intelligence beyond their own investigation.

Stage 12. Discovery of intention to shoot a named individual.

Ethics considerations

The introduction of intelligence of the intention to shoot a named individual adds to the justification of morally risky surveillance once again, and now the justification is at a strong level – seriousness, strength of evidence and imminence are all high.

But this situation also provides police with an acute dilemma: on the one hand, what if police do inform either the named individual or the suspects, and as a result the suspects subsequently take increased anti surveillance measures? But on the other, what if police hesitate to inform the individual and he is shot? The priority of protecting life means, and the potential victim's moral entitlement that the state make use of all chances to avoid that possibility mean that the information certainly cannot be ignored, however convenient to the investigation. Only if police are confident that they are able to prevent the planned attempt on the victim's life in a different way are police entitled to withhold from telling the victim – and such confidence is surely not possible if intelligence about the plan is partial and incomplete (as such intelligence very often is).

Stage 13. Police in possession of detailed intelligence

Ethics considerations

At this stage police receive more detailed information about the importation of drugs and guns – when it is due to take place, and via what route. This detailed information meets the requirements of seriousness and imminence to justify morally risky measures. The most common way in which an investigative measure might be morally risky is by invading privacy in some way. However, other kinds of moral risks may be posed by intelligence sharing, particularly if intelligence is shared with regimes with poor records on respecting human rights. Such intelligence sharing may be used by the foreign jurisdiction to generate a profile to assist with intercepting the foreign national at the border before he/she can leave the country. The profile may be used as a basis for enhanced scrutiny and searches at the border. Intrusive searches can be justified, especially given the credible intelligence of drugs and arms shipments. But repeated searches past the point it is clear that the suspect has nothing hidden on their person, for example, are excessive and serve no good purpose. And the profile relied upon could lead to discrimination if it depends on a characteristic such as ethnicity – even if, say, there is an evidence based case for saying that the trafficking of certain illegal drugs is dominated by organisations predominantly of particular ethnicities. (For example, Paoli and Reuter (2008) find that Turkish and Albanian groups are dominant in the importation, trafficking and open air dealing of heroin in a number of European countries, such as the UK, while Colombian groups dominate the importation of Cocaine into Spain and the Netherlands, the main entry points for the drug into Europe).[53] If this happens, and

[53] Paoli and Reuter, 2008, 13.

the border guards do indeed use ethnicity as part of the profile to identify the foreign national, this risks discrimination.[54] The home jurisdiction must consider the human rights record of the foreign jurisdiction before sharing intelligence and consider the likely consequences.

Stage 14. Z and foreign national engaging in frequent air travel

Ethics considerations

The point about the riskiness of intelligence sharing will also apply to sharing intelligence with border agencies – again, the home jurisdiction should consider if there is any danger, for example, of a crude profile being employed by people screening for the foreign national. Sharing intelligence on a suspect with a border agency might result in additional scrutiny being directed against the innocent individuals who share the same ethnicity. Searches of innocent people may be justified if carried out on a sufficiently strong basis, and within appropriate legal restraint. The home policing agency needs to consider the likely consequence of intelligence sharing with the border agency beyond their investigation.

Fundamental rights considerations

Body scanners

The following fundamental rights may be affected by the use of the eqo security scanner:

- The right to the protection of personal data (Article 8 of the CFREU; Article 8 of the ECHR).
- The right to respect for private life (Article 7 of the CFREU; Article 8 of the ECHR; and Article 17 of ICCPR).

Millimeter wave body scanners produce a low-quality image of a person's body that is rather opaque, which resembles a photographic negative. The operator does not see this image, but a generic graphical representation of a human person with the location of the suspect item highlighted. As such, no personal data is visible to the operator. The description of the technology seems to suggest that no personal data is actually being processed, since the 'image processing computer' processes 'reflected signals' of concealed objects, and no information relating to an identified or identifiable natural person is being captured.

As images of a millimetre wave scanner can make sexual organs visible and/or are able to reveal intentionally concealed physical features (for instance of transsexuals) or medical information (such as evidence of a mastectomy) that people might prefer not to be revealed, its use constitutes an interference with the right to respect for

[54] On the moral risk of discrimination, particularly in relation to making use of ethnic characteristics in profiling, see DETECTER Deliverable D5.4.
www.detecter.bham.ac.uk/pdfs/D5_4_Moral_Risks_of_Profiling_in_Counter-Terrorism.doc

private life. However, since the eqo scanner only shows a generic graphical representation of the person to the operator, the interference with the right to respect for private life will be mitigated. It may, however, result in persons with the above-mentioned concealed features being singled out for a pat search that may be more intrusive than if a pat search was the method applied to everyone. A potential for further intrusion related to non-discrimination arises if body scanners are uncharacteristically used selectively on the basis of 'profiling'. The scenario refers instead to the 'targeted' use of a body scanner in respect of certain individuals.

The potentially affected rights (privacy and data protection) are not absolute but do allow for permissible limitations.

As an image of a human person is produced in the process, even if then replaced by an animated figure before being shown to the human eye, there is an initial phase of revealing one's personal data. As no actual images or other data are stored and as the transitory animation figure is not associated with an identifiable person, the weight of data protection rights remains medium.

As going through a body scanner reveals the physical contours of one's body, even if only to a machine, and as certain categories of persons with intentionally concealed implants will be singled out for a pat search, significant weight is given to the right to privacy.

There is no intrusion in respect of data protection rights. In relation to the right to privacy, the level of intrusion is low.

Luggage screening for explosives and drugs

The primary right affected by luggage screening is the right to privacy, or to a private life. According to established case law private life or privacy is a broad term covering, among others, a right to retain a private sphere in respect of what one is carrying or transporting inside a closed object such as a suitcase. The person wishing to transport such personal items has the right, in principle, to determine to whom he or she shows or declares the contents of the closed container.

In principle, several other fundamental rights can be affected if the right of a person not to disclose the contents of a closed container is compromised. For example, a suitcase may contain religious items or materials, or political publications, the disclosure of which results in revealing the person's religion or political views and in particular in repressive countries may result in violations of the freedom of religion or freedom of expression. Also freedom of movement and the right not to be discriminated against may be implicated. As the scenario focuses on drugs and explosives and the individuals under investigation are 'neutral' persons without any religious or political affiliations, these indirect impacts on other rights can be set aside and the assessment focuses on the direct interference with privacy rights through compromising the person's right not to disclose the contents of the container.

Subjecting an item of cargo or luggage to screening does not result in intrusions into the core of privacy rights. Using GS-MS or X-rays for the detection of explosives or

drugs is in fact less intrusive than the opening of the container which would reveal to the inspectors also 'innocent' items that reflect for instance the religious, political or sexual orientation of the person. Furthermore, the international transport of drugs or explosives is subject to restrictions such as an obligation to declare any hazardous items or an outright ban on such transport. Individuals relying on international transport of cargo and luggage are aware of the fact that various methods of screening are in place for legitimate security reasons. In the scenario, the screening serves the legitimate aim of investigating or detecting crime. Consequently, the intrusions may be legitimate.

Subjecting items of cargo or luggage to screening for explosives or drugs affects a dimension of privacy rights that has at best low weight.

As to the intensity of the intrusion, the above considerations result in an assessment that it is to be considered to be at best low.

Technology considerations

AIS detection, submarine explosives detection, gas chromatography, whole body scanners and luggage screening are a group of highly specialized surveillance technologies. As a rule, they are relatively expensive, and rely on support by third parties. This makes them less usable for a crime-fighting unit; however, their performance in terms of successful identification of illegal goods is typically excellent. (Annex 2)

Stage 15. Intelligence suggests importation coming by sea

Ethics considerations

In the circumstances at this stage of the investigation, use of ship tracking will be unproblematic. It is not a very intrusive technology in any case, and there is a strong case that serious criminal activity is imminent.

Fundamental rights considerations

The use of AIS data alone does not entail an intrusion to the right to the protection of private life and personal data,

If used in combination with other data about an individual, the intensity of intrusion of rights limited by AIS location equipment is medium at most.

AIS equipment provides information about location, course and speed of vessels. It does not as such provide information about location and movements of individuals. As far as this remains the case, the use of AIS does not alone entail an intrusion to the right to the protection of private life.

The case is different if AIS data are used as a part of targeted or proactive criminal investigation in a way in which data collected through AIS is combined with personal data about an individual. In this case, also the use of AIS ship location detection and identification data for the purpose of surveillance of an individual may constitute interference with an individual's right to private life. However, such intrusion is relatively weak. As stated by the ECtHR, GPS surveillance is by its very nature to be

distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information about a person's private life than the use of location data does.

Taken together these reasons suggest that the abstract weight of both the right to protection of personal data and right to private life are weak in the case of AIS location and identification data.

Technology considerations

AIS detection, submarine explosives detection, gas chromatography, whole body scanners and luggage screening are a group of highly specialized surveillance technologies. As a rule, they are relatively expensive, and rely on support by third parties. This makes them less usable for a crime-fighting unit; however, their performance in terms of successful identification of illegal goods is typically excellent. (Annex 2)

Stage 16. Arrests

Ethics considerations

The justification for using listening devices is slightly diminished once suspects carrying out the importation are in police custody, as the threatened crime is no longer imminent. Now the appropriate norms governing justification of surveillance belong to the more familiar, reactive paradigm of criminal investigation. Nevertheless, this does not rule out the possibility of justifying the use of listening devices, especially given that it is still a serious, life threatening crime that is being investigated. However, such surveillance can under no circumstances compromise the norm of lawyer/client confidentiality.

Fundamental rights considerations

The severity of intrusion of listening devices in a police car depends on a number of different factors. The starting point must be that people in police's custody in general continue to enjoy all the fundamental rights and freedoms guaranteed under the Convention.[55] Any restriction on these other rights must be justified. On the other hand, as emphasized by the ECtHR, such justification may well be found in the considerations of security, in particular the prevention of crime and disorder.[56]

In the abstract, the sound recording bugs in a police car endanger rights that have a medium weight. Although the same rights (to data protection and privacy) as are affected by bugging in homes and private vehicles are affected here, a police vehicle is not a place where persons could reasonably expect for a high level of privacy. A person's reasonable expectations to privacy may be a significant, although not necessarily conclusive, factor in a rights assessment. In addition, considerations of

[55] See, Hirst v. the United Kingdom (no. 2) [GC], no. 74025/01, ECHR 2005-IX).
[56] See, Silver and Others v. the United Kingdom, judgment of 25 March 1983, Series A no. 61

security, in particular the prevention of crime and disorder, which typically are relevant in cases concerning arrest may justify broader restrictions to these rights than would be the case in other circumstances. Hence the weighting of both privacy and data protection intrusions are lower here than with bugging in homes or private vehicles. (Annex 3.07)

Technology considerations

Depending on the conditions in which they are used, sound recordings can be very targeted and useful. (Annex 2)

4. Conclusion

This deliverable combines surveys of surveillance technology across the disciplines of ethics, law and technology assessment, on the basis of a scenario that reflects actual situations faced by police end users. We extend the frameworks so far developed in SURVEILLE on the legal and ethical norms of surveillance in organised crime, and for reviewing the efficiency of developing technology. The matrix and the discussion of it demonstrate the ways in which the seriousness of crime and the impermissibility of fundamental rights violations can be taken together in making decisions about using intrusive surveillance. The fact that serious organised crime may pose a great danger to human welfare justifies morally risky actions that would not normally be allowed, but it does not give carte blanche to every measure that could contribute to fighting serious organized crime. Fundamental rights offer immovable protections for the individual against the intrusions of others, but not every intrusion by investigators will cross the threshold for impermissibility. Even intrusions on rights to privacy, or data protection may be consistent with fundamental rights if they are authorised by law, and the abstract weight of the right is lower than the security benefit obtained because of the target's circumstances.

One outcome of combining the various assessment of the use of surveillance technologies in the crime investigation scenario, presented immediately after the matrix itself in section 2.2, was the classification of the 19 usage situations of the 14 technologies as justified, suspect, highly suspect and (legally) impermissible. Although this classification was tied to the specific scenario and remains subject to further work by the SURVEILLE consortium, it demonstrates the value of SURVEILLE research so far.

The matrix provides an accessible overview of these distinct assessments, which are explained further in the discussion of the policing scenario. This discussion clarifies the basis for the assessments of the technologies. It also further outlines the way in which the normative ethical and legal considerations are related, but distinct. Analysis of a suspect's fundamental legal right to privacy and how this is threatened by surveillance technologies will overlap with moral assessments of invading their

privacy. But discussion of one does not make the other redundant. Visualising both kinds of assessment side by side serves a useful purpose for potential end users. However, it is also important to note the limitations of this matrix: while the ethical assessments coded in the matrix reflect wider ethical principles, the scoring of the different technologies' intrusiveness into fundamental rights is tightly linked to the context of the surveillance carried out in the specified scenario Applications of this work to further scenarios, such as deployment of technologies by local authorities, or by police to further kinds of crime, are tasks for future deliverables.

Bibliography

Alexy, Robert. 2002. *A Theory of Constitutional Rights*. Oxford: Oxford University Press

Allen, Anita. 'An Ethical Duty to Protect One's Own Informational Privacy?' in The Alabama Law Review. 2013. vol. 65.

Beauregard, Eric and Martin Bouchard. 'Cleaning up your act: forensic awareness as a detection avoidance strategy' in The Journal of Criminal Justice. 2010. vol. 38. no. 6

Branting, L. Karl. 2005, 'Name Matching in Law Enforcement and Counter-Terrorism' *ICAIL Workshop on Data Mining, Information Extraction, and Evidentiary Reasoning for Law Enforcement and Counter-Terrorism* Bologna, Italy.

DeCew, Judith. 1997. *In Pursuit of Privacy*. New York: Cornell University Press

English, Richard. 2009. *Terrorism: How to Respond*. Oxford: Oxford University Press

Hillyard, Paddy. 1993. *Suspect Community*. Pluto Press

McGregor, Graham. 'Eavesdropping and the Analysis of Everyday Verbal Exchange' In Alan Thomas ed. Methods in Dialectology 1987. Multilingual Matters

McGregor, Graham. 'Eavesdropper Response and the Analysis of Everyday Communicative Events' in Graham McGregor and R. S. White Reception and Response. London: Routledge

Moeckli, Daniel. 2008. *Human Rights and Non-Discrimination in the 'War on Terror'*. Oxford: Oxford University Press

Oatley, Giles, Brian Ewart and John Zeliznikow. 'Decision Support Systems for Police: Lessons from the Application of Data Mining Techniques to 'Soft' Forensic Evidence' in Artifical Intelligence and Law. 2006. vol. 14. no. 1-2

Pantazis, Christina and Simon Pemberton. 'From the Old to the New Suspect Community' in The British Journal of Criminology. 2009 vol. 49 p 646-66

Paoli, Letizia and Peter Reuter 'Drug Trafficking and Ethnic Minorities in Western Europe' in The European Journal of Criminology. 2008. vol. 5 no. 1

Roberts, Adam. 1989. 'Ethics, Terrorism and Counter-Terrorism' in Terrorism and Political Violence. vol. 1. no. 1

Ryberg, Jesper. 'Privacy Rights, Crime Prevention, CCTV, and the Life of Mrs. Aramac' in Res Publica 2007. vol. 13

Spalek, Basia, El Alwa and Laura McDonald. 2008. *Police-Muslim Engagement and Partnerships for the Purpose of Counter-Terrorism: an Examination*. University of Birmingham

Tavani, Herman. 'KDD, data mining, and the challenge for normative privacy' in Ethics and Information Technology. 1999. vol. 1. no. 4 p. 265.

ANNEX 1. DETAILED DESCRIPTIONS OF SURVEILLANCE TECHNOLOGIES

1.1-3 CCTV Technology

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. Relates to matrix Human Rights and Ethical Issues - Visual Spectrum Dome-zoom, tilt, rotate (public place – used (c)overtly)

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. Relates to matrix Human Rights and Ethical Issues - Covert Photography in Public Place

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).

Vulnerability of CCTV cameras

- CCTV cameras can be observed and are vulnerable for destruction. Some CCTV cameras come in dust-tight, explosion proof housing.
- The lens of the camera is vulnerable for sprayed substances that make the image blurry.
- Lasers can blind or damage the cameras
- The CCTV system is vulnerable for hostile intrusion. Wireless IP cameras are in this respect much more vulnerable to hostile intrusion than wired cameras.

1.4-8 Audio Surveillance Technology

The widespread application of audio surveillance technology has been thriving, as it is almost undetectable to the naked eye and it can be hidden in almost any location. Relates to matrix Human Rights and Ethical Issues – Sound Recording Bug/s in …. 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 analog 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 analog 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.

Phone sound bugs are probably the most common audio surveillance device. A phone sound bug is simply a small audio spying device that is usually attached to the inside of the phone and performs an audio surveillance. It sends the digital audio signals during a conversation to another location to stream the voice of the suspect and the contacted person to a monitoring device.

Cell-phone audio surveillance is a technology that uses a normal cell phone, which is equipped with a device that enables an external connection and tracking of all conversations made over that cell phone. Together with the installed GPS system also the location of the caller can be monitored.

1.09 Video camera mounted on a platform micro helicopter
What is it?
A micro-helicopter is the smallest type of UAV or unmanned aerial vehicle, a micro-UAV. Micro-helicopters are usually quadricopters (with 4 propellors). The payload is usually one small camera. Its operating range is small, typically an operator is in close proximity of the quadricopter. Relevant for the scenario is that range and payload capabilities of UAV's vary. The following classes are distinguished:

Category name	Mass [kg]	Range [km]	Flight Altitude [m]	Endurance [hours]
Micro	< 5	< 10	250	1
Mini	<25/30/ 150	< 10	150/250/ 300	< 2
Close Range	25 –150	10 – 30	3000	2 – 4
Medium Range	50 –250	30 – 70	3000	3 – 6
High Alt. Long Endurance	> 250	> 70	> 3000	> 6

Note that the UAV itself is not a surveillance instrument but a platform for carrying surveillance instrumentation.

How does it function?
Though their class may vary, there are always six elements to a UAV (Pastor et al, 2006): the aerial body, aeronautical equipment including the flight computer, the payload, the payload controller, the ground station and a communications network. Payloads may be passive scanning equipment such as camera's, infrared camera's or theraherz detectors. It may be active scanners such as radar or weapons of some kind. For micro-helicopters the aerial body is a small helicopter (often quadricopters) and the payload is a one small camera. Typically an experienced quadricopter operator controls their movements, which means that its operating range is relatively small. This equipment can typically be transported by a car and fly for about 1 hour. Typically, no interference takes place with normal air-transport. Note that a quadricopter can be bought for less than 1000 Euro's on the internet.

Close or medium range UAV's are typically small fixed-wing planes 3-5 meters that have to be launched from airports or small airfields or ships. They are typically able to fly a pre-programmed path or a ground station can manage their flight. They can carry multiple detectors to search the sea for suspect ships. Their size and altitude of flight may mean that it interferes with normal air-transport activities. The cost of such an aeroplane is upward of 100.000 Euro's up to 1.000.000 euro's or more depending on the payload and the level of autonomy.

Ethical Intrusions
Two types of intrusions are discussed here. First, a camera hanging from an airborne observation platform records the environment indiscriminately. Meaning that collateral intrusion takes place. Bystanders, or people under the flight-path of the UAV are recorded as well.

The second type of intrusion is that of airspace. Ordinary (manned) airplanes are not allowed to fly lower than 300 meters due to privacy and safety considerations. Micro UAV's typically operate in that air-space. Larger UAV's may interfere with air-space that is reserved for manned transport, thereby interfering with normal and safe air-travel.

Pastor, E., J. Lopez & P. Royo (2006), 'A hardware/software architecture for UAV payload and mission control', op: http://upcommons.upc.edu/e-prints/bitstream/2117/8697/1/25_digital%20_avionics_pastor.pdf

1.10 AIS Ship Detection

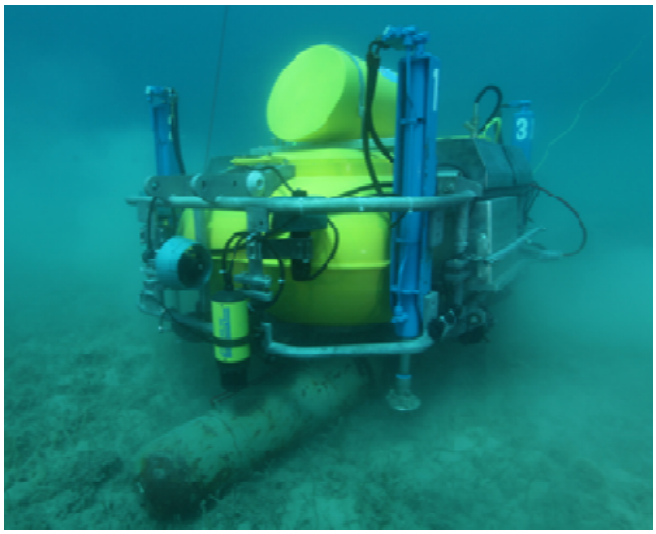
The AIS system (Automatic Identification System) is a complex system to support safe transport on waterways. Seagoing ships are obliged to transmit its type (general cargo, tanker, coaster, etc.), GPS-position, heading, speed, destination, together with a time stamp of the transmission and a unique identification number (MMSI, Maritime Mobile Service Identity) via VHF radio frequencies. Often additional information is transmitted such as ship length, draught and sometimes the type of cargo. Typically, this information is transmitted every 3 seconds. The information can be received by other ships in the vicinity or by coastal receivers. When other ships receive the information they can improve the accuracy of navigational maps and prevent accidents more effectively. Coastal receivers help port authorities guide ships safely into busy harbours or channels whilst at the same time keep track of all the ships going into and out of the harbour. For surveillance, it's use lies in keeping track of ships that carry suspect cargo or suspect individuals. Note that ALL AIS data in a defined jurisdiction (say, the Netherlands) is stored for a year or more, which enables retrospective crime analyses. Unfortunately, the AIS system is only required for large commercial vessels. Smaller fishing vessels, sailing ships or recreational vessels (including power boats) are not required to have an AIS transmitter. Also, the range of a VHF radio is limited so land-based AIS stations only receive the part of the path close to the coast. Inland shipping is typically recorded over the whole course of the journey.

- IMO. AIS transponders. Available: http://www.imo.org/OurWork/Safety/Navigation/-Pages/AIS.aspx [Accessed 2013-06-04].
- WIKIPEDIA. Automatic Identification System. Available: http://en.wikipedia.org/wiki-/Automatic_Identification_System [Accessed 2013-06-04].
- Harati-Mokhtari, A., Wall, A., Brooks, P., Wang, J., 2007. Automatic Identification System (AIS): data reliability and human error implications. Journal of navigation 60 (3), 373.

1.11 Explosives detection near harbour

What is it?

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.



UNCOSS: Final Report UNCOSS, 2012

How does it function?

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 (camera's) 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.

Ethical Intrusions
This piece of equipment is used under water. Intrusion may be that national coastal waters may be entered without permission.

http://www.uncoss-project.org/scripts/home/publigen/content/templates/show.asp?L=EN&P=55

1.12 Gas chromatography drugs detector

Gas chromatography is a sensitive analysis technique for chemicals. A sample is vaporized in a heated chamber and the vapour is carried through a long capillary tube (1 to 5 meters) together with a carrier gas (air, nitrogen or helium). The capillary is covered with an adsorbent on the inside. The time that a compound takes to travel through the capillary depends on the affinity between the adsorbent and the adsorbent (the compound temporarily 'sticks' to the adsorbent, the better it sticks, the longer it takes for the compound to exit the capillary). The time it takes to exit the capillary, or the time relative to a tracer compound, is characteristic of a specific chemical and can therefore be identified in the original sample. Samples can contain dozens of different compounds that can thus be identified within a minute or even in seconds. Typically for drugs detection, combining chromatography with mass spectroscopy further enhances the sensitivity. The compounds exiting the chromatograph enter a mass spectrometer, which detects extremely low concentrations of chemicals and, as a bonus, automatically provides additional information to determine which chemical compound is detected. The detection limits may be in the order of micrograms per litre of sample (so in the order of parts per billion).

The high sensitivity makes it possible to detect illicit materials (drugs, explosives or any other suspect compound) on a person, in the air, on surfaces of suitcases etc. etc. However, when the concentrations of suspect compounds near the detection threshold, the uncertainty about the presence of a compound becomes uncertain.

- WIKIPEDIA. Gas chromatography–mass spectrometry. Available: http://en.wikipedia.org-/wiki/Gas_chromatography%E2%80%93mass_spectrometry [Accessed 2013-06-04].

McNair HM, 2009, Basic Gas Chromatograpy 2nd ed., Wiley & Sons, New York.

1.13 Full body scanner eqo

A full-body scanner eqo is a device that detects objects on a person's body for security screening purposes using a form of electromagnetic radiation. The 3D scanning system provides a provide the operators with a millimetre-wave image, thus providing more privacy for the person being screened than the x-ray body scanner. A generic graphical representation of the person is presented to the

operator. The system software detects concealed objects and indicated their location with a marker on the appropriate part of the graphical display. This feature both simplifies the scanning procedure and also speeds up the overall process.

Typical uses for this technology include detection of items for commercial loss prevention, smuggling and screening at government buildings and airport security checkpoints.

How does it function?

The traditional full body scanner use x-ray. The operator may see the image of human body details. The full body scanner eqo use millimetre-wave to provide privacy for the person being screened. Different materials exhibit differing properties when interacting with electromagnetic energy. These properties vary with the temperature, density and the molecular composition of the matter. Eqo system operates like a sonar or radar device, hence the product's eqo name referring to the system's technological approach of sending out and analysing 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 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 analysed electronically.

14. Luggage screening technology

Security screening of luggage or cargo is a standard practice, in particular when such items travel through air but also more generally. Traditionally, X-ray machines using radiactive emissions have been used to locate and identify metal items. They remain in use together with other equipment, for instance Explosive Detection Systems (EDS) and Explosives Trace Detection (ETD) for explosives detection, and bottled liquids scanner (BLS) screening systems. New generation bottled liquids scanner systems have the ability to detect a wider range of explosive materials and use light waves to screen sealed containers for explosive liquids. If a bag or other item requires additional screening, it may be automatically diverted to a resolution room where security officers will inspect it to ensure it doesn’t contain a threat item.

1.15 Money laundering technology

What is it?

Money laundering technology is to prevent concealing illicit sources of money. Many of 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:

- Wire transfer screening to determine where to target further investigations,
- Knowledge acquisition to construct new profiles for use during screening,
- Knowledge sharing to disseminate profiles of money laundering activities quickly, reliably, and in a useful form,
- Data transformation to produce data that can be easily screened and analyzed.

Note that the technology is only part of a normal financial crime investigation.

How does it work?
We found no detailed information about the working of search programs. These are 'data crawlers' and in might, in some respects, be not so different from a Google search engine that 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.

1.16-17 Data Analysis Tools
Data analysis tools to examine large data sets on the internet or in data communication to find certain pre-defined classifiers are widely used in crime fighting and anti-terrorism surveillance. Relates to matrix Human Rights and Ethical Issues – Networked Data Analysis and Data Transfer Analysis.

In general uncertain intelligence information from the internet or from other data communication has to be interpreted, integrated, analyzed, and evaluated to provide awareness of the situation, using situational and threat assessment methods.
Social Network Analysis (SNA) is a method of statistical investigation of the patterns of communication within groups. The basic concept of the method is the hypothesis that the way members of a group communicate with each other and members of other groups reveals important information about the group itself. The investigations are performed via the method of structural analysis, which is based on a mathematical graph model consisting of nodes and edges that model the actors and the communication, respectively, within the group. In addition all kinds of weights can be introduced in the model, which represent the probability of an event to take place within the model. Bayesian belief networks (BBN) is one such uncertainty modeling and information fusion methodology to exploit uncertain causal relationships between large collections of variables.

Data analysis tools are widely used crime fighting tools in the law enforcement community. However, not much is known about the effectiveness of the analysis tools. The effectiveness of the tools depends heavily on the quality of the pre-

defined classifiers, which in the end have a large impact on the final outcome of the researched data.

Data analysis tools can potentially, if used in an appropriate way, help police decision makers and front-line police officers to benefit from the crime data analysis products, where the tools are the main theme in each policing strategy that aims to reduce crime, to prevent further offending, and to apprehend criminals.
Many data analysis tools have been used to stop terrorist programs under the U.S. government. The programs in which these tools were used have been discontinued due to controversy over whether they violate the 4th Amendment to the United States Constitution.

1.18 Location tracking of cellular phones/smartphones
Mobile phone tracking is a technology that locates and tracks the position of a moving phone. A mobile phone is located using the signal that phone emits to communicate with nearby antenna towers. Signal strengths are then studied to determine how close the phone is to antenna towers and a specific location.

How does it function?
The technology of locating is based on measuring power levels and antenna patterns and uses the concept that a powered mobile phone always communicates wirelessly with one of the closest base stations, so knowledge of the location of the base station implies the cell phone is nearby.

Advanced systems determine the sector in which the mobile phone resides and roughly estimate also the distance to the base station. Further approximation can be done by interpolating signals between adjacent antenna towers. Qualified services may achieve a precision of down to 50 meters in urban areas where mobile traffic and density of antenna towers (base stations) is sufficiently high. Rural and desolate areas may see miles between base stations and therefore determine locations less precisely.

19. (Mobile) Phone tapping
Phone tapping or wire tapping is the monitoring of telephone calls and Internet access by covert means. Technical details of these techniques are not in the public domain. For fixed phones and Internet lines, a crime investigator has to get access to the computer network of an internet provider or phone provider (which is usually combined). Generally, a court order is required. How this works exactly is unclear but phone records, when calls are made and to whom, and a log-file about Internet activity and e-mail can be supplied relatively easily.

Mobile phone tapping requires phone-tapping software that needs to be installed as an invisible application on a smart-phone (which usually requires manual installation on the pone itself). Once such software is installed nearly all information on the phone can be accessed, including but not limited to: tracing calls, receiving copies of text messages, access to the contact list, view Internet sites that were visited, receiving copies of photos, GPS tracking, listening to both sides of a telephone

conversation, and recording sounds in the environment when the telephone is not operated. The software can be bought from the Internet and can be as cheap as 60$.

- Wilcox, T (2008). Tapping your cell Phone. Verkregen op 20 oktober, 2012: http://www.wthr.com/story/9346833/tapping-your-cell-phone?clienttype=printable
- Shanina S & Heinsbroek J, 2012, Phone-Tapping Software, Exercise for education in: WM0823, Security and Technology (in Dutch).

ANNEX 2 EXTENDED EXPLANATION OF METHODOLOGY FOR SCORING USABILITY OF TECHNOLOGIES IN SCENARIO

Coen van Gulijk, DELFT

Introduction

This section describes the first attempt to design a usability assessment for surveillance technologies in SURVEILLE. It gives an indication of the 'usability' or perhaps the 'suitability' of surveillance technologies in the prevention and prosecution of serious crime. The exercise is coined *usability assessment*. This work is specifically designed to assess the technologies that are mentioned in the MERPOL scenario in SURVEILLE but could be used in another context as well. The usability of surveillance devices of any type depends on the context in which a device is applied and the purpose for which it is used. Nevertheless, an *a priori* assessment is useful when the police or any other crime-fighting organization makes decisions about which technologies to select.

It is important that the reader understands that the development of a framework for usability assessment is a research line in the SURVEILLE project that is still ongoing. This first framework for the assessment is based on current knowledge about factors or attributes; further refinement will follow in later deliverables for SURVEILLE such as deliverables 3.2, 3.3, 3.4, 3.5 and 3.9.

Method

A semi-quantitative method is used for the usability assessment. Robert Alexy's weight formula for competing principles, utilized by the EUI in the legal assessment of surveillance technologies, was taken as an example of how abstract concepts (fundamental rights) can be balanced through a semi-quantitative method. A similar semi-quantitative method is constructed here. Numeric values, or scores, are assigned to attributes of surveillance technologies relating to usability. These attributes, to some extent, follow from research topics in the SURVEILLE project.

Four factors are used in this scoring method. They were derived from a set of rules for the assessment of public health surveillance systems in the US {1, 2} and attributes that were identified in the SURVEILLE project. They are: effectiveness, cost, privacy-by-design and excellence.

Our current knowledge about the technologies and the maturity of the framework only allow for nominal scoring methods on these four factors. That means that certain predefined attributes are either present or not present in a given technology. So a comparative judgment about whether a particular technology scores better than another technology on the same attribute is not included. At least for the time being, the method excludes ordinal, interval, ratio or absolute judgment scales.

The assignment of factors is as follows. Effectiveness is scored from 0 to 3, depending on which three effectiveness attributes are present. Cost is also scored from 0 to 3, and ditto for privacy by design features. Excellence is a separate attribute, which scores either 0 or 1. The scores of the four factors are added together which yields an overall usability score ranging from 0 to 10.

In the security or crime-control domain, there is no clear definition of what effective surveillance technology is. As part of this research, the following definition is adopted within the SURVEILLE project:

> *Effective*: the technology has the technical capacity to deliver increased security, and when employed for a defined goal within the necessary context (good location, trained operators, a larger security system, etc.) achieves the intended outcome.

This definition is important because it assumes that the technology is used 'correctly' in the sense that trained operators are able to create optimal conditions for the technology to function adequately. This is held to be true for all attributes: all technologies function as they should.

Attributes for scoring

This section describes the attributes for scoring on the usability assessment and the conditions for scoring. The four factors that are treated are effectiveness, cost, privacy by design and excellence. Ten attributes are assigned to these factors.

EFFECTIVENESS

Three attributes are described that are either present or not present in the surveillance technology. They are: delivery, simplicity, and sensitivity.

Attribute 1 follows from the definition of effectiveness: delivery. The assessment of this attribute hinges on the question whether a particular technology, in a particular context, given that it is applied in the correct way yields a useful outcome. Useful outcomes are: detection of prohibited conduct, items or substances, sufficient facts for justifying pre-emptive actions and sufficient leads to continue an investigation with the same or other surveillance technologies. When there is evidence of prior successes or success is reasonably achievable this attribute scores a 1, else it is 0.

Attribute 2 is related to the effort in surveillance operations: simplicity. Simplicity relates to the structure and ease of operation that a surveillance technology provides. As a general rule, the simpler a surveillance technology, the more useful it is in crime control. When the structure required for a surveillance operation involves more than one external expert and/or stakeholders, it is considered to be a complex structure operation. When the surveillance technology has proven ease of use in prior cases or its ease of use is reasonably achievable this attribute scores a 1.

Attribute 3 is the sensitivity of the technology. The sensitivity relates to the likelihood of error. A technology may deliver information that is open for multiple interpretations or provides vague data that enables a wrong conclusion. For

instance, recording a telephone conversation could be done by phone tapping or by CCTV cameras. The phone tap is more sensitive when it comes to recording the exact conversation making it less likely that false conclusions are drawn than with CCTV; in contrast, the CCTV footage is more sensitive when it comes to understanding whether someone was coerced into performing the phone call. When there is evidence of a high rate of errors in the interpretation, or errors could reasonably be expected, this attribute scores a 1. When there is no evidence about the error rate and an assessment cannot be made it also scores 0. Else it scores 1.

COST

Cost scores give an indication of the financial burden of a surveillance technology. Since surveillance technologies vary widely and their use is varied it is hard to give precise indications for the cost of technologies. Future work in SURVEILLE strives to produce a cost model of surveillance technologies. In this first scoring method a very rough indication is used. Three attributes are used here. As before, this is a nominal scoring method so either the attribute is present or it is not. The attributes are: purchase costs, personnel requirements, and additional resources. They are explained below.

Attribute 4 is the purchase cost. Purchase cost is the money spent on buying the equipment and associated systems. Unfortunately, it is not so easy to determine which equipment is expensive and which is not. Prices may vary per vendor and budgets may vary per crime control unit. The money spent during an operation is not the same as the purchase cost; it is also determined by the frequency of use, the total lifetime, and maintenance costs. Without further research, cost per operation is too difficult to assess and purchase cost is used as a proxy. Here, we consider the equipment list from deliverable 2.6 in which the cost range is estimated to vary from surveillance technologies costing several hundreds of euros up to one million euro. Price ranges upward of 50.000 euros are considered to be expensive, or at least not easily allocated. This scores a 0; if prices are lower, a 1 is scored.

The cost in attribute 5 is related to the number of personnel involved in the use of the surveillance technology. Personnel, in this attribute, are restricted to personnel of the organization that performs the surveillance task. This can be within a single police force, a single national coordination team or a dedicated technical surveillance team. Note that it is assumed that personnel received training and is experienced with the technology. When two or less persons are involved in handling the intelligence gathering process in an operation, it scores a 1. Else, this attribute is 0.

Attribute 6 indicates whether external partners are required in the use of the surveillance technology. These could be commercial partners or vendors that operate the surveillance technology that need to be contracted for their assistance. Regardless of the amount of money spent, it is a financial complication that drives cost up. So when a third party has to be contracted this attribute scores a 0, else it scores 1.

PRIVACY BY DESIGN

Privacy by design is an important design parameter in surveillance technology but it is by no means straightforward. This topic is often associated with the protection of personal data but that does not necessarily depend on the surveillance technology itself but the way in which data-storage systems are organized. Nevertheless, some basic attributes assist this analysis. They are observation of persons, collateral intrusion and hardware and software protection.

Attribute 7 is related to what surveillance technology actually observes: people or objects. When a surveillance technology only observes chemicals, objects or data, it scores a 1. When it records people, their behavior or records their voices, it scores a 0.

Attribute 8 is related to collateral intrusion. The question is whether a surveillance technology can perform targeted surveillance or whether it records a larger group of people where only one is relevant. When it is targeted to the individual or individuals under investigation this attribute scores a 1, else it scores a 0.

Attribute 9 indicates whether it is difficult, from a technological perspective, to insert privacy-by-design rules. This can be either in the design of the hardware or software for the system. When it is difficult, from a technological point of view to adhere to privacy-by-design principles this attribute scores 0, else it scores 1.

EXCELLENCE

Excellence is a single attribute for the usability of the system. This attribute can add a single point to the usability assessment. This is when a given technological system has proven its use beyond reasonable doubt. Explicit examples include iris-scans or DNA sampling for personal identification; their correctness and excellence have been proven both scientifically and successfully applied in crime fighting without doubt. Therefore, when a surveillance technology has proven its use beyond doubt, it scores a 1, else it scores 0.

Application to MERPOL Scenario

19 technologies are treated in the matrix related to the crime investigation scenario provided by Merseyside Police. Each of the technologies were analyzed through usability assessment. These estimates were made to the best of the abilities of the technological analyst, based on the information in the scenario. The results are shown in table 1. A brief description of the analysis follows below.

The first two technologies, CCTV systems, can be expected to yield results at a relatively low cost but it is hard to protect privacy. Results could include: identification of associates, proof of illegal activities, or proof of association. Some of these facts may be used in court cases. Photography scores higher than the CCTV since it does not indiscriminately record all persons in an area, also, photos that do not provide relevant facts can easily be omitted from the investigation which makes photos less privacy sensitive.

Depending on the conditions in which they are used, sound recordings can be very targeted and useful. Sound recording in public places makes any form of privacy by design useless since many people may be overheard and it may be hard to use as evidence in court since the identity of the individual has to be proven beyond doubt.

The micro-helicopter, in this application, is related to the CCTV surveillance instruments discussed earlier and has a similar usability score.

AIS detection, submarine explosives detection, gas chromatography, whole body scanners and luggage screening are a group of highly specialized surveillance technologies. As a rule, they are relatively expensive, and rely on support by third parties. This makes them less usable for a crime-fighting unit; however, their performance in terms of successful identification of illegal goods is typically excellent.

Data analysis techniques give a crime-fighting unit an idea about the crime network and a profile for the associated partners relatively cheaply (though the training level of operatives might have to be high). These facts will probably enable justification for the use of additional surveillance but it is unknown whether they can be used as evidence in courtrooms. With data traffic, it is relatively easy to implement privacy-by-design rules because data can be targeted and stored selectively.

Phone tapping and locating is a targeted activity that can give results fast. Also, privacy-by-design rules can work very well. To the current analyst it is unknown whether these methods should be marked as 'excellent' but they might be.

Conclusion

A relatively straightforward semi-quantitative usability assessment was designed to rate how well surveillance technologies are suited for use in crime investigations.

		EFFICIENCY			COST			PRIVACY-B-D			EX.
		#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
TECHNOLOGY AND USE	SCORE										
Visual spectrum dome–zoom, tilt, rotate (public place – used overtly)	6	1	1	1	1	1	0	0	0	0	1
Visual spectrum dome–zoom, tilt, rotate (public place – used covertly)	7	1	1	1	1	1	1	0	0	0	1
Covert photography in public place	9	1	1	1	1	1	1	0	1	1	1
Sound recording bug/s in target's home address.	8	1	1	1	1	1	1	0	1	0	1
Sound recording bug/s in target's vehicle.	8	1	1	1	1	1	1	0	1	0	1

Sound recording bug/s on public transport used by target.	3	0	1	0	1	1	0	0	0	0	0
Sound recording bug/s in police vehicle transporting target following arrest.	4	0	1	0	1	1	1	0	0	0	0
Sound recording bug/s in target's prison cell.	5	0	1	0	1	1	1	0	1	0	0
Video camera mounted on a platform micro helicopter	6	1	1	0	1	1	1	0	0	0	1
AIS ship location detection and identification	5	0	0	1	1	0	0	1	1	1	0
Explosives detection near harbor	4	1	0	0	0	0	0	1	1	1	0
Gas chromatography drugs detector	8	1	1	1	0	1	0	1	1	1	1
Whole body scanner eqo	6	0	1	1	0	1	0	0	1	1	1
Luggage screening technology	7	1	1	1	0	1	0	0	1	1	1
money laundering technology	7	1	0	1	1	1	1	1	0	1	0
Networked data analysis	7	1	0	1	1	1	1	1	0	1	0
Data transfer analysis (name recognition) technology	6	0	0	1	1	1	1	1	0	1	0
Location tracking of cellular phones/smartphones	7	0	1	1	1	1	0	1	1	1	0
Mobile phone (including contact data) tap	8	1	1	1	1	1	0	1	1	1	0

Four factors of the technology are assessed: effectiveness, cost, privacy-by-design and excellence. These are subdivided into ten attributes. The resulting scores for the technologies vary between 3 and 9, indicating that the method is broadly able to capture the different features of a technology. The judgments in this work are from the analyst alone. It is advisable, however, to make these judgments in teams of experts.

The current information about the scenario, the technology and interpretation of efficiency and effectiveness in the security domain is relatively abstract. This led to the choice for a nominal scoring method: an attribute is either present or it is not whereas in real life, the situation is typically more complicated. Therefore, it is best to think of this method as a preliminary method one that could develop further over time.

(1} Klaucke DN, Buehler JW, Thacker SB, Parrish RG, Trowbridge FL, Berkelman RL, 1988, Guidelines for Evaluating Surveillance Systems, *MMWR* **37(S-5)**;1-18.

{2} German RR, Lee LM, Horan JM, Milstein RL, Petrowski CA, Waller MN, Birkhead GS, 2001, Updated Guidelines for Evaluating Public Health Surveillance Systems, *MMWR* **50(RR13)**;1-35.

ANNEX 3. FUNDAMENTAL RIGHTS TECHNOLOGY ASSESSMENT SHEETS (EUI)

These fundamental rights assessment sheets[57] were produced by the EUI team within SURVEILLE, under the guidance of Prof Martin Scheinin. On the basis of templates produced by Dr Juha Lavapuro and Prof Tuomas Ojanen, each assessment sheet was drafted by an individual member of the team. The drafts were then discussed by the whole team towards reaching consensus about the scoring of the application of a technology on a given fundamental right. The scores generated for each technology are primarily a result of two factors: first the weight, or importance of the particular fundamental right affected in the context of the scenario, and second, an assessment of the degree of intrusion into that right. Each of these two factors is marked as 1, 2 or 4. A score of '1' represents a low, '2' a medium and '4' a high relative weighting of the fundamental right. A score of '1' represents a low, '2' a medium and '4' a high (or serious) level of intrusion into that right.

These two scores are multiplied with each other and then with a value assessing the reliability of the state of the law, to factor in and compensate for the abstraction from a specific jurisdiction. The scale is as follows: ½ is the lowest value indicating the understanding of a lay person; ¾, is a medium value resulting from the agreement within the expert team, in the absence of clear case law; and 1 is the highest value, deriving from the assessment of the expert team supported by reference to clear case law.

If at least a minimal level of intrusion into a fundamental right is identified, the resulting score can range from 1/2 to 16, where the values 1/2 and 16 signify the lowest and the greatest intrusion, respectively. However, any values above 10 represent an impermissible interference with the given fundamental right, even when a very high security benefit would be obtained. The rationale lies in the comparison between the usability and fundamental rights score. Accordingly, even the highest usability score, which weighs 10, cannot legitimise the intrusion into a fundamental right weighing more than 10. When the usability score is lower than 10, any fundamental rights intrusion above that score also indicates an impermissible measure.

The drafter of each sheet is indicated by the initials of the person as follows:

JA Jonathan Andrew
JL Juha Lavapuro
TO Tuomas Ojanen
MGP Maria Grazia Porcedda

[57] For a discussion of the metholodology to assess the fundamental rights impact of surveillance technologies, see section 2.3.3 in this SURVEILLE Deliverable D2.6 and, for earlier SURVEILLE work, Maria Grazia Porcedda, 'Paper Establishing Classification of Technologies on the Basis of Their Intrusiveness into Fundamental Rights. SURVEILLE Deliverable D2.4', Florence, European University Institute (2013).

MS Martin Scheinin
MV Mathias Vermeulen

The description of technologies are either drafted by the TU Delft team, or a revised form of the same.

1 Closed-circuit television (CCTV): Visual spectrum dome–zoom, tilt, rotate (public place – used overtly) (TO)

1.1. Description of the surveillance technology (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. Relates to matrix Human Rights and Ethical Issues - Visual Spectrum Dome-zoom, tilt, rotate (public place – used (c)overtly)

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 pre-set amount of time before they become automatically archived.

Vulnerability of CCTV cameras

- CCTV cameras can be observed and are vulnerable for destruction. Some CCTV cameras come in dust-tight, explosion proof housing.
- The lens of the camera is vulnerable for sprayed substances that make the image blurry.
- Lasers can blind or damage the cameras
- The CCTV system is vulnerable for hostile intrusion. Wireless IP cameras are in this respect much more vulnerable to hostile intrusion than wired cameras.

1.2. Fundamental rights affected

The following fundamental rights may be affected by the ***overt*** use of CCTV in public places:

1.1.1 The right to respect for private life (Article 7 of the CFREU; Article 8 of the ECHR; and Article 17 of ICCPR)

In light of the case law by the European Court of Human Rights (the ECtHR), there are a number of elements relevant to a consideration of whether the *overt* use of CCTV in public places amounts to an interference with private life under Article 8 of the European Convention on Human Rights (ECHR).[58]

On the one hand, the case law of the ECtHR shows that not all private actions in the public context fall under the scope of application of the right to private life. The ECtHR has explicitly ruled that the monitoring of the actions of an individual in a public place by the use of photographic equipment that does not record the visual data does not, as such, give rise to an interference with the individual's private life.[59]

On the other hand, the ECtHR has held that Article 8 protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world, and it may include activities of a professional or business nature.[60] There is, therefore, a zone of interaction of a

[58] Convention for the Protection of Human Rights and Fundamental Freedoms, as Amended by Protocols No 11 and 14, CETS n° 005, p. 4 November 1950.

[59] See e.g. Case of Herbecq and the Association "Ligue Des Droits De L'homme" V. Belgium, n. 32200/96 and 32201/96, European Court of Human Rights, 14 January 1998 at 92.

[60] See, for example, Case of Friedl V. Austria, n. 15225/89, European Court of Human Rights, 31 January 1995.

person with others, even in a public context, which may fall within the scope of "private life". [61]

Moreover, the ECtHR has noted as follows:

> "There are a number of elements relevant to a consideration of whether a person's private life is concerned in measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain."[62]

From these premises, the ECtHR has held that the compilation of data by security services on particular individuals, even without the use of covert surveillance methods, constituted an interference with the applicants' private lives. [63] Furthermore, the ECtHR has ruled that the disclosure to the media for broadcast use of video footage of the applicant whose suicide attempt was caught on CCTV was a serious interference with the applicant's private life, notwithstanding that the applicant was in a public street. In making this conclusion, the ECtHR attached, first, weight to the fact that the applicant was not there for the purposes of participating in any public event and he was not a public figure. Moreover, while the actual suicide attempt was neither recorded nor therefore disclosed, the footage of the immediate aftermath was recorded and disclosed directly to the media for further broadcasting and publication purposes. Therefore, while just being filmed by CCTV did not give rise to privacy considerations under Article 8, it was the disclosure of the CCTV material, revealing the applicant's actions to the public in a manner in which he could never have foreseen, that constituted " a serious interference with the applicant's right to respect for his private life".[64]

Finally, ECtHR has ruled that right to private life is applicable if the police is regulating the security camera so that it could take clear footage of the applicant for the purposes of using that footage in criminal investigation.[65]The ECtHR has also held that the permanent recording of the voices of suspects made while they answered questions in a public area of a police station as police officers listened to them was regarded as the processing of personal data about them amounting to an

---

[61] See, Case of P. G. And J. H. V. The United Kingdom, n. 44787/98, European Court of Human Rights, 25 December 2001 at § 56.

[62]Ibid., at § 57.

[63] Case of Amann V. Switzerland, n. 27798/95, European Court of Human Rights, 16 February 2000 at §§ 65-67; Case of Rotaru V. Romania, n. 28341/95, European Court of Human Rights, 4 May 2000 at §§ 43-44.

[64] Case of Peck V. The United Kingdom, n. 44647/98, European Court of Human Rights, 28 January 2003.

[65] Ibid.

interference with their right to respect for their private lives. This interpretation is in line with broader jurisprudence where the ECtHR has consistently held that the *covert* taping of telephone conversations falls within the scope of Article 8 in both aspects of the right guaranteed, namely, respect for private life and correspondence.[66]

In conclusion, while the mere use of CCTV in public places does not, as such, necessarily give rise to privacy considerations, the *overt* use of CCTV in public places can be seen as constituting an interference with private life under Article 8 of the ECHR in the following situations:

- Material obtained from the overt use of CCTV in public place is used by the police or other (law enforcement) authorities in an unforeseen or intrusive manner;
- Material obtained from the overt use of CCTV is disclosed to the public and/or to the media for further broadcasting and publication purposes; and
- The overt use of CCTV material involves processing of personal data whenever the individual is identified (see in more detail below).

As the meaning and scope of the rights guaranteed in the CFREU must be regarded as corresponding to rights in the ECHR by virtue of Article 52, paragraph 3, of the CFREU, the above considerations also apply to Article 7 of the CFREU.

1.1.2 The right to personal data (Article 8 of the CFREU; Article 8 of the ECHR; Article 17 of the ICCPR)

The right to personal data is protected by the Article 8 of the CFREU which states in paragraph 1 that ”e]veryone has the right to the protection of personal data concerning him or her”. According to the case law of the Court of Justice of the European Union, that fundamental right is closely connected with the right to respect of private life expressed in Article 7 of the Charter.[67]

---

[66] Case of Klass and Others V. Germany n. 5029/71, European Court of Human Rights, 6 September 1968 at § 41.

[67] See e.g. Case C-275/06, Productores De Música De España (Promusicae) V Telefónica De España Sau, n. Court of Justice of the European Union, 29 January 2008 at § 63. The link between privacy and data protection is also reflected in recitals 10 to 12, and Article 1(1) of Directive 95/46/Ec of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Data Protection Directive), OJ L 281, p. 31-50, 23 Novemebr 1995. See also in this respect, the Volkszählungsurteil, n. 1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1, German Bundesverfassungsgericht (Federal Constitutional Court), 15 December 1983. See also more recently, 1 Bvr 256/08, 1 Bvr 263/08, 1 Bvr 586/08, n. Bundesverfassungsgericht (German Federal Constitutional Court), 2 March 2010. Available on: www.bundesverfassungsgericht.de.

The right to the protection of personal data is also guaranteed by Article 8 of the ECHR, Article 17 of the ICCPR, and the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which has been ratified by all the EU Member States. The ECtHR has held that the protection of personal data is of fundamental importance to a person's enjoyment of his right to respect for private life.[68]

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter the Data Protection Directive)[69] features as the major EU instrument designed to remove the obstacles to the free movement of data without diminishing the protection of personal data. According to the European Court of Justice, the Data Protection Directive adopted "at Community level, the general principles which already formed part of the law of the Member States in the area in question".[70] Recitals 10, 11 and 12 of that Directive also state that the aim of the Data Protection Directive is to ensure a high level of protection of fundamental rights.

The data protection directive applies to "any operation or set of operations which is performed upon personal data, "called "processing " of data. According to Article 3 (1) it applies "to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a fling system or are intended to form part of a filing system".

The definition of "personal data", as well as the "processing of personal data" are central to a consideration of whether there is an interference with the right to personal data by the overt use of CCTV in public places.

Article 2 of the Data Protection Directive defines "personal data" and the "processing of personal data" as follows:

> "(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;" and
>
> "(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by

[68] See Case of S. And Marper V. The United Kingdom, n. 30562/04 and 30566/04, European Court of Human Rights.
[69] Data Protection Directive.
[70] See Case C-369/98, the Queen V Minister of Agriculture, Fisheries and Food, Ex Parte Trevor Robert Fisher and Penny Fisher, n. Court of Justice of the European Union, 14 September 2000 at § 34.

transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."

Furthermore, the Data Protection Directive lays down specific conditions when such processing will be permitted, in respect to "sensitive data" such as those revealing "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning sex or health life".[71]

It follows from the above premises that the CCTV material can be seen as constituting personal data to the extent that this material allows, directly or indirectly, the identification of the individual. Moreover, the use of CCTV can be regarded as constituting "the processing of personal data" to the extent that the CCTV material is subject to e.g. "collection", "recording" or "dissemination". The same applies to the extent that the CCTV material is analyzed or otherwise "processed" by the police or other authorities for law enforcement purposes.

Furthermore, if the CCTV material is interpreted so as to associate race, ethnicity, religion or sexual orientation with the person whose image has been recorded, this material constitutes "sensitive data". Such data may be processed only if certain strict conditions under Article 8 of the Data Protection Directive are met. As the scenario deals with 'neutral' individuals and no such associations are made, we are assuming that there is no processing of sensitive data..

The ECtHR has also held that privacy considerations may arise once any systematic or permanent record about an individual comes into existence. Therefore, files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method.[72] It can, therefore, be concluded that the *overt* use of CCTVs in public places amounts to an interference with the individuals rights *both* to private life *and* to the protection of personal data.

1.3. Limitations to rights involved

The affected rights are not absolute, in the sense that they permit restrictions or limitations that serve a legitimate aim, are prescribed by the law in a precise and foreseeable manner, and are both necessary and proportionate in nature.

Article 8(2) ECHR expressly recognises the possibility of limitations to that right, as does Article 9 of Convention No 108 in respect of the right to protection of personal data. Article 52 of the CFREU likewise deals with the criteria for the limitation of rights. The requirement that the grounds on which the processing of personal data is allowed shall be clearly and precisely laid down by the law is also one of the fundamental principles pertaining to the protection of personal data. This is, *inter*

[71] Data Protection Directive, at article 8.
[72] See Rotaru V. Romania at §§ 43 44.

alia, indicated by Article 8 of the CFREU which explicitly requires that personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

Furthermore, the Data Protection Directive contains specific provisions concerning the grounds for legitimate processing of data (Article 7), and lays down when such processing will be permitted, in respect to 'sensitive data' such as those revealing 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning sex or health life' (Article 8).

By and large, the overt use of CCTV in public places does not usually result in intrusions of the core of these rights. Hence, intrusions by the overt use of CCTVs may be permissible but the legitimacy of the intrusion ultimately depends on the relationship between the level of intrusion and the importance towards the aim of that intrusion. The greater the degree of non-satisfaction of, or detriment to, a fundamental right, the greater must be the importance of satisfying the other legitimate aim.

As this assessment is not geared towards a specific jurisdiction, no assessment is possible concerning the requirement that the requirement that any intrusion into fundamental rights is 'prescribed by the law'. Any reader is, therefore, reminded that the use of any specific surveillance technology will make it necessary to verify that there was a proper legal basis for the measures undertaken.

1.4. Level of intrusion

The severity of fundamental rights intrusion created by the overt use of CCTVs in public places depends on number of different aspects.

First of all, it should be kept in mind that the mere monitoring of the actions of an individual in a public place by the use of CCTV does not, as such, necessarily at all give rise to an interference with the individual's private life.

Private life considerations may arise, however, once any systematic or permanent recording of the CCTV material occurs or when such material is analysed or otherwise ”processed” by the police or other authorities. On such occasions, the overt use of CCTV in public places can be seen as interfering with the individuals rights both to privacy and to the protection of personal data. It can, furthermore, be assessed that whereas the level of intrusion remains low with regard the right to private life (1), medium level of intrusion can be established with regard to the protection of personal data (2).

If the CCTV material reveals the individual's racial or ethnic origin or other categories of sensitive data, the level of intrusion into the right to personal data can be regarded as being high (4).

- An individual's liberty right of being able to decide what information to share and with whom may as such be considered to fall close to the core of the right to private life and hence to be of significant (medium or high)

weight. However, the weight of this right is usually weaker in public contexts, especially in situations involving the overt use of CCTV.

- The protection of personal data has been understood to have fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the ECHR.[73]
- The need for data protection safeguards is all the greater where such data are used for police purposes.[74]

Regarding the intensity of these restrictions, at least following considerations must be taken into account:

- Although the right to private life is applicable in public contexts, the overt use of CCTV in public places can usually be understood as intruding at the outer border of the right to private life and to the protection personal data. After all, a person in a public place will inevitably be seen by some member of the public who is also present. Monitoring by such technological means as CCTV of the same public scene is of a similar character, especially in cases involving the overt use of CCTV because the individual is then, at least in principle, aware of being seen and/or filmed by CCTV. In terms of the right to privacy in general, this kind of intrusion is low (1)
- Regarding the right to protection of personal data, the intrusion can also be regarded as being low, except in cases in which the CCTV material reveals sensitive data. The strict requirements set forth for the processing of sensitive data reflect the severity of intrusion, the intensity of which can be assessed to be at least medium (2).[75]

As to the reliability of these considerations, there exists well established case law about privacy rights, data protection and freedom of communication. There is even one judgment by the ECtHR specifically dealing with privacy considerations pertaining to the use of CCTV in public place.[76] The state of law can thus be regarded as being clear and reliable (1).

1.5. Quantification

	Abstract weight[77]	***Intrusiveness***[78]	***Reliability of the state of***	***Value***[80]

[73] See S. And Marper V. The United Kingdom.
[74] Ibid.
[75] See Case of M. M. V. The United Kingdom, n. 24029/07 European Court of Human Rights, 29 April 2013.
[76] Peck V. The United Kingdom.
[77] Scale: 1 low, 2 medium, 4 high.

			law[79]	
Data protection	***1***	***2***	***1***	***2***
Right to private life	***1***	***1***	***1***	***1***

1.6. Further considerations

This assessment does not include the right to a fair trial. Hence, the possible use of the recordings as evidence in the trial has not been addressed.

This assessment focuses on intrusion into the rights of the actual target. As CCTV will be used overtly in public space, it is very likely that other persons will be seen and recorded as well. Even if these persons are not identified, this will mean an intrusion into their right to private life. If the persons are identified, also data protection issues arise. That said, the overt nature of CCTV reduces the intrusion also in respect of these persons.

In the above assessment, the weight of the fundamental rights in question has been assessed in relation to surveillance without judicial authorization. If the surveillance measure is authorised by the judiciary, the weight (and the overall score) should be multiplied by 3/4.

[78] Scale: as above.

[80] Scale: when applied by an expert team, from ¾ to 16. All values above 10 (i.e., either 12 or 16) will mean that no security benefit from the use of the technology as described can legitimise its use due to fundamental rights consequences.

[79] Scale: ½ low (lay person), ¾ medium (expert team), 1 high (expert team with reference to clear case law).

2 Closed-circuit television (CCTV): Visual spectrum dome–zoom, tilt, rotate (public place – used covertly) (TO)

2.1 Description of the surveillance technology

See description in sheet # 1.

2.2 Fundamental rights affected

The following fundamental rights may be affected by the ***covert*** use of CCTV in public places:

2.2.1 The right to respect for private life (Article 7 of the CFREU; Article 8 of the ECHR; and Article 17 of ICCPR).

In light of the case law by the European Court of Human Rights (the ECtHR), there are a number of elements relevant to a consideration of whether the *covert* use of CCTV's in public places amounts to an interference with private life under Article 8 of the ECHR.

On the one hand, the case law of the ECtHR shows that not all private actions in the public context fall under the scope of application of the right to private life. The ECtHR has explicitly ruled that the monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life.[81]

On the other hand, the ECtHR has held that Article 8 protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world, and it may include activities of a professional or business nature.[82] There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life".[83]

Moreover, the ECtHR has noted as follows:

> "There are a number of elements relevant to a consideration of whether a person's private life is concerned in measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private life considerations may arise, however,

[81] See e.g. Case of Herbecq and the Association "Ligue Des Droits De L'homme" V. Belgium at 92.
[82] See, for example, Friedl V. Austria.
[83] See, P. G. And J. H. V. The United Kingdom.

once any systematic or permanent record comes into existence of such material from the public domain."[84]

From these premises, the ECtHR has held that the compilation of data by security services on particular individuals, even without the use of covert surveillance methods, constituted an interference with the applicants' private lives. [85] Furthermore, the ECtHR has ruled that the disclosure to the media for broadcast use of video footage of the applicant whose suicide attempt was caught on CCTV was a serious interference with the applicant's private life, notwithstanding that the applicant was in a public street. In making this conclusion, the ECtHR attached, first, weight to the fact that the applicant was not there for the purposes of participating in any public event and he was not a public figure. Moreover, while the actual suicide attempt was neither recorded nor therefore disclosed, the footage of the immediate aftermath was recorded and disclosed directly to the media for further broadcasting and publication purposes. Therefore, while just being filmed by CCTV did not give rise to privacy considerations under Article 8, it was the disclosure of the CCTV material, revealing the applicant's actions to the public in a manner in which he could never have foreseen, that constituted " a serious interference with the applicant's right to respect for his private life".[86]

Finally, ECtHR has ruled that right to private life is applicable if the police is regulating the security camera so that it could take clear footage of the applicant for the purposes of using that footage in criminal investigation.[87] The ECtHR has also held that the permanent recording of the voices of suspects made while they answered questions in a public area of a police station, as police officers listened to them, was regarded as the processing of personal data about them amounting to an interference with their right to respect for their private lives. This interpretation is in line with broader jurisprudence where the ECtHR has consistently held that the *covert* taping of telephone conversations falls within the scope of Article 8 in both aspects of the right guaranteed, namely, respect for private life and correspondence.[88]

In conclusion, while the mere use of CCTV in public places does not. as such, necessarily give rise to privacy considerations, the *covert* use of CCTV in public places can be seen as constituting an interference with private life under Article 8 of the ECHR in the following situations:

- Material obtained from the covert use of CCTV in public place is used by the police or other (law enforcement) authorities in an unforeseen or intrusive manner;

[84] Ibid., at § 57.
[85] Amann V. Switzerland at §§ 65-67; Rotaru V. Romania at §§ 43 44.
[86] Peck V. The United Kingdom.
[87] Ibid.
[88] See already Klass and Others V. Germany at § 41.

- Material obtained from the covert use of CCTV is disclosed to the public and/or to the media for further broadcasting and publication purposes; and
- The covert use of CCTV material involves processing of personal data whenever the individual is identified (see in more detail below).

As the meaning and scope of the rights guaranteed in the CFREU must be regarded as corresponding to rights in the ECHR by virtue of Article 52, paragraph 3, of the CFREU, the above considerations also apply to Article 7 of the CFREU.

2.2.2 The right to personal data (Article 8 of the CFREU; Article 8 of the ECHR)

The right to personal data is protected by the Article 8 of the CFREU which states in paragraph 1 that "[e]veryone has the right to the protection of personal data concerning him or her". According to the case law of the Court of Justice of the European Union, that fundamental right is closely connected with the right to respect of private life expressed in Article 7 of the Charter.[89]

The right to the protection of personal data is also guaranteed by Article 8 of the ECHR, Article 17 of the ICCPR, and the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which has been ratified by all the EU Member States. The ECtHR has held that the protection of personal data is of fundamental importance to a person's enjoyment of his right to respect for private life.[90]

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter the Data Protection Directive)[91] features as the major EU instrument designed to remove the obstacles to the free movement of data without diminishing the protection of personal data. According to the European Court of Justice, the Data Protection Directive adopted "at Community level, the general principles which already formed part of the law of the Member States in the area in question".[92] Recitals 10, 11 and 12 of that Directive also state that the aim of the Data Protection Directive is to ensure a high level of protection of fundamental rights.

The data protection directive applies to "any operation or set of operations which is performed upon personal data", called "processing" of data. According to Article 3 (1) it applies "to the processing of personal data wholly or partly by automatic

[89] See e.g. C-275/06 - Promusicae at § 63. The link between privacy and data protection is also reflected in recitals 10 to 12, and Article 1(1) of the Data Protection Directive. See also in this respect, the Volkszählungsurteil. See also, more recently, 1 Bvr 256/08, 1 Bvr 263/08, 1 Bvr 586/08. Available on: www.bundesverfassungsgericht.de.

[90] See S. And Marper V. The United Kingdom at § 103.

[91] Data Protection Directive.

[92] See C-369/98 - Fisher at § 34.

means, and to the processing otherwise than by automatic means of personal data which form part of a fling system or are intended to form part of a filing system".

The definition of "personal data", as well as the "processing of personal data" are central to a consideration of whether there is an interference with the right to personal data by the covert use of CCTV in public places.

Article 2 of the Data Protection Directive defines "personal data" and the "processing of personal data" as follows:

> "(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;" and
>
> "(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."
>
> Furthermore, the Data Protection Directive lays down specific conditions when such processing will be permitted, in respect to "sensitive data" such as those revealing "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning sex or health life".[93]

It follows from the above premises that the CCTV material can be seen as constituting personal data to the extent that this material allows, directly or indirectly, the identification of the individual. Moreover, the use of CCTV can be regarded as constituting "the processing of personal data" to the extent that the CCTV material is subject to e.g. "collection", "recording" or "dissemination". The same applies to the extent that the CCTV material is analyzed or otherwise "processed" by the police or other authorities for law enforcement purposes.

Furthermore, if the CCTV material is interpreted so as to associate race, ethnicity, religion or sexual orientation with the person whose image has been recorded, this material constitutes "sensitive data". Such data may be processed only if certain strict conditions under Article 8 of the Data Protection Directive are met. As the scenario deals with 'neutral' individuals and no such associations are made, we are assuming that there is no processing of sensitive data.

[93] Data Protection Directive, at article 8.

The ECtHR has also held that privacy considerations may arise once any systematic or permanent record about an individual comes into existence. Therefore, files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method.[94] It can, therefore, be concluded that the *covert* use of CCTVs in public places amounts to an interference with the individuals rights *both* to private life *and* to the protection of personal data.

2.3 Limitations to rights involved

The affected rights are not absolute, in the sense that they permit restrictions or limitations that serve a legitimate aim, are prescribed by the law in a precise and foreseeable manner, and are both necessary and proportionate in nature.

Article 8(2) ECHR expressly recognises the possibility of limitations to that right, as does Article 9 of Convention No 108 in respect of the right to protection of personal data. Article 52 of the CFREU likewise deals with the criteria for the limitation of rights. The requirement that the grounds on which the processing of personal data is allowed shall be clearly and precisely laid down by the law is also one of the fundamental principles pertaining to the protection of personal data. This is, *inter alia*, indicated by Article 8 of the CFREU which explicitly requires that personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

Furthermore, the Data Protection Directive contains specific provisions concerning the grounds for legitimate processing of data (Article 7), and lays downs when such processing will be permitted, in respect to 'sensitive data' such as those revealing 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning sex or health life' (Article 8).

By and large, the covert use of CCTV in public places does not usually result in intrusions of the core of these rights. Hence, intrusions by the covert use of CCTVs may be permissible but the legitimacy of the intrusion ultimately depends on the relationship between the level of intrusion and the importance towards the aim of that intrusion. The greater the degree of non-satisfaction of, or detriment to, a fundamental right, the greater must be the importance of satisfying the other legitimate aim.

As this assessment is not geared towards a specific jurisdiction, no assessment is possible concerning the requirement that the requirement that any intrusion into fundamental rights is 'prescribed by the law'. Any reader is, therefore, reminded that the use of any specific surveillance technology will make it necessary to verify that there was a proper legal basis for the measures undertaken.

[94] See Rotaru V. Romania.

2.4 Level of intrusion

The severity of fundamental rights intrusion created by the covert use of CCTVs in public places depends on number of different aspects.

First of all, it should be kept in mind that the mere monitoring of the actions of an individual in a public place by the use of CCTV does not, as such, necessarily at all give rise to an interference with the individual's private life.

Private life considerations may arise, however, once any systematic or permanent recording of the CCTV material occurs or when such material is analysed or otherwise ”processed” by the police or other authorities. On such occasions, the covert use of CCTV in public places can be seen as clearly interfering with the individuals rights both to privacy and to the protection of personal data. It can, furthermore, be assessed that whereas the level of intrusion remains low with regard the right to private life (1), medium level of intrusion can be established with regard to the protection of personal data (2).

If the CCTV material reveals the individual’s racial or ethnic origin or other categories of sensitive data, the level of intrusion into the right to personal data can be regarded as being high (4).

- Individual’s liberty right of being able to decide what information to share and with whom may as such be considered to fall close to the core of the right to private life and hence to be of significant (medium or high) weight. However, the weight of this right is usually weaker in public contexts. The covert use of CCTVs somewhat increases the level of intrusion.
- Protection of personal data has been understood to have fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the ECHR.[95]
- The need for data protection safeguards is all the greater where such data are used for police purposes.[96]

Regarding the intensity of these restrictions, at least following considerations must be taken into account:

- Although the right to private life is also applicable in public contexts, the use of CCTV in public places can usually be understood as intruding at the outer border of the right to private life and to the protection personal data. After all, a person in a public place will inevitably be seen by some member of the public who is also present. Monitoring by such technological means as CCTV of the same public scene is of a similar character.

[95] See S. And Marper V. The United Kingdom.
[96] Ibid.

- However, the covert use of CCTV entails that the individual cannot be aware of being filmed by CCTV. In terms of the right to privacy in general, this kind of intrusion can be regarded as medium. (2)
- With regard the right to protection of personal data, the intrusion can also be assessed to be medium, except in cases in which CCTV material reveals sensitive data. The strict requirements set forth for the processing of sensitive data reflect the severity of intrusion, the intensity of which can be regarded as being high (4).[97]

As to the reliability of these considerations, there exists well-established case law about privacy rights, data protection and freedom of communication. There is even one judgment by the ECtHR specifically dealing with privacy considerations pertaining to the use of CCTV in public place.[98] In addition, there are a number of judgments by the ECtHR on the use of covert surveillance methods in light of Article 8 of the ECHR. The state of law can thus be regarded as clear and reliable (1).

2.5 Quantification

	Abstract weight[99]	***Intrusiveness***[100]	***Reliability of the state of law***[101]	***Value***[102]
Data protection	***2***	***4***	***1***	***8***
Right to private life	***1***	***2***	***1***	***2***

2.6 Further considerations

This assessment does not include the right to a fair trial. Hence, the possible use of the recordings as evidence in the trial has not been addressed.

This assessment focuses on intrusion into the rights of the actual target. As CCTV will be used in public space, it is very likely that other persons will be seen and recorded as well. Even if these persons are not identified, this will mean an intrusion into their right to private life. If the persons are identified, also data protection issues arise.

---

[97] See M. M. V. The United Kingdom.
[98] Peck V. The United Kingdom.
[99] Scale: 1 low, 2 medium, 4 high.
[100] Scale: as above.
[101] Scale: ½ low (lay person), ¾ medium (expert team), 1 high (expert team with reference to clear case law).
[102] Scale: when used by expert team, from ¾ to 16. All values above 10 (i.e., either 12 or 16) will mean that no security benefit from the use of the technology as described can legitimise its use due to fundamental rights consequences.

In the above assessment, the weight of the fundamental rights in question has been assessed in relation to surveillance without judicial authorization. If the surveillance measure is authorised by the judiciary, the weight (and the overall score) should be multiplied by 3/4.

3 Covert photography in a public space (MV)

3.1 Description of the surveillance technology (TU Delft)

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).

Vulnerability of CCTV cameras

- CCTV cameras can be observed and are vulnerable for destruction. Some CCTV cameras come in dust-tight, explosion proof housing.
- The lens of the camera is vulnerable for sprayed substances that make the image blurry.
- Lasers can blind or damage the cameras
- The CCTV system is vulnerable for hostile intrusion. Wireless IP cameras are in this respect much more vulnerable to hostile intrusion than wired cameras.

3.2 Fundamental rights affected

The following fundamental rights may be affected by covert photography in a public space:

3.2.1 The right to respect for private life (Article 7 of the CFREU; Article 8 of the ECHR; and Article 17 of ICCPR).

In light of the case law by the European Court of Human Rights (the ECtHR), there are a number of elements relevant to consider whether covert photography in a public place amounts to an interference with the right to private life under Article 8 of the ECHR.

The ECtHR has explicitly ruled that the monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual

data does not, as such, give rise to an interference with the individual's private life.[103] According to the Court "a person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character".[104]

However, the ECtHR has also held that Article 8 protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world, and it may include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life". [105] If a picture was taken, the European Commission of Human Rights – and later the Court – have assessed to which extent the photographs taken in a public place relate to 'private' or 'public' matters. The Commission has ruled that the taking of photographs and their retention of a participant at a sit-in by the police does not constitute an interference with the right to private life, since the photographs "relate to a public incident" (in this case, a manifestation of several persons in a public place, in which the applicant was voluntarily taking part). [106] A different situation could arise if photos taken at a public place depict a person in "scenes from her daily life, thus involving activities of a purely private nature such as engaging in sport, out walking, leaving a restaurant or on holiday". [107] The first situation could be seen as an occasion "when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner", while the second situation is covered by a person's reasonable expectation to privacy. According to the Court, this last criterion may be "a significant, although not necessarily conclusive, factor". [108] In the case of Peck v. UK, being filmed by CCTV in a public place did not give rise to privacy considerations under Article 8, but the disclosure of the CCTV material to the media for further broadcasting and publication purposes, which revealed the applicant's actions to the public in a manner in which he could never have foreseen, constituted "a serious interference with the applicant's right to respect for his private life".[109]

Hence, the Court's assessment also differs whether the material thus obtained was envisaged for "a limited use" or "was likely to be made available to the general public". In the case of Friedl v. Austria the Commission found for instance that one of the reasons why there was no interference with the right to private life was because the pictures were "solely taken for the purposes (…) of recording the character of

[103] See e.g. Case of Herbecq and the Association "Ligue Des Droits De L'homme" V. Belgium at 92.
[104] Ibid.
[105] See P. G. And J. H. V. The United Kingdom.
[106] Friedl V. Austria. There had been complaints that the participants of the sit-in had been 'camping' and cooking at the site, which resulted in obstruction of pedestrian traffic and a lot of trash. See also Peck, where the ECtHR attached weight to the fact that the applicant was not there for the purposes of participating in any public event. Peck V. The United Kingdom.
[107] Case of Von Hannover V. Germany, n. 59320/00, European Court of Human Rights, 24 June 2004 at § 61.
[108] P. G. And J. H. V. The United Kingdom at § 56.§
[109] Peck V. The United Kingdom.

the manifestation and the actual (sanitary) situation at the place in question" or "recording the conduct of the participants in the manifestation in view of ensuing investigation proceedings for offences (against the Road Traffic Regulations)". [110] The Commission has earlier found that the use of individual photographs in the course of a criminal investigation does not constitute an interference with the right to private life where the photographs concerned had either been previously provided voluntarily in connection with applications for official documents, or had been obtained on the occasion of a previous arrest, and were not made available to the general public *nor used for any purpose other than the criminal proceedings in question*.[111]

Private life considerations may arise once any "systematic or permanent record" comes into existence of such material from the public domain".[112] The ECtHR has held that the compilation of data by security services on particular individuals, even without the use of covert surveillance methods, constituted an interference with the applicants' private lives.[113] This is different compared to a situation when "the individual persons on the photographs taken remain anonymous in that no names were noted down, the personal data recorded and photographs taken were not entered into a data processing system, and no action was taken to identify the persons photographed on that occasion by means of data processing".[114]

Finally, the European Court of Human Rights has highlighted the threat of secret interferences with the right to private life in its case law under Article 8.[115] Since secret measures take place without the knowledge of the individual who has been put under surveillance, seeking an effective remedy against this interference is rendered more difficult or even prevented. Often the individual concerned cannot take a direct part in any review proceedings of the interference either.[116] The Court has noted that this has an impact beyond the individual. In such a context, "widespread suspicion and concern among the general public that secret surveillance powers are being abused" would not be unjustified according to the Court.[117] In view of the risk of abuse intrinsic to "any system of secret surveillance", the Court has claimed that any such system "must be based on a law that is particularly precise, especially as the technology available for use is continually

[110] Friedl V. Austria. There had been complaints that the participants of the sit-in had been 'camping' and cooking at the site, which resulted in obstruction of pedestrian traffic and a lot of trash.
[111] Case of Lupker and Others V. The Netherlands, n. 18395/91, European Court of Human Rights, 7 December 1992. (Emphasis added.)
[112] P. G. And J. H. V. The United Kingdom at § 56.
[113] Amann V. Switzerland at §§ 65-67; Rotaru V. Romania at §§ 43 44.
[114] Friedl V. Austria at § 50.
[115] See Case of Weber and Saravia V. Germany, n. 54934/00, European Court of Human Rights, 29 June 2006 at § 93; Case of Association for European Integration and Human Rights and Ekimdzhiev V. Bulgaria, n. 62540/00, European Court of Human Rights, at § 75; Case of Liberty and Others V. The United Kingdom, n. 58243/00, European Court of Human Rights, 01 July 2008 at § 62; Case of Iordachi V. Moldova, n. 25198/02, European Court of Human Rights, 10 February 2009 at § 39.
[116] See also Klass and Others V. Germany at § 52.
[117] Case of Kennedy V. The United Kingdom, n. 26839/05, European Court of Human Rights, 18 August 2010 at § 124.

becoming more sophisticated."[118] The European Court of Human Rights developed a strict set of minimum safeguards that should be set out in statute law in order to avoid abuses of power "in cases of secret measures of surveillance": the nature of the offences which may give rise to the surveillance; a definition of the categories of people liable to be under surveillance; a limit on the duration of the surveillance; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which the data should be deleted.[119]

In conclusion, while the mere taking of photographs in public places does not automatically give rise to privacy considerations, the *covert* making of photographs in public places can be seen as constituting an interference with private life under Article 8 of the ECHR in the following situations:

- Material obtained from the covert use of photographs in a public place is used by the police or other (law enforcement) authorities in an unforeseen or intrusive manner;
- Material obtained from the covert use of photographs is disclosed to the public and/or to the media for further broadcasting and publication purposes; and
- The covert use of photographs involves processing of personal data whenever the individual is identified (see in more detail below).

As the meaning and scope of the rights guaranteed in the CFREU must be regarded as corresponding to rights in the ECHR by virtue of Article 52, paragraph 3, of the CFREU, the foregoing considerations also apply to Article 7 of the CFREU.

3.2.2 The right to personal data (Article 8 of the CFREU; Article 8 of the ECHR; Article 17 of the ICCPR)

The right to personal data is protected by the Article 8 of the CFREU which states in paragraph 1 that "[e]veryone has the right to the protection of personal data concerning him or her". According to the case law of the Court of Justice of the European Union, that fundamental right is closely connected with the right to respect of private life expressed in Article 7 of the Charter.[120] The Data Protection Directive applies to "any operation or set of operations which is performed upon personal data", called "processing" of data. According to Article 3 (1) it applies "to the processing of personal data wholly or partly by automatic means, and to the

[118] See Case of Kopp V. Switzerland, n. 23224/94, European Court of Human Rights, 25 March 1998 at § 72; Weber and Saravia V. Germany at § 93.
[119] Weber and Saravia V. Germany at § 95.
[120] See e.g. C-275/06 - Promusicae at § 63. The link between privacy and data protection is also reflected in recitals 10 to 12, and Article 1(1) of the Data Protection Directive. See also in this respect, the German Bundesverfassungsgericht (Federal Constitutional Court) Volkszählungsurteil. See also, more recently, 1 Bvr 256/08, 1 Bvr 263/08, 1 Bvr 586/08. Available on: www.bundesverfassungsgericht.de.

processing otherwise than by automatic means of personal data which form part of a fling system or are intended to form part of a filing system".

The definition of "personal data", as well as the "processing of personal data" are central to a consideration of whether there is an interference with the right to personal data by the covert use of photography in public places. Article 2 of the Data Protection Directive defines "personal data" and the "processing of personal data" as follows:

> "(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;" and
>
> "(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."

Furthermore, the Data Protection Directive lays down specific conditions when such processing will be permitted, in respect to "sensitive data" such as those revealing "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning sex or health life".[121] Since every photo of a person can reveal at least a person's racial or ethnic origin, and perhaps a person's health status, such pictures can be considered sensitive data as defined in Art. 8 (1) of the Directive, with the result that these data may not be processed without the individual's consent.[122] According to the Data Protection Working Party 29, the term ""data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership" is to be understood that not only data which by its nature contains sensitive information is covered by this provision, but also data from which sensitive information with regard to an individual can be concluded".[123] This is not a straightforward task. A picture that shows a person praying in a particular way reveals religious beliefs, but this is not necessarily true for a picture of a person in front of a mosque or a cathedral.

It follows from the foregoing premises that the photographs can be seen as constituting personal data to the extent that this material allows, directly or indirectly, the identification of the individual. Moreover, the use of photographs can be regarded as constituting "the processing of personal data" to the extent that the

[121] Data Protection Directive, at article 8.
[122] Article 29 Data Protection Working Party, 'Advice Paper on Special Categories of Data ("Sensitive Data")', (Brussels, 2011) at 8.
[123] Ibid.

photographs are subject to e.g. ”collection”, ”recording” or ”dissemination”. The same applies to the extent that photographs is analysed or otherwise ”processed” by the police or other authorities for law enforcement purposes.

The ECtHR has also held that privacy considerations may arise once any systematic or permanent record about an individual comes into existence. Therefore, files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method.[124] It can, therefore, be concluded that the *covert* use of photography in public places amounts to an interference with the individuals rights *both* to private life *and* to the protection of personal data.

3.3 Limitations to rights involved

The affected rights are not absolute, in the sense that they permit restrictions or limitations that serve a legitimate aim, are prescribed by the law in a precise and foreseeable manner, and are both necessary and proportionate in nature.

Article 8(2) ECHR expressly recognises the possibility of limitations to that right, as does Article 9 of Convention No 108 in respect of the right to protection of personal data. Article 52 of the CFREU likewise deals with the criteria for the limitation of rights. The requirement that the grounds on which the processing of personal data is allowed shall be clearly and precisely laid down by the law is also one of the fundamental principles pertaining to the protection of personal data. This is, *inter alia*, indicated by Article 8 of the CFREU which explicitly requires that personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

Furthermore, the Data Protection Directive contains specific provisions concerning the grounds for legitimate processing of data (Article 7), and lays downs when such processing will be permitted, in respect to ‘sensitive data’ such as those revealing ‘racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning sex or health life’ (Article 8).

By and large, the covert use of photography in public places does not usually result into intrusions of the core of these rights. Hence, intrusions by covertly taking photographs may be permissible but the legitimacy of the intrusion ultimately depends on the relationship between the level of intrusion and the importance towards the aim of that intrusion. The greater the degree of non-satisfaction of, or detriment to, a fundamental right, the greater must be the importance of satisfying the other legitimate aim.

A literal reading of the Data Protection Directive would suggest that every picture of a person would constitute ‘sensitive data’, since a picture shows – at the very least – the colours of somebody’s skin. However, it could be argued that the ‘sensitivity’ of a particular picture should be determined according to its context and not simply

[124] See Rotaru V. Romania.

based on an enumerative list under Art. 8(1). This approach was suggested in a paper by Simitis for the Council of Europe in 1999. In order to determine the 'sensitivity' of the picture, "the specific interests of the controller (i.e the law enforcement official) as well as of the potential recipients of the data, the aims for which the data are collected, the conditions of the processing and its possible consequences for the persons are factors that, put together, allow both the range and effects of the processing to be discerned and thus to determine its degree of sensitivity. An evaluation of the sensitivity requires hence more than a mere look at the data".[125] The issue of sensitivity would arise, for instance, if the storing of a picture is interpreted so as to associate race, ethnicity, religion or sexual orientation with the person whose image has been recorded.

As this assessment is not geared towards a specific jurisdiction, no assessment is possible concerning the requirement that any intrusion into fundamental rights is 'prescribed by the law'. Any reader is, therefore, reminded that the use of any specific surveillance technology will make it necessary to verify that there was a proper legal basis for the measures undertaken.

3.4 Level of intrusion

The severity of fundamental rights intrusion created by the covert use of photographs in public places depends on a number of different aspects.

Private life considerations may arise once any systematic or permanent recording of the CCTV material occurs or when such material is analysed or otherwise "processed" by the police or other authorities. On such occasions, the covert use of photography can be seen as clearly interfering with the individual's rights both to privacy and to the protection of personal data. It can, furthermore, be assessed that whereas the level of intrusion remains low with regard the right to private life (1), medium level of intrusion can be established with regard to the protection of personal data (2).

If the storing of a picture is interpreted so as to associate race, ethnicity, religion or sexual orientation with the person whose image has been recorded., the level of intrusion into the right to personal data can be regarded as being high.

- Individual's liberty right of being able to decide what information to share and with whom may as such be considered to fall close to the core of the right to private life and hence to be of significant (medium or high) weight. While the weight of this right is usually weaker in public contexts, the covert use of photography somewhat increases the level of intrusion.

[125] Spiros Simitis, 'Revisiting Sensitive Data', Council of Europe (1999). Available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Report_Simitis_1999.pdf.

- Protection of personal data has been understood to have fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the ECHR.[126]
- The need for data protection safeguards is all the greater where such data are used for police purposes.[127]

Regarding the intensity of these restrictions, at least following considerations must be taken into account:

- Although the right to private life is also applicable in public contexts, the covert photography of public places can usually be understood as intruding at the outer border of the right to private life and to the protection personal data. After all, a person in a public place will inevitably be seen other members of the public who are also present.
- However, the covert use of photography results in the individual not being aware of being photographed. In terms of the right to privacy in general, this kind of intrusion can be regarded as medium. (2)
- With regard the right to protection of personal data, the intrusion can also be assessed to be medium, except in cases where the photograph is interpreted so as to associate race, ethnicity, religion or sexual orientation with the person whose image has been recorded. The strict requirements set forth for the processing of sensitive data reflect the severity of intrusion, the intensity of which can be regarded as being high (4).[128]

As to the reliability of these considerations, there exists well-established case law about privacy rights and data protection. In addition, there are a number of judgments by the ECtHR on the use of covert surveillance methods in light of Article 8 of the ECHR. The state of law can thus be regarded as clear and reliable (1).

3.5 Quantification

	Abstract weight[129]	***Intrusiveness***[130]	***Reliability of the state of law***[131]	***Value***[132]

[126] See S. And Marper V. The United Kingdom.
[127] Ibid.
[128] See M. M. V. The United Kingdom.
[129] Scale: 1 low, 2 medium, 4 high.
[130] Scale: as above.
[131] Scale: ½ low (lay person), ¾ medium (expert team), 1 high (expert team with reference to clear case law).

Data protection	***2***	***4***	***1***	***8***
Right to private life	***1***	***2***	***1***	***2***

3.6 Further considerations

This assessment does not include the right to a fair trial. Hence, the possible use of the photographs as evidence in the trial has not been addressed.

This assessment focuses on intrusion into the rights of the actual target. As the photograph will be taken in public, it is highly likely that other persons will be present in the picture as well. Even if these persons are not identified, this will mean an intrusion into their right to private life. If the persons are identified, data protection issues arise as well.

In the above assessment, the weight of the fundamental rights in question has been assessed in relation to surveillance without judicial authorization. If the surveillance measure is authorised by the judiciary, the weight (and the overall score) should be multiplied by 3/4.

[132] Scale: when used by expert team, from ¾ to 16. All values above 10 (i.e., either 12 or 16) will mean that no security benefit from the use of the technology as described can legitimise its use due to fundamental rights consequences.

4 Sound recording bug at home (MV & JL)

4.1 Description of the surveillance technology (TU Delft)

Audio surveillance devices, like phone bugs, distant audio recorders or cell-phone audio bugs[133] 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.

Phone sound bugs are probably the most common audio surveillance devices. A phone sound bug is simply a small audio spying device that is usually attached to the inside of the phone and performs audio surveillance. It sends the digital audio signals during a conversation to another location to stream the voice of the suspect and the contacted person to a monitoring device.

4.2 Fundamental rights affected

The following fundamental rights may be affected by the use of sound recording bugs at a target's home:

[133] Cell-phone audio surveillance is a technology that uses a normal cell phone, which is equipped with a device that enables an external connection and tracking of all conversations made over that cell phone. Together with the installed GPS system also the location of the caller can be monitored.

4.2.1 The right to respect for private life (Article 7 of the CFREU; Article 8 of the ECHR; and Article 17 of ICCPR).

In Vetter v. France the court found the eavesdropping on conversations through bugs a "serious" interference with the right to private life, especially when the main goal of the bug is to intercept one or more person's communications through the device, which was comparable to the interception of one's communications.[134] Accordingly, such a measure should be based on a law that is particularly precise. According to the Court, "it is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated".[135] The law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which public authorities are entitled to resort to such covert measures. In the case of Khan v. UK for instance, there existed no statutory system to regulate the use of covert listening devices and as such could not be considered to be in accordance with the law. In Vetter v. France, the Court highlighted that the provisions in the code of criminal procedure which guaranteed the secrecy of correspondence did not make any reference to "sound", which suggested that the law only regulated the "interception of correspondence through telecommunications". Such an intrusive measure cannot be based "on general enactments or principles or else from an analogical interpretation of legislative provisions - or court decisions - concerning investigative measures different from telephone tapping, notably searches and seizure of property. Although plausible in itself, such "extrapolation" does not provide sufficient legal certainty in the present context".[136] Besides this common requirement, the Court has indicated further minimum safeguards to which covert surveillance measures need to adhere to. Domestic regimes must specify the offences which may justify an interception order, subjective limitations to particular categories of people, chronological limits of the monitoring, the procedure to be followed for examining, using, sharing and storing the data obtained, the precautions to be taken when communicating these data to third parties, the circumstances in which the information can be erased or destroyed, and the provision of prior or ex post facto review by a judge or other genuinely (objectively and subjectively) impartial authority, factually and hierarchically independent from the body in charge of imposing such measures, empowered to certify that recordings were genuine and reliable. Should national legislation omit to refer to some of the above-mentioned elements, the Court will extend its assessment to domestic case-law which may be relevant to safeguarding individuals.

Both Khan and Vetter were recorded while visiting the bugged house of a third person. The place of the bug did not influence the Court's decision on the legality of the interference. Yet, it is important to point out that the Court has interpreted the

[134] See Case of Khan V. The United Kingdom, n. 35394/97, European Court of Human Rights, 12 May 2000 at § 26; Case of Vetter V. France, n. 59842/00, European Court of Human Rights, 31 May 2005 at § 20.
[135] Case of Kruslin V. France, n. 11801/85, European Court of Human Rights, 24 April 1990 at § 33.
[136] Ibid., at § 34.

notion of a 'home' – just as the term 'privacy' – in a flexible way, as a narrow interpretation of the term home "could give rise to the same risk of inequality of treatment as a narrow interpretation of the notion of "private life".[137] The notion of 'home' has covered a second house, a holiday home or another place providing longterm accommodation;[138] a house belonging to another person being occupied, for a significant period or on an annual basis, by someone else;[139] business premises, when there is no clear distinction between a person's office and private residence or between private and business activities; [140] a company's registered office, branches or other business premises;[141] and non-traditional residences such as caravans.[142]

4.2.2 The right to personal data (Article 8 of the CFREU; Article 8 of the ECHR, Article 17 of the ICCPR).

The right to personal data is protected by the Article 8 of the CFREU, as well as Article 8 of the ECHR and on the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which has been ratified by all the EU Member States. To the extent that an individual can be identified, the recording of sound constitutes personal data. In Directive 95/46/EC, of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data personal data are defined as "any information relating to an identified or identifiable natural person", also referred to as the "data subject. Moreover, the purpose of Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such data being defined as "any information relating to an identified or identifiable individual" (Article 2)

---

[137] See Case of Niemietz V. Germany, n. 13710/88, European Court of Human Rights, 16 December 1992 at § 30.

[138] "The Court notes in this context that it may not always be possible to draw precise distinctions, since a person may divide his time between two houses or form strong emotional ties with a second house, treating it as his home." Case of Demades V. Turkey, n. 16219/90, European Court of Human Rights, 31 July 2003 at § 32.

[139] Case of Mentes and Others V. Turkey, n. 23186/94, European Court of Human Rights, 28 November 1997 at § 73.

[140] Niemietz V. Germany at § 30.

[141] Case of Stes Colas Est and Others V. France, n. 37971/97, European Court of Human Rights, 16 April 2002 at § 41.

[142] Case of Buckley V. The United Kingdom, n. 20348/92, European Court of Human Rights, 25 September 1996 at §§ 53 54.

Data protection rights are also protected by Article 8 of the ECHR and Article 17 of the ICCPR. As stated by the ECtHR, private-life considerations may arise once any systematic or permanent record about an individual comes into existence. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method.[143] Furthermore, in the case of P.G. and J.H. v. the United Kingdom, ECtHR held that a recording and analysis of prison cell conversations for the purpose of recording the voice of the target for identification, was regarded as concerning the processing of personal data about the individuals.[144]

The ECtHR has considered it essential, in the context of the recording and communication of criminal record data as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures; as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.[145]

4.3 Limitations to rights involved

The affected rights are not absolute, in the sense that they permit restrictions or limitations that serve a legitimate aim, are prescribed by the law in a precise and foreseeable manner, and are both necessary and proportionate in nature. The conditions for restrictions into the affected fundamental rights are spelled out in, inter alia, CFREU Art. 52, ECHR Art. 8 and ICCPR Art. 17.

The sound recording bugs placed at a person's home might result in intrusions of the core of those rights.[146] Alternatively, if assessed as highly intrusive but not affecting the inviolable core of a fundamental right, intrusions by these bugs may nevertheless not be permissible but the legitimacy of the intrusion ultimately depends on the relationship between the level of intrusion and the importance towards the aim of that intrusion. The greater the degree of non-satisfaction of, or detriment to, a fundamental right, the greater must be the importance of satisfying the other legitimate aim.

As this assessment is not geared towards a specific jurisdiction, no assessment is possible concerning the requirement that any intrusion into fundamental rights is 'prescribed by the law'. Any reader is, therefore, reminded that the use of any

[143] See Rotaru V. Romania.

[144] See P. G. And J. H. V. The United Kingdom.

[145] See M. M. V. The United Kingdom.

[146] Intrusions into the essential core of a fundamental right, or into absolute rights that allow for no limitations, could in principle result in an aggregate score of 16 where the weight of the right and the level of intrusion are not even addressed separately. For the sace of consistency, these assessment sheets nevertheless apply the two-step approach of assessing separately the weight of the fundamental right and the degree of intrusion, resulting in the maximum score of 4 x 4 = 16.

specific surveillance technology will make it necessary to verify that there was a proper legal basis for the measures undertaken. Moreover, with regard to protection of personal data, the ECtHR has considered it essential, in the context of the recording and communication of criminal record data as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures; as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.[147]

4.4 Level of intrusion

In the abstract, and even without applying the construction of an inviolable core of fundamental rights (that would directly give the score of 16), the sound recording bugs in a person's home rights have a severe impact on the right to private life (4) and significant weight with regard to protection of personal data (4). This is based on following key points.

- Individual's liberty right of being able to decide what information to share and with whom may as such be considered to fall close to the core of the right to private life.
- The weight of this right is very strong in a person's home – or another analogously intimate non-public space.
- Protection of personal data has been understood to have fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the ECHR.[148]
- The need for data protection safeguards is all the greater where the such data are used for police purposes.[149]

As to the intensity of these restrictions, at least following considerations must be taken into account:

- Based on case law of the ECtHR, the intrusion caused by sound recording bugs is more susceptible of interfering with a person's right to respect for private life than for instance GPS surveillance, because it discloses more information on a person's conduct, opinions or feelings. According to our assessment, the intensity of intrusion is severe (4).
- As regards the right to protection of personal data, the intrusion may be severe especially if organized in systematic fashion. In the context of the recording and communication of criminal record data as in telephone tapping, secret surveillance and covert intelligence-gathering, the ECtHR has emphasized it to be essential, to have clear, detailed rules that

[147] See M. M. V. The United Kingdom.
[148] See S. And Marper V. The United Kingdom.
[149] Ibid.

provide sufficient guarantees against the risk of abuse and arbitrariness. The strict requirements set forth for processing of personal data in criminal investigation reflect the severity of the intrusion.[150] The intensity of intrusion is severe (4).

The above considerations result in the maximum score of 16 (4 x 4), the same as if the conclusion had been drawn directly on the basis of positioning the situation within the inviolable core of privacy and data protection rights.

As to the reliability of the above considerations, there exists widely established case law about privacy rights, data protection and freedom of communications. In terms of protection of personal data, the state of law is clear and reliable (1). With regard to the general right to private life in one's own home, no directly applicable case exists. However, there are analogously applicable legal materials. The reliability of our intrusiveness analysis is also hear high (1).

4.5 Quantification

	Abstract weight[151]	***Intrusiveness***[152]	***Reliability of the state of law***[153]	***Value***[154]
Data protection	***4***	***4***	***1***	***16***
Right to private life	***4***	***4***	***1***	***16***

4.6 Further considerations

This assessment does not include the right to a fair trial. Hence, the possible use of the recordings as evidence in the trial has not been addressed.

This assessment focuses on intrusion into the rights of the actual target. As the bug will be used in the person's home, it is possible that voices of other persons will be heard and recorded as well. Even if these persons are not identified, this will mean an intrusion into their right to private life. If the persons are identified, also data protection issues arise.

[150] See M. M. V. The United Kingdom.
[151] Scale: 1 low, 2 medium, 4 high.
[152] Scale: as above.
[153] Scale: ½ low (lay person), ¾ medium (expert team), 1 high (expert team with reference to clear case law).
[154] Scale: when used by expert team, from ¾ to 16. All values above 10 (i.e., either 12 or 16) will mean that no security benefit from the use of the technology as described can legitimise its use due to fundamental rights consequences.

In the above assessment, the weight of the fundamental rights in question has been assessed in relation to surveillance without judicial authorization. If the surveillance measure is authorised by the judiciary, the weight (and the overall score) should be multiplied by 3/4.

5 Sound recording bug in target's vehicle (JL)

5.1 Description of the surveillance technology

See description in sheet # 4.

5.2 Fundamental rights affected

The following rights are typically affected by the use of sound recording bugs in target's vehicle:

5.2.1 The right to personal data (Article 8 of the CFREU; Article 8 of the ECHR).

To the extent that an individual can be identified, the recordings of sounds in target's vehicle constitute personal data.

The right to personal data is explicitly protected by the Article 8 of the CFREU as well as an attribute to the privacy right protected by Article 8 of the ECHR. In Directive 95/46/EC, personal data are defined as "any information relating to an identified or identifiable natural person", also referred to as the "data subject. Moreover, the purpose of Council of Europe's Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such data being defined as "any information relating to an identified or identifiable individual" (Article 2)

Data protection rights are protected also by article 8 of the ECHR and article 17 of the ICCPR which provide for the broader right to the respect of private life/privacy. As stated by the ECtHR, private-life considerations may arise once any systematic or permanent record about an individual comes into existence. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method.[155] Furthermore, in the case of *P.G. and J.H. v. the United Kingdom*, ECtHR held that a recording and analysis of prison cell conversations for the purpose of recording the voice of the target for identification, was regarded as concerning the processing of personal data about the individuals.[156] Finally, in the case of *Uzun v. Germany,* the ECtHR held that installation of GPS tracking vehicle to a car belonging to a third person for the purpose of tracking the movements of the target constituted interference with private life because, among others, the tracking data was recorded, systematically collected and stored for criminal investigation.[157]

[155] See Rotaru V. Romania.
[156] See P. G. And J. H. V. The United Kingdom.
[157] See Case of Uzun V. Germany, n. 35623/05, European Court of Human Rights, 2 September 2010 at § 51.

5.2.2 The right to respect for private life (Article 7 of the CFREU; Article 8 of the ECHR; and Article 17 of ICCPR)

According to established case law private life is a broad term covering, among others, a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world.[158] More specifically, the ECtHR found in the case of *Uzun v. Germany* that a surveillance via GPS tracking device that had been installed a car in order to track down target's movement, interfered with target's right to private life. In fact, the court stated that acoustical surveillance methods were more susceptible of interfering with a person's right to respect for private life, "because they disclose more information on a person's conduct, opinions or feelings".[159] For these reasons, it is manifestly clear that sound recording bugs in target's vehicle amount to an intrusion into a person's right to private life.

5.3 Limitations to the rights involved

The affected rights are not absolute, in the sense that they permit restrictions or limitations that serve a legitimate aim, are prescribed by the law in a precise and foreseeable manner, and are both necessary and proportionate in nature. However, the interference must be prescribed by law and be justified according to pursuit of a legitimate aim. The conditions for restrictions into the affected fundamental rights are spelled out in, inter alia, CFREU Art. 52, ECHR Art. 8 and ICCPR Art. 17.

The sound recording bugs in target's vehicle do not result into intrusions into the core of those rights. This being the case, intrusions may be legitimate. In these situations, the legitimacy of the intrusion depends ultimately on the relationship between the level of intrusion and the importance of the aim of that intrusion. The greater the degree of non-satisfaction of, or detriment to, a fundamental right, the greater must be the importance of satisfying the other legitimate aim.

As this assessment is not geared towards a specific jurisdiction, no assessment is possible concerning the requirement that any intrusion into fundamental rights is 'prescribed by the law'. Any reader is, therefore, reminded that the use of any specific surveillance technology will make it necessary to verify that there was a proper legal basis for the measures undertaken. Moreover, the ECtHR has considered it essential, in the context of the recording and communication of criminal record data as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures; as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the

[158] See, for example, Friedl V. Austria.
[159] See Uzun V. Germany at § 52.

integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.[160]

5.4 Level of intrusion

In the abstract, the sound recording bugs in target's car endanger rights that have at least medium but probably severe weight with regard to the right to private life (2-4) and significant weight with regard to protection of personal data (4). This is based on following key points.

- Individual's liberty right of being able to decide what information to share and with whom may as such be considered to fall close to the core of the right to private life.
- Weight of this right is usually weaker in public contexts.
- Protection of personal data has been understood to have fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the ECHR.[161]
- The need for data protection safeguards is all the greater where the such data are used for police purposes.[162]

As to the intensity of these restrictions, at least following considerations must be taken into account:

- Based on case law of the ECtHR, the intrusion caused by sound recording bugs in target's vehicle is more susceptible of interfering with a person's right to respect for private life than for instance GPS surveillance, because it discloses more information on a person's conduct, opinions or feelings. With regard to person's reasonable expectations about the level of privacy of conversations, a private car is analogous to private houses. In any case, the intrusion is more severe than intrusion caused by mere GPS tracking of target's vehicle or its photographing in public places. According to our assessment, the intensity of intrusion is severe (4).
- As regards the right to protection of personal data, the intrusion may be severe especially if organized in systematic fashion. In the context of the recording and communication of criminal record data as in telephone tapping, secret surveillance and covert intelligence-gathering, The ECtHR has emphasized it to be essential, to have clear, detailed rules that provide sufficient guarantees against the risk of abuse and arbitrariness. The strict requirements set forth for processing of personal data in criminal investigation reflect the severity of the intrusion.[163] The intensity of intrusion is severe (4).

[160] See M. M. V. The United Kingdom.
[161] See S. And Marper V. The United Kingdom.
[162] Ibid.
[163] See M. M. V. The United Kingdom.

As to the reliability of these considerations, there exists widely established case law about privacy rights, data protection and freedom of communications. In terms of protection of personal data, the state of law is clear and reliable (1). With regard to the general right to private life in one's own car, no directly applicable case exists. However, there are analogously applicable legal materials. The reliability of our intrusiveness analysis is medium.

5.5 Quantification

	Abstract weight	***Intrusiveness***	***Reliability of the state of law***	***Total value***
Data protection	***2***	***4***	***1***	***8***
Right to private life	***2-4***	***4***	***3/4***	***6-12***

5.6 Further considerations

This assessment does not include the right to a fair trial. Hence, the possible use of the recordings as evidence in the trial has not been addressed.

This assessment focuses on intrusion into the rights of the actual target. As the bug will be used in the target's private car, it is unlikely but possible that voices of other persons will be heard and recorded as well. Even if these persons are not identified, this will mean an intrusion into their right to private life. If the persons are identified, also data protection issues arise.

In the above assessment, the weight of the fundamental rights in question has been assessed in relation to surveillance without judicial authorization. If the surveillance measure is authorised by the judiciary, the weight (and the overall score) should be multiplied by 3/4.

6 Sound recording bug on public transport used by target (JL)

6.1 Description of the surveillance technology (TU Delft)

See description in sheet # 4.

6.2 Fundamental rights affected

The following fundamental rights may be affected by the use of sound recording bugs on public transport used by target:

6.2.1 The right to personal data (Article 8 of the CFREU; Article 8 of the ECHR)

The right to personal data is protected by the Article 8 of the CFREU, as well as Article 8 of the ECHR and on the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which has been ratified by all the EU Member States.

To the extent that an individual can be identified, the recording of sound in public transport constitutes personal data. In Directive 95/46/EC, of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995) personal data are defined as "any information relating to an identified or identifiable natural person", also referred to as the "data subject. Moreover, the purpose of Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such data being defined as "any information relating to an identified or identifiable individual" (Article 2)

Data protection rights are also protected by Article 8 of the ECHR and Article 17 of the ICCPR. As stated by the ECtHR, private-life considerations may arise once any systematic or permanent record about an individual comes into existence. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method.[164] Furthermore, in the case of P.G. and J.H. v. the United Kingdom, ECtHR held that a recording and analysis of prison cell conversations for the purpose of recording the voice of the target for identification, was regarded as concerning the processing of personal data about the individuals.[165]

The ECtHR has considered it essential, in the context of the recording and communication of criminal record data as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures; as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the

[164] See Rotaru V. Romania.

[165] See P. G. And J. H. V. The United Kingdom.

integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.[166]

6.2.2 The right to respect for private life (Article 7 of the CFREU; Article 8 of the ECHR; and Article 17 of ICCPR)

The right to private life is also applicable in public contexts such as public transport vehicles. Although no directly applicable case law exists about the relationship between privacy rights and sound recording bugs in public vehicles, several analogously applicable guidelines are available. First, according to established case law of the ECtHR, private life is a broad term covering, among others, a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world.[167] As noted by the European Court of Human Rights there is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life".[168]

However, not all private actions in the public context fall under the scope of application of the right to private life, however. In P.G. and J.H. v. United Kingdom, the Court further noted as follows:

> "There are a number of elements relevant to a consideration of whether a person's private life is concerned in measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain." Furthermore, the ECtHR has held that normal use of security cameras per se whether in the public street or on premises, such as shopping centres or police stations where they serve a legitimate and foreseeable purpose, do not raise issues under Article 8 § 1 of the Convention.[169]

Nevertheless, the case is different if the use of material obtained from public context is used by the authorities in an unforeseen and intrusive manner or if the use of surveillance technology involves processing of personal data. In both of these cases, Article 8 applies. In Peck v. the United Kingdom (judgment of 28 January 2003), the disclosure to the media for broadcast use of video footage of the applicant whose

[166] See M. M. V. The United Kingdom.
[167] See, for example, Friedl V. Austria.
[168] See P. G. And J. H. V. The United Kingdom.
[169] See Case of Perry V. The United Kingdom, n. 63737/00, European Court of Human Rights, 17 July 2003.

suicide attempt was caught on close circuit television cameras was found to be a serious interference with the applicant's private life, notwithstanding that he was in a public place at the time. The ECtHR has also held that right to private life is applicable if the police is regulating the security camera so that it could take clear footage of the applicant for the purposes of using that footage in criminal investigation.[170] Moreover, the Court has also held that the permanent recording of the voices of suspects made while they answered questions in a public area of a police station as police officers listened to them was regarded as the processing of personal data about them amounting to an interference with their right to respect for their private lives. This interpretation is in line with broader jurisprudence where the ECtHR has consistently held that the covert taping of telephone conversations falls within the scope of Article 8 in both aspects of the right guaranteed, namely, respect for private life and correspondence.[171] Similarly, recoding conversations in an apartment has been found to interfere with the right to private life.[172]

Hence, the public space as such does not define the scope of application of the right to private life. The actual purpose of using the surveillance technology, and the subsequent uses of the obtained data are more decisive factors. Recording of the data and the systematic or permanent nature of the record usually give rise to privacy considerations.[173] This entails, in turn, that the use of sound recording bugs in public transport must be prescribed by law and pursue a legitimate aim.

6.3 Limitations to rights involved

The affected rights are not absolute, in the sense that they permit restrictions or limitations that serve a legitimate aim, are prescribed by the law in a precise and foreseeable manner, and are both necessary and proportionate in nature. The conditions for restrictions into the affected fundamental rights are spelled out in, inter alia, CFREU Art. 52, ECHR Art. 8 and ICCPR Art. 17.

The sound recording bugs in public transport do not result into intrusions of the core of those rights.[174] Hence, intrusions by these bugs may be permissible but the legitimacy of the intrusion ultimately depends on the relationship between the level of intrusion and the importance towards the aim of that intrusion. The greater the degree of non-satisfaction of, or detriment to, a fundamental right, the greater must be the importance of satisfying the other legitimate aim.

---

[170] Ibid.

[171] See already Klass and Others V. Germany at § 41.

[172] See Case of Bykov V. Russia, n. 4378/02, European Court of Human Rights, 10 March 2009.

[173] See, for example, Rotaru V. Romania.

[174] Intrusions into the core, or into absolute rights that allow for no limitations, give an aggregate score of 16 where the weight of the right and the level of intrusion are not even addressed separately.

As this assessment is not geared towards a specific jurisdiction, no assessment is possible concerning the requirement that any intrusion into fundamental rights is 'prescribed by the law'. Any reader is, therefore, reminded that the use of any specific surveillance technology will make it necessary to verify that there was a proper legal basis for the measures undertaken. Moreover, with regard to protection of personal data, the ECtHR has considered it essential, in the context of the recording and communication of criminal record data as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures; as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.[175]

6.4 Level of intrusion

The severity of fundamental rights intrusion created by sound recording bugs on public transport used by the target depends on number of different aspects.

At the abstract level, the sound recording bugs in public transport endanger rights or attributes of rights that have a low weight in regard the right to private life (1) and medium weight with regard to the protection of personal data (2).

- Individual's liberty right of being able to decide what information to share and with whom may as such be considered to fall close to the core of the right to private life and hence to be of significant (medium or high) weight. However, this weight of this right is usually weaker in public contexts.
- Protection of personal data has been understood to have fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the ECHR.[176]
- The need for data protection safeguards is all the greater where such data are used for police purposes.[177]

As to the intensity of these restrictions, at least following considerations must be taken into account:

- Although the right to private life is also applicable in public contexts, in typical cases, the recording of sounds in public transport can be understood as intruding at the outer border of privacy rights. A person who talks in the public transport will inevitably be heard by some member of the public who is also present. Monitoring by technological

[175] See M. M. V. The United Kingdom.
[176] See S. And Marper V. The United Kingdom.
[177] Ibid.

means of the same public scene is of a similar character. In terms of the right to privacy in general, this kind of intrusion is low (1)

- With regard the right to protection of personal data, the intrusion may be significant. In the context of the recording and communication of data that records criminal conduct as in telephone tapping, secret surveillance and covert intelligence-gathering, the ECtHR has emphasized it to be essential, to have clear, detailed rules that provide sufficient guarantees against the risks of abuse and arbitrariness. The strict requirements set forth for the processing of personal data in criminal investigation reflect the severity of intrusion.[178] The intensity of the intrusion may be assessed to be high (4).

As to the reliability of these considerations, there exists well established case law about privacy rights, data protection and freedom of communication. In terms of the protection of personal data, the state of law is clear and reliable (1). With regard to the respect for general right to private life in public transport, no directly applicable case exists. However, there are analogously applicable legal materials. The reliability of the above intrusiveness analysis is medium.

6.5 Quantification

	Abstract weight[179]	***Intrusiveness***[180]	***Reliability of the state of law***[181]	***Value***[182]
Data protection	***2***	***4***	***1***	***8***
Right to private life	***1***	***1***	***3/4***	***3/4***

6.6 Further considerations

This assessment does not include the right to a fair trial. Hence, the possible use of the resulting recordings as evidence in the trial has not been addressed.

[178] See M. M. V. The United Kingdom.
[179] Scale: 1 low, 2 medium, 4 high.
[180] Scale: as above.
[181] Scale: ½ low (lay person), ¾ medium (collective assessment by a team of experts), 1 high (expert team with reference to clear case law).
[182] Scale: from 0 (no intrusion) to 16. All values above 10 (i.e., either 12 or 16) will mean that no security benefit from the use of the technology as described can legitimise its use due to fundamental rights consequences. However, judicial authorization of the surveillance results in a different scale.

This assessment focuses on intrusion into the rights of the actual target. As the bug will be used in public transport, it is very likely that voices of other persons will be heard and recorded as well. Even if these persons are not identified, this will mean an intrusion into their right to private life. If the persons are identified, also data protection issues arise.

We will need to address separately third-party intrusions and the risk of abusive use of the technology in relation to the actual target.

In the above assessment, the weight of the fundamental rights in question has been assessed in relation to surveillance without judicial authorization. If the surveillance measure is authorised by the judiciary, the weight (and the overall score) should be multiplied by 3/4. This is based on the idea that the weight of a fundamental right is greater in relation to the executive than in relation to the judiciary.

7 Sound recording bug in police vehicle transporting target following arrest (JL)

7.1 Description of the surveillance technology

See description in sheet # 4.

7.2 Fundamental rights affected

The following rights are typically affected by the use of listening devices in police vehicle transporting target following arrest.

7.2.1 The right to personal data (Article 8 of the CFREU; Article 8 of the ECHR)

To the extent that an individual can be identified, the recordings of sounds in police vehicle following arrest constitute personal data.

The right to personal data is explicitly protected by the Article 8 of the CFREU as well as an attribute to the privacy right protected by Article 8 of the ECHR.

In Directive 95/46/EC, personal data are defined as "any information relating to an identified or identifiable natural person", also referred to as the "data subject. To the extent that the individual can be identified, the recordings of police car conversations constitutes personal data. Moreover, the purpose of Council of Europe's Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such data being defined as "any information relating to an identified or identifiable individual" (Article 2) Similar right is protected also by the article 8 of the ECHR. As stated by the ECtHR, private-life considerations may arise once any systematic or permanent record about an individual comes into existence. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method.[183] In the case of P.G. and J.H. v. the United Kingdom, ECtHR held that a recording and analysis of prison cell conversations for the purpose of recording the voice of the target for identification, must be regarded as concerning the processing of personal data about the individuals.[184]

In the context of the recording and communication of criminal record data as in telephone tapping, secret surveillance and covert intelligence-gathering, the ECtHR has considered it essential, to have clear, detailed rules governing the scope and application of measures; as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the

[183] See Rotaru V. Romania.

[184] See P. G. And J. H. V. The United Kingdom.

integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.[185]

7.2.2 The right to respect for private life (Article 7 of the CFREU; Article 8 of the ECHR; and Article 17 of ICCPR)

The right to respect for private life applies also to the taping of target's voice in police car. These recordings may be analogously compared to recordings made in police station and prison cell. As ECtHR has held several times, the use of the audio- and video-recording devices in the cell, the visiting area and on a fellow prisoner amount to an interference with the right to private life under Article 8 § 1 of the Convention[186]. More specifically, in the case P.G. and J.H. v. the United Kingdom, the Court held that already cell recordings taken merely for a use as voice samples already fell into the scope of the protection afforded by Article 8 of the ECHR. This interpretation is in line with broader jurisprudence where the ECtHR has consistently held that the covert taping of telephone conversations falls within the scope of Article 8 in both aspects of the right guaranteed, namely, respect for private life and correspondence.[187] In essence, the use of listening devices in prison cell interferes with the individuals' liberty right of being able to decide what information to share and with whom.

7.3 Limitations to rights involved

The affected rights are not absolute, in the sense that they permit restrictions or limitations that serve a legitimate aim, are prescribed by the law in a precise and foreseeable manner, and are both necessary and proportionate in nature. However, the interference must be prescribed by law and be justified according to pursuit of a legitimate aim. The conditions for restrictions into the affected fundamental rights are spelled out in, inter alia, CFREU Art. 52, ECHR Art. 8 and ICCPR Art. 17.

The sound recording bugs in police vehicle transporting the target after an arrest do not result in intrusions into the core of those rights. This being the case, intrusions may be legitimate. In these situations, the legitimacy of the intrusion depends ultimately on the relationship between the level of intrusion and the importance of the aim of that intrusion. The greater the degree of non-satisfaction of, or detriment to, a fundamental right, the greater must be the importance of satisfying the other legitimate aim.

As this assessment is not geared towards a specific jurisdiction, no assessment is possible concerning the requirement that any intrusion into fundamental rights is 'prescribed by the law'. Any reader is, therefore, reminded that the use of any specific surveillance technology will make it necessary to verify that there was a proper legal basis for the measures undertaken. Moreover, the ECtHR has

[185] See M. M. V. The United Kingdom.
[186] See Khan V. The United Kingdom; M. M. V. The United Kingdom.
[187] See already Klass and Others V. Germany at § 41.

considered it essential, in the context of the recording and communication of criminal record data as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures; as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.[188]

7.4 Level of intrusion

The severity of intrusion of listening devices in a police car depends on number of different aspects. The starting point must be that people in police's custody in general continue to enjoy all the fundamental rights and freedoms guaranteed under the Convention.[189] Any restrictions on these other rights require to be justified. On the other hand, as emphasized by the ECtHR, such justification may well be found in the considerations of security, in particular the prevention of crime and disorder.[190]

In the abstract, the sound recording bugs in a police car endanger rights that have a medium weight (2).

- Individual's liberty right of being able to decide what information to share and with whom may be considered to fall close to the core of the right to private life.
- Protection of personal data has been understood to have fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the ECHR.[191]
- The need for data protection safeguards is all the greater where such data are used for police purposes.[192]

As to the intensity of these restrictions, at least following considerations must be taken into account:

- A police vehicle is not a place where persons could reasonable expect for a high level of privacy. A person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor in a privacy right assessment.

[188] See M. M. V. The United Kingdom.
[189] See Case of Hirst V. The United Kingdom, n. 74025/01, European Court of Human Rights, 6 October 2005.
[190] See Case of Silver and Others V. The United Kingdom, n. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, European Court of Human Rights, 24 October 1983.
[191] See S. And Marper V. The United Kingdom.
[192] Ibid.

- Considerations of security, in particular the prevention of crime and disorder, which typically are relevant in cases concerning arrest may justify broader restrictions than would be the case in other circumstances. (1)
- With regard the right to the protection of personal data, the intrusion may be severe especially if organized in systematic fashion. In the context of the recording and communication of criminal record data as in telephone tapping, secret surveillance and covert intelligence-gathering, The ECtHR has emphasized it to be essential, to have clear, detailed rules that provide sufficient guarantees against the risk of abuse and arbitrariness. The strict requirements set forth for processing of personal data in criminal investigation reflect the severity of intrusion.[193] The intensity of intrusion may be assessed to be severe (4).

As to the reliability of these considerations, there exists widely established case law about privacy rights, data protection and freedom of communications. No real issues of interpretive difficulties arise. As such, findings are legally reliable. (1)

7.5 Quantification

	Abstract weight	***Intrusiveness***	***Reliability of the state of law***	***Value***
Data protection	***2***	***4***	***1***	***8***
Right to private life	***2***	***1***	***1***	***2***

7.6 Further considerations

This assessment does not include the right to a fair trial. Hence, the possible use of the recordings as evidence in the trial has not been addressed.

This assessment focuses on intrusion into the rights of the actual target. As the bug will be used in a police car following arrest, it is assumed that the fundamental rights of other persons will not be affected

In the above assessment, the weight of the fundamental rights in question has been assessed in relation to surveillance without judicial authorization. If the surveillance measure is authorised by the judiciary, the weight (and the overall score) should be multiplied by 3/4.

[193] See M. M. V. The United Kingdom.

8 Sound recording bug in target's prison cell (JL)

8.1 Description of the surveillance technology

See description by TU Delft.

8.2 Fundamental rights affected

8.2.1 The right to personal data (Article 8 of the CFREU; Article 8 of the ECHR)

To the extent that an individual can be identified, the recordings of sounds in prison cell constitute personal data.

The right to personal data is explicitly protected by the Article 8 of the CFREU as well as an attribute to the privacy right protected by Article 8 of the ECHR.

In Directive 95/46/EC, personal data are defined as "any information relating to an identified or identifiable natural person", also referred to as the "data subject. To the extent that the individual can be identified, the recordings of prison cell conversations constitutes personal data. Moreover, the purpose of Council of Europe's Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such data being defined as "any information relating to an identified or identifiable individual" (Article 2) Similar right is protected also by the article 8 of the ECHR. As stated by the ECtHR, private-life considerations may arise once any systematic or permanent record about an individual comes into existence. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method.[194] In the case of P.G. and J.H. v. the United Kingdom, ECtHR held that a recording and analysis of prison cell conversations for the purpose of recording the voice of the target for identification, must be regarded as concerning the processing of personal data about the individuals.[195]

In the context of the recording and communication of criminal record data as in telephone tapping, secret surveillance and covert intelligence-gathering, the ECtHR has considered it essential, to have clear, detailed rules governing the scope and application of measures; as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the

[194] See Rotaru V. Romania at §§ 43 44.
[195] See P. G. And J. H. V. The United Kingdom.

integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.[196]

8.2.2 The right to respect for private life (Article 7 of the CFREU; Article 8 of the ECHR; and Article 17 of ICCPR)

The right to respect for private life applies also to the taping of prison cell conversations. As ECtHR has held several times, the use of the audio- and video-recording devices in the cell, the prison visiting area and on a fellow prisoner amount to an interference with the right to private life under Article 8 § 1 of the Convention[197]. More specifically, in the case P.G. and J.H. v. the United Kingdom, the Court held that already cell recordings taken merely for a use as voice samples fell into the scope of the protection afforded by Article 8 of the ECHR. This interpretation is in line with broader jurisprudence where the ECtHR has consistently held that the covert taping of telephone conversations falls within the scope of Article 8 in both aspects of the right guaranteed, namely, respect for private life and correspondence. [198] One of the attributes of right to private life covers the confidentiality of communications, which can be intruded upon by those covert technologies that are able to capture personal communications by voice, telephone, letter or electronic mean. In particular, and taking into account that human rights do not stop at the gates of a prison,[199] the use of listening devices in a prison cell interferes with the individuals liberty right of being able to decide what information to share and with whom.

Right to fair trial (would be relevant with regard to subsequent uses of recorded data but not covered in the matrix)

8.3 Limitations to rights involved

The affected rights are not absolute, in the sense that they permit restrictions or limitations that serve a legitimate aim, are prescribed by the law in a precise and foreseeable manner, and are both necessary and proportionate in nature. However, the interference must be prescribed by law and be justified according to pursuit of a legitimate aim. The conditions for restrictions into the affected fundamental rights are spelled out in, inter alia, CFREU Art. 52, ECHR Art. 8 and ICCPR Art. 17.

The sound recording bugs in prison cell do not result in intrusions into the core of those rights. This being the case, intrusions may be legitimate. In these situations, the legitimacy of the intrusion depends ultimately on the relationship between the

[196] See M. M. V. The United Kingdom.
[197] See Khan V. The United Kingdom; M. M. V. The United Kingdom.
[198] See already Klass and Others V. Germany at § 41.
[199] See Case of Golder V. The United Kingdom, n. European Court of Human Rights, 21 February 1975 at § 36.

level of intrusion and the importance of the aim of that intrusion. The greater the degree of non-satisfaction of, or detriment to, a fundamental right, the greater must be the importance of satisfying the other legitimate aim.

As this assessment is not geared towards a specific jurisdiction, no assessment is possible concerning the requirement that any intrusion into fundamental rights is 'prescribed by the law'. Any reader is, therefore, reminded that the use of any specific surveillance technology will make it necessary to verify that there was a proper legal basis for the measures undertaken. Moreover, with regard to protection of personal data, the ECtHR has considered it essential, in the context of the recording and communication of criminal record data as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures; as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.[200]

8.4 Level of intrusion

The severity of intrusion of prison cell listening devices depends on number of different aspects. The starting point must be that prisoners in general continue to enjoy all the fundamental rights and freedoms save for the right to liberty, where lawfully imposed detention expressly falls within the scope of Article 5 of the ECHR.[201] Any restriction on these other rights require to be justified. On the other hand, as emphasized by the ECtHR, such justification may well be found in the considerations of security, in particular the prevention of crime and disorder, which inevitably flow from the circumstances of imprisonment. Accordingly, the ECtHR has found broad restrictions on the right of prisoners to correspond as violating Article 8 whereas stopping of specific letters, containing threats or other objectionable references were justifiable in the interests of the prevention of disorder or crime.[202]

In the abstract, the sound recording bugs in prison cell endanger rights that typically have a medium weight (2). This assessment is based on following key arguments.

- Individual's liberty right of being able to decide what information to share and with whom may be considered to fall close to the core of the right to private life.
- Protection of personal data has been understood to have fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the ECHR.[203]
- The need for data protection safeguards is all the greater where such data are used for police purposes.[204]

[200] See M. M. V. The United Kingdom.
[201] See Case of Hirst V. The United Kingdom.
[202] See Silver and Others V. The United Kingdom.
[203] See S. And Marper V. The United Kingdom.

As to the intensity of these restrictions, at least following considerations must be taken into account:

- On the one hand, the restriction is potentially very broad and, due to the nature of imprisonment, directed to an already severely limited aspect of private life.
- On the other hand, considerations of security, in particular the prevention of crime and disorder, which inevitably flow from the circumstances of imprisonment, may justify broader restrictions than would be the case in other circumstances.
- The level of intrusiveness depends on the actual form of using the sound recording bugs. If used for a short period of time and narrowly tailored for prevention of crime and disorder in specific circumstances, the intrusion may ultimately be of medium level. (2) If on the other hand recording bugs are used in a sweeping fashion, constantly and without other specified reason than a general need to prevent crimes and disorder, the intrusion may be severe. (4)
- With regard the right to the protection of personal data, the intrusion may be severe especially if organized in systematic fashion. In the context of the recording and communication of criminal record data as in telephone tapping, secret surveillance and covert intelligence-gathering, The ECtHR has emphasized it to be essential, to have clear, detailed rules that provide sufficient guarantees against the risk of abuse and arbitrariness. The strict requirements set forth for processing of personal data in criminal investigation reflect the severity of the intrusion.[205] The intensity of the intrusion is severe (4).

As to the reliability of these considerations, there exists widely established case law about privacy rights, data protection and freedom of communications. No real issues of interpretive difficulties arise. As such, the findings are legally reliable. (1)

8.5 Quantification

	Abstract weight	***Intrusiveness***	***Reliability of the state of the law***	***Value***
Data protection	***2***	***4***	***1***	***8***
Right to private life	***2***	***2-4***	***1***	***4-8***

[204] Ibid.
[205] See M. M. V. The United Kingdom.

8.6 Further considerations

This assessment does not include the right to a fair trial. Hence, the possible use of the recordings as evidence in the trial has not been addressed.

This assessment focuses on intrusion into the rights of the actual target. As the bug will be used in a prison cell, it is possible that voices of other prisoners will be heard and recorded as well. This will mean an intrusion into their right to private life and data protection.

In the above assessment, the weight of the fundamental rights in question has been assessed in relation to surveillance without judicial authorization. If the surveillance measure is authorised by the judiciary, the weight (and the overall score) should be multiplied by 3/4.

9 Video Camera Mounted on Platform Micro Helicopter (JA)

9.1 Description of the surveillance technology (readapted from 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).

9.1.1 Scenario

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.

9.2 Fundamental rights affected

9.2.1 Fundamental right to privacy or private and family life (Article 8 ECHR, Article 7 EUCFR, Article 17 ICCPR)

The protections afforded by the right to privacy require consideration in the case of the use of a platform micro helicopter for surveillance. Certain parallels may be drawn between the use of closed-circuit television (CCTV) and the use of unmanned aerial vehicles (UAVs or 'drones') for the purpose of visual surveillance. Of

importance within the context of the specific use of smaller aerial devices is the degree to which monitoring may be said to be of either an overt or covert nature.[206]

In the context of "private life", the European Court of Human Rights (hereafter *ECtHR*) has recalled that the notion is a broad one, which is not susceptible to exhaustive definition.[207] Of relevance too within the context of aerial surveillance is the ECtHR's assertion that: "Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities."[208]

In the *P.G. and J.H. v. United Kingdom* case the ECtHR further noted as follows:

> "There are a number of elements relevant to a consideration of whether a person's private life is concerned in measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities, which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, though not necessarily conclusive factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (e.g. a security guard viewing through close circuit television) is of a similar character. Private life considerations may arise however once any systematic or permanent record comes into existence of such material from the public domain."[209]

However, the ECtHR has clarified that the monitoring of the actions of an individual in a public place by the use of photographic equipment, which does not record the visual data does not, *per se*, give rise to an interference with the individual's private life.[210] In contrast, were the equipment to record the data, or where there exists a systematic or permanent nature of the record this may give rise to consideration as to whether their has been an interference in the protection guaranteed by Article 8 of the Convention.[211]

---

[206] Platform micro helicopter-type devices function so as to allow both overt and covert capabilities. See, for example, Prox Dynamics, Your Personal Reconnaissance System. Available at: http://www.proxdynamics.com/products/pd_100_prs/ (accessed on 28 May 2013).

[207] Niemietz V. Germany at § 29.

[208] Rotaru V. Romania at § 43.

[209] P. G. And J. H. V. The United Kingdom at § 57.

[210] *See*, for example, Case of Herbecq and the Association "Ligue Des Droits De L'homme" V. Belgium at 92.

[211] "Accordingly, in both the Rotaru and Amann judgments (to which the P.G. and J.H. judgment referred) the compilation of data by security services on particular individuals even without the use of covert surveillance methods constituted an

The manner in which the platform micro helicopter is deployed and operated may influence the assessment of the surveillance as to whether it constitutes an interference. The case of *Perry v. the United Kingdom* provides guidance in this respect: "As stated above, the normal use of security cameras per se whether in the public street or on premises, such as shopping centres or police stations where they serve a legitimate and foreseeable purpose, do not raise issues under Article 8 § 1 of the Convention." [212] Thus monitoring of this nature can be construed to represent a legitimate aim. The Court's guidance does not refer to areas of a notionally different nature, such as that of the home or workplace: it may be concluded therefore that the use of a platform micro helicopter in these locations may be evaluated differently. As evidenced by the above-cited case law, the purpose for which surveillance is conducted by a public authority, and the use made by the party of the data obtained are the significant factors in determining whether an interference has occurred in the right to privacy.

9.2.2 Fundamental right to the protection of personal data (Article 8 ECHR, Article 8 EUCFR)

The EUCFR establishes a distinct right to the protection of personal data in Article 8, which states: "Everyone has the right to the protection of personal data concerning him or her."[213] The ECHR's Article 8's guarantees to a right to privacy have also been interpreted to cover the protection of personal data.[214] Article 17 of the ICCPR has been held to cover the protection of personal data.[215] The ECtHR has reiterated in recent cases [216] of the necessity of there being clear and sufficiently detailed guidelines as to the use of surveillance measures, in addition to minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.[217]

---

interference with the applicants' private lives (Amann V. Switzerland at §§ 65-67; Rotaru V. Romania at §§ 43 44.)." *Peck V. The United Kingdom at § 56.*

[212] Perry V. The United Kingdom at § 40.

[213] Article 8, Charter of Fundamental Rights of the European Union, Official Journal C 303/1, p. 1–22, 14 December 2007.

[214] *See*, for example Case of Leander V. Sweden, n. 9248/81, European Court of Human Rights, 26 March 1987 at § 48; Rotaru V. Romania at § 43.

[215] *See*, for example Frank La Rue, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression,' United Nations Human Rights Council (2011) at 16, § 58. Available at: http://www2.ohchr.org/english/ bodies/hrcouncil/docs (accessed on 22 May 2013)

[216] See, for example, M. M. V. The United Kingdom at § 195.

[217] S. And Marper V. The United Kingdom at § 99.

Also relevant in the European context is the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[218] (hereafter Convention 108). The provisions with the Convention 108 apply to any information relating to an identified or identifiable individual (personal data) processed wholly or partly by automatic means, and both by public and private parties. Of particular note in Convention 108, and of interest to our deliberation as to the permissibility of law utilising aerial surveillance whereby it may engage Article 6 of Convention 108; Article 6 states with respect to 'Special categories of data': "Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards."[219] Monitoring and recording images by this technology may engage this provision. Also relevant in the context of crime prevention activities vis-à-vis data protection is Recommendation No. R(87)15 on regulating the use of personal data in the police sector places on the collection of personal data. The appendix to the recommendation asserts that this activity should be limited to reflect the intention of suppressing a specific criminal offence, rather than reflect a broader preventative mandate of an unspecified description.[220]

The Council Framework Decision 2008/977/JHA[221] applies to and provides for the protection of personal data processed in the framework of police and judicial cooperation in order to prevent, investigate, detect or prosecute a criminal offence or execute a criminal penalty. However, in the context of the given scenario it must be taken into account that the Framework Decision has limited effect in respect of the domestic setting; where data originates and is processed within a Member State its provisions do not apply.[222]

9.2.3 Freedom of movement and residence (Protocol 4 - Article 2 to ECHR, Article 45 EUCFR, Article 12 ICCPR)

Surveillance conducted through the use of a platform micro helicopter may engage the fundamental right to freedom of movement as the technology allows for spatial and temporal information pertaining to an individual's whereabouts to be monitored and collected. This procedure may inhibit a person's enjoyment of free movement where they feel the liberty is restricted by the knowledge that others are aware of

[218] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, CETS No. 108, p. 28 January 1981.
[219] Ibid., at article 6.
[220] Recommendation of the Committee of Ministers Regulating the Use of Personal Data in the Police Sector (Police Recommendation) R (87) 15, p. 17 September 1987.
[221] Council Framework Decision 2008/977/Jha of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters, OJ L 350, p. 60 –71, 30 December 2008.
[222] Ibid. Preamble, recital 7 states: "The scope of this Framework Decision is limited to the processing of personal data transmitted or made available between Member States."

their location. The UN Human Rights Committee has noted with respect to Article 12 of the ICCPR: "Liberty of movement is an indispensable condition for the free development of a person" and that: "The permissible limitations which may be imposed on the rights protected under article 12 must not nullify the principle of liberty of movement, and are governed by the requirement of necessity provided for in article 12, paragraph 3, and by the need for consistency with the other rights recognized in the Covenant."[223]

9.3 Permissible limitations to the fundamental rights that are engaged by the use of the technology for surveillance purposes

The rights that may be affected by the use of a platform micro helicopter by law enforcement for the purposes of monitoring a suspect are not absolute; the provisions within the ECHR, ECUCFR and ICCPR pertaining to the rights to privacy, the protection of personal data, freedom of expression and liberty of movement are all qualified by the permissibility of limitations placed upon them where such restrictions serve a legitimate aim, are necessary and proportionate.

The criteria by which such limitations may be deemed lawful interferences are articulated in, *inter alia*, ECHR Articles 8(2), 10(2), Prot. 4 – Art. 10(2), EUCFR Article 52, ICCPR Articles 12(3) and 19(3). The intrusion into fundamental rights by a law enforcement agency's use of aerial surveillance for the purpose of the detection or the prevention of crime may prove permissible where it can be shown to constitute a proportionate interference. As the review here does not concern a specific jurisdiction, questions as to the foreseeability of the intrusion and whether it be 'prescribed by law' are outwith the scope of this assessment. Nevertheless, in the context of a specific event, prior to deploying a platform micro helicopter, a public authority would need to meet the condition that the impugned measure have some basis in domestic law i.e. be 'prescribed by law'.

The ECtHR has reiterated the importance is places on the obligations incumbent upon the law enforcement agencies for the proper safeguard of fundamental rights in the context of surveillance activity, whereby it: "[F]urther observes that concerns which prompted the elaboration of the Data Protection Convention in regard to the increasing recourse to automation in all sectors are most acutely felt in the police sector, for it is in this domain that the consequences of a violation of the basic principles laid down in the Convention could weigh most heavily on the individual."[224]

---

[223] Human Rights Committee, 'General Comment No. 27. Freedom of Movement (Article 12)', (1999) at §§ 1, 2. Available at: http://www.unhchr.ch/tbs/doc.nsf/(Symbol)/6c76e1b8ee1710e380256824005a10a9?Opendocument(accessed on 28 May 2013).

[224] M. M. V. The United Kingdom at § 126. For further elaboration see ibid., at §§ 121-41. *See* also S. And Marper V. The United Kingdom at § 99.

9.4 Level of intrusiveness

The use of a platform micro helicopter for aerial surveillance of a suspect by law enforcement officials may constitute an intrusion into several distinct fundamental rights. In each instance the severity of each interference is dependent upon a number of distinct criteria.

- With respect to the right to privacy, the level of intrusiveness of the use of aerial surveillance in a public setting can be considerable regardless of whether the device can be readily detected (overt) or not (covert). Thus the interference may be qualified as of a 'medium' weighting. In specific contexts, such as in areas considered generally as outwith the ambit of a public space (such as in a private dwelling), the interference could be considered 'high'.

- The protection of personal data in accordance with the guarantees furnished by Article 8 of the ECHR has been considered pivotal to an individual's enjoyment of their private life: "[T]he Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained."[225] As such, the collection and storage of data pertaining to the use of an aerial surveillance device will be subject to particular scrutiny.

- Furthermore, the ECtHR has stated that the need for such safeguards is all the more necessary where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes.[226]

- The extent to which the use of a platform micro helicopter to conduct aerial surveillance intrudes on freedom of movement is less clear. However, ECtHR case law provides guidance where the Court has noted that the notion of being "necessary in a democratic society" in respect of a surveillance activity must be considered to infer that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued.[227] In addition, the Court will likely seek to ascertain whether other methods of investigation that are comparatively less intrusive would prove to be less effective.

9.5 Qualifying the intrusion on the basis of a scale

[225] *See* S. And Marper V. The United Kingdom at § 103.
[226] Peck V. The United Kingdom at § 59.
[227] Uzun V. Germany at § 78.

	Abstract weight[228]	*Intrusiveness*[229]	*Reliability of the state of law*[230]	*Value*[231]
Right to privacy	***2***	***2-4***	***1***	***4-8***
Data protection	***1***	***1***	***¾***	***3/4***
Freedom of Movement	***2***	***2***	***¾***	***3***

9.6 Further considerations

This assessment does not include the right to a fair trial. Hence, the possible use of the recordings as evidence in the trial has not been addressed.

This assessment provides a focus solely in respect of the rights of the individual targeted for surveillance. However, the use of an aerial surveillance device will most likely subject other persons to monitoring, and may therefore also constitute interferences in respect of their fundamental rights, particularly as regards the rights to privacy and the protection of personal data.

In the above assessment, the weight of the fundamental rights in question has been assessed in relation to surveillance without judicial authorization. If the surveillance measure is authorised by the judiciary, the weight (and the overall score) should be multiplied by 3/4.

[228] Scale: 1 low, 2 medium, 4 high.
[229] Scale: as above.
[230] Scale: ½ low (lay person), ¾ medium (expert team), 1 high (expert team with reference to clear case law).
[231] Scale: when used by expert team, from ¾ to 16. All values above 10 (i.e., either 12 or 16) will mean that no security benefit from the use of the technology as described can legitimise its use due to fundamental rights consequences.

10 AIS ship location detection and identification (JL)

10.1 Description of the surveillance technology (readapted from 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. 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: http://www.marinetraffic.com/ais/nl/). AIS based ship location and identification data may be used in a targeted and proactive investigation of alleged importation of drugs and weapons via sea.

10.2 Fundamental rights affected

The following fundamental rights may be affected by the use of AIS ship location detection and identification.

10.2.1 The right to the protection of personal data (Article 8 of the CFREU; Article 8 of the ECHR, Article 17 of the ICCPR)

Based on the technology description, AIS equipment provides information about vessels. It is intended to assist a vessel's watchstanding officers and allow maritime authorities to track and monitor vessel movements. This information includes data such as unique identification, position, course, and speed, of the vessels but not about persons on board the ship. Accordingly, AIS ship location detection and identification does not directly involve the processing of personal data. As far as this remains the case, the sole use of AIS does not entail an intrusion to the right to the protection of personal data.

Conversely, in case AIS data are used as a part of targeted or proactive criminal investigation in a way in which data collected through AIS is combined with personal data about an individual that has been gathered from other sources, also AIS ship location detection and identification data will constitute personal data. For instance, ECtHR has held in case Uzun V. Germany, that the applicant's observation via GPS, in

the circumstances, and the processing and use of the data obtained thereby amounted to an interference with his private life as protected by Article 8 § 1.[232] As to the fact that the AIS location detection and identification system is overt instead of covert, it is of relevance that the ECtHR has held that the systematic collection and storing of data by security services on particular individuals, even without the use of covert surveillance methods, constituted an interference with these persons' private lives.[233] However, as said, the use of AIS ship location and identification data alone does not interfere with protection of personal data.

10.2.2 The right to respect for private life (Article 7 of the CFREU; Article 8 of the ECHR; and Article 17 of ICCPR)

The right to private life is also applicable in public contexts such as public transport vehicles and ships. In the above-mentioned case Uzun v. Germany, the ECtHR considered that installation of GPS device on individual's car and his surveillance via GPS-tracking data amounted to an interference with his private life as protected by Article 8 § 1. However, AIS equipment provides information about location, course and speed of vessels. It does not as such provide information about location and movements of individuals. As far as this remains the case, the use of AIS does not alone entail an intrusion to the right to the protection of private life.

Like above, the case is different if AIS data are used as a part of targeted or proactive criminal investigation in a way in which data collected through AIS is combined with personal data about an individual. In this case, also the use of AIS ship location detection and identification data for the purpose of surveillance of an individual may constitute interference with individual's right to private life. However, such intrusion is relatively weak. As stated by the ECtHR, GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information about a person's private life than the use of location data does.

10.3 Limitations to rights involved

The use of AIS data alone does not entail an intrusion to the right to the protection of private life and personal data

If used in combination with other data about an individual, the weight of the rights limited by AIS location equipment is medium at most. First, AIS tracking is overt, in fact publicly accessible. Second, according to ECtHR's holding in the case Uzun v. Germany, analogously similar GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life.

[232] See Uzun V. Germany at § 52.
[233] See S. And Marper V. The United Kingdom at § 105.

Third, AIS is primarily tracking movements of ships instead of people. Hence, its use falls under privacy rights only in conjunction with personal data collected from other sources. Taken together these reasons suggest that the abstract weight of both the right to protection of personal data and right to private life are weak (1) in the case of AIS location and identification data.

10.4 Intensity of intrusion

The use of AIS data alone does not entail an intrusion to the right to the protection of private life and personal data,

If used in combination with other data about an individual, the intensity of intrusion of rights limited by AIS location equipment is medium at most. This follows from the ECtHR's reasoning in the case Uzun v. Germany in which the court stated that rather strict standards, set up and applied in the specific context of surveillance of telecommunications were not applicable as such to cases concerning surveillance via GPS of movements in public places. Hence, the court considered that the intensity of intrusion imposed by location-based surveillance interfered less with the private life of the person concerned than the interception of his or her telephone conversations. Therefore, the court applied the more general principles that provide for adequate protection against arbitrary interference with Article 8 rights.

10.5 Quantification

	Abstract weight[234]	***Intrusiveness***[235]	***Reliability of the state of law***[236]	***Value***[237]
Data protection – AIS alone	***0***	***0***	***1***	***0***
Right to private life – AIS alone	***0***	***0***	***1***	***0***
Data protection – AIS in combination with personal data	***2***	***2***	***1***	***4***

[234] Scale: 1 low, 2 medium, 4 high.
[235] Scale: as above.
[236] Scale: ½ low (lay person), ¾ medium (expert team), 1 high (expert team with reference to clear case law).
[237] Scale: when used by expert team, from ¾ to 16. All values above 10 (i.e., either 12 or 16) will mean that no security benefit from the use of the technology as described can legitimise its use due to fundamental rights consequences.

Right to private life – AIS in combination with personal data	***2***	***2***	***1***	***4***

10.6 Further considerations

This assessment does not include the right to a fair trial. Hence, the possible use of the resulting information as evidence in the trial has not been addressed. That said, no additional issues are likely to arise.

This assessment focuses on intrusion into the rights of the actual target. As AIS will be used to track the route of a ship in the context of following the importing of a shipment of drugs and weapons, it is unlikely that any other persons than those implicated by the actual operation will be affected. Hence, there is no need to address possible third-party intrusion.

If we assume that the suspect items travel separately from the suspect persons, the first two assessments above (resulting in zero intrusion) apply.

In the above assessment, the weight of the fundamental rights in question has been assessed in relation to surveillance without judicial authorization. If the surveillance measure is authorised by the judiciary, the weight (and the overall score) should be multiplied by 3/4. This is based on the idea that the weight of a fundamental right is greater in relation to the executive than in relation to the judiciary. This is of course relevant only if contrary to the above assumption the suspect persons travel on the same ship as the suspect items and the latter two assessments therefore apply.

11 Explosives detector near harbor (MS)

12 Gas chromatography drugs detector (MS)

13 Luggage screening technology (X-ray) (MS) (TU Delft Sheet # 14)

13.1 Description of the surveillance technologies (readapted from TU Delft)

The use of these technologies is not specified in the scenario. Gas chromatography mass spectrometry (GC-MS) can be used to detect for example drugs or explosives in luggage or on a human person. An explosives detector is mounted on an ROV (Remotely Operated Vehicle). In this context, an ROV 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 suspicious objects and then remotely analyse the contents of the object. Traditional X-ray is based on radioactive emission through a physical object and is routinely used in the screening of luggage and cargo that travel through air. It appears that the use situations for all these three technologies in the scenario are directed on physical objects (luggage, items dropped off a ship, or cargo) without the presence of a human target.

13.2 Fundamental rights affected

The following rights are potentially affected by the use of luggage screening technologies.

13.2.1 The right to respect for private life (Article 7 of the CFREU; Article 8 of the ECHR; and Article 17 of ICCPR)

According to established case law private life or privacy is a broad term covering, among others, a right to retain a private sphere in respect of what one is carrying or transporting inside a closed object such as a suitcase. The person wishing to transport such personal items has the right, in principle, to determine to whom he or she shows or declares the contents of the closed container.

13.2.2 Other rights

In principle, several other fundamental rights can be affected if the right of a person not to disclose the contents of a closed container is compromised. For example a suitcase may contain religious items or materials, or political publications, the disclosure of which results in revealing the person's religion or political views and in particular in repressive countries may result in violations of the freedom of religion or freedom of expression. Also freedom of movement and the right not to be discriminated against may be implicated. As the scenario focuses on drugs and explosives and the individuals under investigation are 'neutral' persons without any

religious or political affiliations, these indirect impacts on other rights can be set aside and the assessment focuses on the direct interference with privacy rights through compromising the person's right not to disclose the contents of the container.

13.3 Limitations to the rights involved

The right to privacy is not absolute, in the sense that it permits restrictions or limitations that serve a legitimate aim, are prescribed by the law in a precise and foreseeable manner, and are both necessary and proportionate in nature. However, the interference must be prescribed by law and be justified according to pursuit of a legitimate aim. The conditions for restrictions into the affected fundamental rights are spelled out in, inter alia, CFREU Art. 52, ECHR Art. 8 and ICCPR Art. 17.

Subjecting an item of cargo or luggage to screening does not result in intrusions into the core of privacy rights. Using GS-MS or X-rays for the detection of explosives or drugs is in fact less intrusive than the opening of the container which would reveal to the inspectors also 'innocent' items that reflect for instance the religious, political or sexual orientation of the person. Furthermore, the international transport of drugs or explosives is subject to restrictions such as an obligation to declare any hazardous items or an outright ban on such transport. Individuals relying on international transport of cargo and luggage are aware of the fact that various methods of screening are in place for legitimate security reasons. In the scenario, the screening serves the legitimate aim of investigating or detecting crime. Consequently, the intrusions may very well be legitimate. The legitimacy of the intrusion depends ultimately on the relationship between the level of intrusion and the importance of the aim of that intrusion. The greater the degree of non-satisfaction of, or detriment to, a fundamental right, the greater must be the importance of satisfying the other legitimate aim.

As this assessment is not geared towards a specific jurisdiction, no assessment is possible concerning the requirement that any intrusion into fundamental rights is 'prescribed by the law'. Any reader is, therefore, reminded that the use of any specific surveillance technology will make it necessary to verify that there was a proper legal basis for the measures undertaken.

13.4 Level of intrusion

In the abstract, subjecting items of cargo or luggage to screening for explosives or drugs affect a dimension of privacy rights that has at best low weight (1).

As to the intensity of the intrusion, the above considerations result in an assessment that it is to be considered to be at best low (1).

As to the reliability of these considerations, there is no established case law about privacy rights in respect of non-disclosure of the contents of a closed item of cargo or luggage. The reliability of our intrusiveness analysis is medium (3/4).

13.5 Quantification

	Abstract weight	*Intrusiveness*	*Reliability of the state of law*	*Total value*
Right to private life	***0-1***	***0-1***	***3/4***	***0-3/4***

13.6 Further considerations

This assessment does not include the right to a fair trial. Hence, the possible use of the resulting findings as evidence in the trial has not been addressed.

This assessment focuses on intrusion into the rights of the actual target. As the use of gas and explosives detectors will be targeted upon the suspect individuals, it is highly unlikely that any intrusion into rights of third parties would occur.

In the above assessment, the weight of the fundamental rights in question has been assessed in relation to surveillance without judicial authorization. If the surveillance measure is authorised by the judiciary, the weight (and the overall score) should be multiplied by 3/4.

14 Eqo security scanner (“full body scanner”) (MV) (TU Delft Sheet # 13)

14.1 Description of the surveillance technology (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 analysing 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 analysed electronically.

14.2 Fundamental rights affected

The following fundamental rights may be affected by the use of the eqo security scanner:

14.2.1 The right to the protection of personal data (Article 8 of the CFREU; Article 8 of the ECHR)

Millimeter wave body scanners produce a low-quality image of a person’s body that is rather opaque, which resembles a photographic negative. The operator does not see this image, but a generic graphical representation of a human person with the location of the suspect item highlighted. As such, no personal data is visible to the operator. The description of the technology seems to suggest that no personal data is actually being processed, since the ‘image processing computer’ processes ‘reflected signals’ of concealed objects, and no information relating to an identified or identifiable natural person is being captured.

14.2.2 The right to respect for private life (Article 7 of the CFREU; Article 8 of the ECHR; and Article 17 of ICCPR)

As images of a millimeter wave scanner can make sexual organs visible and/or are able to reveal intentionally concealed physical features (for instance of transsexuals) or medical information (such as evidence of a mastectomy) which people might prefer not to be revealed, its use constitutes an interference with the right to respect for private life. However, since the eqo scanner only shows a generic graphical representation of the person to the operator, the interference with the right to respect for private life will be mitigated. It may however result in persons with above-mentioned concealed features being singled out for a pat search which may be more intrusive than if pat search was the method applied to everyone. A potential of further intrusion related to non-discrimination arises if body scanners are uncharacteristically used selectively on the basis of 'profiling'. The scenario in fact referes to the 'targeted' use of a body scanner in respect of certain individuals.

14.3 Limitations to rights involved

The potentially affected rights (privacy and data protection) are not absolute but do allow for permissible limitations.

As an image of a human person is produced in the process, even if then replaced by an animated figure before being shown to the human eye, there is an initial phase of revealing one's personal data. As no actual images or other data are stored and as the transitory animation figure is not associated with an identifiable person, the weight of data protection rights remains at medium level (2).

As going through a body scanner entails revealing the physical contours of one's body, even if only to a machine, and as certain categories of persons with intentionally concealed implants will be singled out for a pat search, a high level weight of the right to privacy is identified (4).

14.4 Level of intrusion

There is no intrusion in respect of data protection rights (0). In relation to the right to privacy, the level of intrusion is low (1).

14.5 Quantification

There is no case law in the issue but as several assessments of the fundamental rights impact of body scanners have been made, including by the EU Fundamental Rights Agency, the reliability of the assessment is medium (3/4).

	Abstract weight[238]	*Intrusiveness*[239]	*Reliability of the state of law*[240]	*Value*[241]
Data protection	***2***	***0***	***¾***	***0***
Right to private life	***4***	***1***	***¾***	***3***

14.6 Further considerations

It is to be noted that a previous generation of full body scanners did show a graphic image of a naked body to the screener, and that some of them included the technical capacity of storing the images or transferring them to a computer or even the internet. Our assessment does not relate to those products which were considered highly intrusive.

This assessment does not include the right to a fair trial. That said, no material results from the use of a body scanner that could be used as evidence in court.

No third-party intrusions arise.

In the above assessment, the weight of the fundamental rights in question has been assessed in relation to surveillance without judicial authorization. If the surveillance measure is authorised by the judiciary, the weight (and the overall score) should be multiplied by 3/4.

[238] Scale: 1 low, 2 medium, 4 high.
[239] Scale: as above.
[240] Scale: ½ low (lay person), ¾ medium (expert team), 1 high (expert team with reference to clear case law).
[241] Scale: when used by expert team, from ¾ to 16. All values above 10 (i.e., either 12 or 16) will mean that no security benefit from the use of the technology as described can legitimise its use due to fundamental rights consequences.

15 Anti-Money laundering (AML) technologies and HEMOLIA (MGP)

15.1 Money laundering tools and HEMOLIA (partly readapted from TU Delft's description)

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 analysed.
- 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 Web search engine. They search for financial anomalies. Anomalies may include the following: uncharacteristically large financial deposits; organizations or banks that were already associated with money laundering in earlier investigations; suspect gambling operators; and connections between known criminals and financial flows.

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*."[242]
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.

[242] See at: http://www.hemolia.eu/.

HEMOLIA tries to mitigate the privacy and data protection concerns that Anti-Money laundering technology raises[243] 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."[244]

15.1.1 Scenario-based use of HEMOLIA

The use of Anti-Money laundering technology is proposed in phase 4 of the scenario in relation to the investigation of drug and firearms smuggling (*ex ante facto*): LE agents ponder the initiation of "financial background enquiries and developments of the financial profiles on all nominal suspects." How software like HEMOLIA could be used in this situation is unclear. In this paper, we hypothesize that the police obtains 'pushes' of financial transactions for all relevant individuals (so that the privacy preserving feature becomes irrelevant), coupled with telecom information. Unfortunately, we do not have sufficient information to assess the functioning of HEMOLIA in the abstract. Thus, this paper will only review the lawfulness of HEMOLIA in relation to its use by the police in the current investigation.

15.2 Infringed fundamental rights (in the abstract)

Since suspects X, Y and Z are 'neutral' individuals, that is not identified by any features exposing them to discrimination, and no coercive action is imposed upon them, the following rights are not affected: non-discrimination, freedom of expression and information, and freedom of movement. Thus, the rights affected are data protection and privacy. However, the processing of data revealing sensitive information may affect some attributes of freedom of thought, conscience and religion.
Keeping in mind what was said above about the specificities of the Anti-Money laundering tools and HEMOLIA, and the contextual use, the relevant attributes are:

[243] A European Union working party, for example, has announced a list of 44 recommendations to better harmonize, and if necessary pare back, the money laundering laws of EU member states to comply with fundamental privacy rights. In the United States, groups such as the American Civil Liberties Union have expressed concern that money laundering rules require banks to report on their own customers, essentially conscripting private businesses "into agents of the surveillance state".
[244] See at: http://www.hemolia.eu/.

- Charter of Fundamental Rights of the European Union (EUCFR) Article 8 (data protection): sensitive data; data minimization (HEMOLIA);
- EUCFR Article 7 (privacy): confidential communications (HEMOLIA), social identity and relations; and autonomy and participation;
- EUCFR Article 10 (thought, conscience and religion): *forum internum.*[245]

15.2.1 The nature of banking and telecom data

HEMOLIA is a database fusing banking and telecom data collected in different circumstances and sending alerts on the mined information, which is a 'personal data file system' within the meaning of article 2 letter c of Directive 95/46[246], wherein data are processed within the meaning of said article 2 letter b.

Data produced in the course of banking and telecom activities are personal because they are identification numbers enabling to identify directly individuals, as laid down by the article 2, letter a. As for banking data, it should be self-evident that it constitutes personal data (see also recital 33 and article 28 of Directive 2005/60 on money laundering).

Telecom data have been the object of specific legislation. Pursuant to article 1 of Directive 2006/24 (Data Retention Directive) [247] , the content of electronic communications, including information consulted using an electronic communications network, should not be retained. 'Communication' is defined in article 2 letter d of Directive 58/2002 (E-privacy Directive)[248] as "any information exchanged or conveyed between a finite number of parties by means of a *publicly available electronic communications service*." We should therefore exclude the collection of content-related information from the analysis of the HEMOLIA database. The data that could seemingly be fused and retained are traffic and location data, which are defined in Directive 2002/58.

Pursuant to article 2 letter b, 'traffic data' means "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof." In turn, 'location data' (article 2 letter c) means "any data processed in an electronic communications network, indicating the geographic position of the terminal equipment."

---

[245] A synthesis of the content of these rights is contained in Porcedda (2013).

[246] Data Protection Directive.

[247] Directive 2006/24/Ec of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/Ec (Data Retention Directive), p. 54–63, 13 April 2006.

[248] Directive 2002/58/Ec of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) (E-Privacy Directive), p. 37-47, 31 July 2002.

Moreover, it should be recalled that the European Court of Human Rights (ECtHR) asserted that the notion of private life (article 8 ECHR) should be interpreted broadly and that it:

> "[C]orresponds with that of the Council of Europe's Convention of 28 January 1981 (…) whose purpose is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined as "any information relating to an identified or identifiable individual" (Article 2)."[249]

As acknowledged by the ECtHR in *Copland v. UK*, telephone calls, information derived from the "monitoring of personal Internet usage"[250], and e-mails amount to private life and correspondence within the meaning of article 8 §1 ECHR. Article 8 protects all types of correspondence irrespective of whether they are private.[251] The Court further clarified that "information relating to the date and length of telephone conversations and in particular the numbers dialled can give rise to an issue under Article 8 as such information constitutes an "integral element of the communications made by telephone. The mere fact that these data may have been legitimately obtained by the College, in the form of telephone bills, is no bar to finding an interference with rights guaranteed under Article 8.""[252] The ECtHR also declared that the person has a reasonable expectation of privacy if there is no warning about the monitoring of 'correspondence'.[253]

While the ECtHR has not, in the knowledge of the writer, explicitly ruled on the nature of banking data, such data could be deemed to fall within the meaning of private life as it could reveal information that fall within the meaning of private life as judged by the Court in a number of cases.[254]

Thus, the collection of personal data is susceptible of affecting both the fundamental rights to data protection (article 8 EUCFR) and private and family life (article 7 EUCFR as interpreted by ECtHR under ECHR article 8).

15.2.2 Data Protection

The collection of personal data represents an interference with the right to data protection, unless it fulfils one of the conditions of legitimacy, as addressed in section 4. The attributes that are likely to be affected are sensitive data for generic Anti-Money laundering, and data minimization for HEMOLIA.

---

[249] Rotaru V. Romania.

[250] This formulation is vague; it is unclear whether it includes the indexing of the searches made, or the monitoring of published information. Case of Copland V. The United Kingdom, n. 62617/00, European Court of Human Rights, 3 April 2007 at § 41.

[251] Niemietz V. Germany at § 32.

[252] Copland V. The United Kingdom at § 43.

[253] Ibid., at § 42.

[254] For instance, Shimovolov v. Russia; Leander v. Sweden; and S. and Malone v. the United Kingdom.

15.2.2.1 Sensitive data

While banking data and telecom data are not considered sensitive data *per se*, they can *reveal* sensitive information about the data subject pursuant to article 8 of Directive 95/46[255] and 6 of Council Framework Decision 2008/977/JHA[256] (which would ideally apply to the present case, where information about individuals from different member states are requested). Article 6 lays down that "The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of data concerning health or sex life shall be permitted only when this is strictly necessary and when the national law provides adequate safeguards." Thus, the processing of banking (and telecom) data is likely to intrude upon the protection of sensitive data, unless the law provides for appropriate safeguards.

15.2.2.2 Data minimization

The integration between financial/banking data and telecom data (HEMOLIA) raise the issue of data minimization, i.e. the use of the minimum amount of data necessary.

In S. and Malone v. United Kingdom, the ECtHR acknowledged that "The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards (…). The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that *such data are relevant* and *not excessive in relation to the purposes* for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."[257] The ECtHR went further and noted that "The core principles of data protection require the retention of data to be *proportionate* in relation to the purpose of collection and insist on limited periods of storage (see paragraphs 41-44 above). These principles appear to have been consistently applied by the Contracting States in the police sector in accordance with the Data Protection Convention and subsequent Recommendations of the Committee of Ministers (see paragraphs 45-49 above)."[258]

The fusion of telecom data with financial data for the purposes of detecting money laundering is likely to infringe the attribute of data minimization.

15.2.3 Secondary effects of the processing of sensitive data

[255] Data Protection Directive.

[256] Council Framework Decision 2008/977/Jha.

[257] Malone V. The United Kingdom, n. 8691/79, European Court of Human Rights, 2 August 1984 at § 103.

[258] Ibid., at § 107.

In the context of the scenario, the processing of information revealing sensitive data that relate to X, Y and Z's participation in society (autonomy and participation), could affect at least the right to freedom of thought, conscience and religion (article 10 EUCFR), The fused data may reveal one's religion or political preferences (*forum internum*).

15.2.4 Privacy

Collecting and storing data relating to the private life of an individual fall within the application of article 8 § 1 ECHR.[259] The ECtHR clarified that "the storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8"[260] and that "to establish the existence of such an interference, it does not matter whether the information communicated is of a sensitive character or whether the persons concerned have been inconvenienced in any way."[261] *A fortiori*, and as acknowledged by the ECtHR in Rotaru v. Romania,[262] the Court stressed that the storage and use of the information, coupled with refusing the applicant an opportunity to challenge it, amount to an interference.

Moreover, insufficient knowledge of the collection appears as an important factor to appraise the existence of an interference with one's private life.[263] Indeed, a person has a reasonable expectation of privacy if there is no warning about the monitoring of 'correspondence'.[264]

The fusion of banking/financial and telecom data will also produce effects on two other attributes: autonomy and participation; and social relations and identity.

15.3 Limitations to the rights and level of intrusion

15.3.1 Limitations

Neither data protection nor privacy nor freedom of thought, conscience and religion are configured as absolute rights in the sense of not allowing for any limitations (see D2.4 for more details). The attributes of privacy analysed have different weights. *Since the confidentiality of personal communications is very close to the core of the right to privacy, the weight given to the attribute is 4. The attributes autonomy and participation, and social relations and identity, are not close to the core, and should weigh 1.*

---

[259] Amann V. Switzerland at § 65.

[260] Ibid.

[261] ibid., at § 69; Joined Cases C-465/00, C-138/01 and C-139/01, K Rechnungshof (C-465/00) V Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) V Österreichischer Rundfunk, n. Court of Justice of the European Union, 20 May 2003 at § 75.

[262] Rotaru V. Romania at § 46.

[263] Copland V. The United Kingdom at § 44.

[264] Ibid., at § 42.

As for data protection, since sensitive data *are very close to the core, the weight given to the attribute is 4. Data minimization in the context of police operations should have a medium weight of 2.*
As for freedom of thought, conscience and religion, the *forum internum* is very close to the core (thus would weight 4 in other circumstances), but since the scenario is based on the assumption of non-discrimination, *it weighs 2*.
Thus, the permissibility of the intrusion is subject to an assessment of legality, necessity and proportionality. Establishing whether the intrusion is "in accordance with the law" within the meaning of article 8.2 ECHR and "provided for by the law" (article 52.1 EUFCR) is not possible, due to the fact that the scenario is jurisdiction-neutral.

15.4 Level/intensity of intrusion

Based on the discussion on the three rights, and with a view to provide an assessment, it could be said that, in the context of the scenario where only the information of the suspects is obtained (the assessment would be different for the blanket use of HEMOLIA as such to filter suspect transactions), the intensity of the intrusion is not as such as to impede the enjoyment of the right. *In all cases, the intensity of the intrusion should weigh 2.*

15.4.1 Considerations on the permissibility of Anti-Money laundering tools and HEMOLIA

In the scenario, the police investigate on illicit drugs and arms trafficking, which are areas of particularly serious crime with a cross-border dimension (article 83 TFEU[265]). Article 3 letter a of the Council Framework Decision 2008/977/JHA, which oversees the exchange of personal data transmitted or made available between Member States (article 1 letter a), lays down that "Personal data may be collected by the competent authorities only for specified, explicit and legitimate purposes in the framework of their tasks and may be processed only for the same purpose for which data were collected. Processing of the data shall be *lawful* and adequate, relevant and not excessive in relation to the purposes for which they are collected."[266]

Directive 2005/60/EC of The European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing[267] defines money laundering as an offence and lays down rules to combat it. Pursuant to article 3.5 letter b, drugs trafficking is

[265] Consolidated Versions of the Treaty on European Union (Teu) and the Treaty on the Functioning of the European Union (Tfeu), Official Journal C 83/01, p. 30 March 2010.
[266] Council Framework Decision 2008/977/Jha.
[267] See at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2005L0060:20110104:EN:PDF (accessed on 15 June 2013).

identified as a serious crime, the profits of which, converted into property, constitute money laundering.
In particular, credit and financial institutions are obliged to apply due diligence for the sake of money laundering, and to report any activities susceptible of constituting suspicious activities of money laundering. Pursuant to article 30, they must keep records and statistical data for the purposes of investigations. Member states have to establish financial inspection units (FIUs) tasked with combatting money laundering and terrorist financing. Recital 43 reminds that the Commission is empowered to adopt implementing rules to clarify the technical aspects of the provisions of the Directive, taking into account technological development useful for the fight against money laundering.

The link between money laundering and trafficking is clarified further by Council Recommendation of 25 April 2002 on improving investigation methods in the fight against organised crime linked to organised drug trafficking: simultaneous investigations into drug trafficking by criminal organisations and their finances/assets.[268]
The recitals recall the Commission's plan to use new investigation techniques (1); promote the simultaneous use of investigation techniques (4 and 5); encourage to make use of multiple sources, ranging from police databases to private sources (8).
The latter, in particular, gives indication about the types of authorization needed in relation to the source of information: "internal such as the databases of law enforcement bodies" (no need of authorization); "or external whether public (with public access where relevant) or private (consultation by means of a court order)."
Point A of the Recommendation invites to apply simultaneous investigation techniques targeting financial assets, point B encourages the setting up of groups specialized in assets investigation, point C recommends creating direct liaisons between responsible individuals of relevant authorities (police, tax etc.) and, in general, point B supports the creation of joint investigation teams and the support by Europol.

Prima facie, existing regulation seems to support the creation of Anti-Money laundering and systems like HEMOLIA for the financial and banking data part. It should be reminded that the expressions "in accordance with the law" and "provided for by the law" are two-fold.[269] Not only should there be a legal basis in domestic law, but such law should also respect certain features in terms of quality. Inter alia, it should be accessible, respect the rule of law[270] and, when the law does

[268] See at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002H0515%2801%29:EN:HTML (accessed on 15 June 2013).
[269] See, *inter alia*, Perry V. The United Kingdom at § 45; Case of Shimovolos V. Russia, n. 30194/09, European Court of Human Rights, 21 June 2011 at § 67.
[270] Amann V. Switzerland at § 70.

not concerns a secret measure of surveillance[271], enable individuals to foresee[272] the consequences[273] it has upon them.

However, the legislation does not mention the integration of information collected in the course of Telecom activities into a single database for the purposes of money laundering. Directive 2006/24 [274] lays down rules on the mandatory retention of telecom data for the purposes of serious crime. Illicit drugs and arms trafficking are considered serious crimes pursuant to article 83 TFEU. However, article 4 of Directive 2006/24 mandates that "data retained in accordance with this Directive are provided only to the competent national authorities in *specific cases* and *in accordance with national law*. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights."
Thus, the systematic fusion of banking and telecom data in a unique database would require a dedicated legal basis[275] adopted at the member state level.[276] *Prima facie*, it seems that the fusion of telecom and banking data is unlawful.

Disproportionality has to be judged on a case-by-case basis, in relation to the legitimate aim.[277] The ECtHR judged that the prevention of crime and the protection of the rights of others are legitimate aims under paragraph 2 of Article 8.[278] In *Laender v. Sweden*, the ECtHR clarified that *"*The notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued (see, inter alia, the Gillow judgment of 24 November 1986, Series A no. 109, p. 22, § 55). However, the Court recognises that the national authorities enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved." [279]
The ECtHR stated that "There can be no doubt as to the necessity, for the purpose of protecting national security, for the Contracting States to have laws granting the competent domestic authorities power, firstly, to collect and store in registers not

[271] Shimovolos V. Russia at § 68.
[272] Case of Yildirim V. Turkey, n. 3111/10, European Court of Human Rights, 18 December 2012 at § 57.
[273] Ibid., at § 59.
[274] Data Retention Directive.
[275] Case of Taylor-Sabori V. The United Kingdom, n. 47114/99, European Court of Human Rights, 22 January 2003 at §§ 18 19.
[276] Case C-301/06, Ireland V European Parliament and Council n. Court of Justice of the European Union, 10 February 2009.
[277] Niemietz V. Germany at § 37.
[278] Ibid., at § 36.
[279] Leander V. Sweden at § 58.

accessible to the public information on persons (…).”[280] However, a “system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it… (see the Klass and Others judgment of 6 September 1978, Series A no. 28, pp. 23-24, §§ 49-50).”[281]

15.5 Quantification

The reliability of the above considerations must be assessed. Data protection: the state of the law is clear, especially with regards to sensitive data and data minimization; moreover, case law on both attributes exists. The reliability of the analysis of intrusiveness is 1.

Private life: either directly applicable case law exists, or analogously applicable legal materials that are relevant for the case under analysis. The reliability of the analysis of intrusiveness is 1.

Freedom of thought, conscience and religion: the right was considered in terms of secondary effects, and relied on the analysis of a team member based on previous study of case law. Reliability is thus ¾.

	Abstract weight[282]	***Intrusiveness***[283]	***Reliability of the state of law***[284]	***Value***[285]
Data protection – sensitive data	***4***	***2***	***1***	***8***
Data protection - minimization	***2***	***2***	***1***	***4***
Right to private life - communications	***4***	***2***	***1***	***8***
Right to private life – autonomy and participation/ social identity and relations	***1***	***2***	***1***	***2***
Freedom of thought, conscience and	***2***	***1***	***¾***	***1,5***

[280] Ibid., at § 59.
[281] Ibid., at § 60.
[282] Scale: 1 low, 2 medium, 4 high.
[283] Scale: as above.
[284] Scale: ½ low (lay person), ¾ medium (expert team), 1 high (expert team with reference to clear case law).
[285] Scale: when used by expert team, from ¾ to 16. All values above 10 (i.e., either 12 or 16) will mean that no security benefit from the use of the technology as described can legitimise its use due to fundamental rights consequences.

religion (forum internum)				

15.6 Further considerations

This assessment does not include the right to a fair trial. Hence, the possible use of the recordings as evidence in the trial has not been addressed.
This assessment provides a focus solely in respect of the rights of the individual targeted for surveillance; therefore, as we are assuming the somewhat uncharacteristic targeted use of HEMOLIA, no significant issues of third-party intrusion arise. However, the use of anti-money laundering technology, and HEMOLIA in particular, could apply to third party individuals that are not the target of investigations, and may therefore interfere with their fundamental rights to privacy, personal data, thought conscience and religion, association and assembly (etc.).
In the above assessment, we are assuming that the condition of being prescribed by law is met; otherwise, the measure would be impermissible. Furthermore, we are not assuming judicial authorization. But we add a caveat that judicial authorization results in a multiplier of ¾, so that for instance value 8 becomes 6 and therefore potentially permissible when strong security interests are being served effectively and efficiently.

16 Generic data analysis tools used on open data (MGP)

16.1 Description of the technology (readapted from TU Delft's description)

Data analysis tools are sense-making technologies for big data: they are able to examine large datasets on the Internet or in communications to find certain pre-defined classifiers, and are widely used for crime fighting and anti-terrorism surveillance.
In general, intelligence gathered on the Internet or from other types of communications has to be interpreted, integrated, analysed, and evaluated to provide awareness of the situation, using situational and threat assessment methods.

Social Network Analysis (SNA) is a method enabling statistical analysis of the patterns of communication within groups (i.e. social relations). The method is based on the hypothesis that the way members of a group communicate within and outside the group reveals important information about the group itself.
The investigations are performed with the method of *structural analysis*, which is based on a mathematical graph model consisting of nodes and edges that model the actors and the communication, respectively, within the group.
In addition, all kinds of weights can be introduced in the model, which represent the probability of an event to take place within the model. '**Bayesian belief networks (BBN)'** is one such uncertainty modelling and information fusion methodologies to exploit uncertain causal relationships between large collections of variables.

Data analysis tools are widely used by the law enforcement community as crime fighting tools. However, little is known about the effectiveness of the analysis tools. The *effectiveness depends heavily on the quality of the pre-defined classifiers*, which in the end have a large impact on the final outcome of the researched data.
If used in an appropriate way, data analysis tools can help police decision makers and front-line police officers to benefit from the products of crime data analysis, where the tools are the main theme in each policing strategy that aims to reduce crime, to prevent further offending, and to apprehend criminals. Many data analysis tools have been used by the U.S. Government to stop terrorist programs.[286]

Data analysis tools performing social network analysis abound.[287] Collecting, interpreting, integrating, analysing, and evaluating large data sets combines the four

[286] Note: Delft wrote "The programs in which these tools were used have been discontinued due to controversy over whether they violate the 4th Amendment to the United States Constitution." The recent revelation on PRISM as far as analysis tools are concerned suggest that this may not be the case.
[287] A list can be found at: http://www.gmw.rug.nl/~huisman/sna/software.html (accessed on 16 June 2013).

types of functions identified in SURVEILLE D2.4[288]: fusing, identifying, mining, and interpreting. The potential intrusion of data analysis tools on fundamental rights can be severe, and a generic fundamental rights assessment cannot be conducted. A meaningful analysis requires describing the context and objective for which they are used.

16.1.1 Scenario-based use of data analysis tools: lawful and bona fides uses

Data analysis tools carrying out social network analysis (e.g. Networked Data Analysis and Data Transfer Analysis) appear in steps one to four of the scenario. Based on low-grade intelligence, the police consider performing analysis on, but not limited to, open data relating to X, discovering association with Y and Z, which triggers a covert Internet investigation (steps 3 and 4), including 'friending' the suspects on social media. 'Open data' are data posted on the Web and freely available and accessible to any user's browsing.

The scenario describes operations based on officers' lawful conduct and *bona fides*. At this stage, we must assume that the code is written in such a way that the software:

- Is not used for 'fishing expeditions', and that no databases of 'suspects' are built based on the data collected;
- Does not retain (or it automatically deletes) irrelevant data sieved in the process, that is data relating to innocent 'bystanders' or the private life of the suspect (i.e. family and private relations etc.)[289]
- Is controlled by police officers, so that any risks of automation are eliminated.

These and other potential for abuses will be treated elsewhere.[290]

Two operations could be identified from the scenario:

a. The use of tools to analyse *open data*, akin to the police patrolling the roads.
b. 'Following' specific individuals covertly based on evidence of a potential crime.

It appears that the use of data analysis tools is *covert* in both phases, since it is invisible and unannounced. It is unclear whether the analysis is performed on personal communications inaccessible to the wider public. The latter would require higher thresholds of justification, necessity and proportionality and has relevant implications for the fundamental rights analysis. However, since there are no clear hints at this, *I will consider the use of tools to analyse open data only, and will simply mention the problem of communications*. The purpose is to identify the social network of suspect X, who is a neutral individual, that is one without any particular

[288] Porcedda (2013).

[289] See the following case on data minimization (proportionality) in case of search and seizure of electronic data: Case of Robathin V. Austria, n. 30457/06, European Court of Human Rights, 3 July 2012.

[290] Likewise, the analysis may change in connection to a specific tool.

features susceptible of causing discrimination. Thus, no profiling[291] operations are derived from these tools.

16.2 Interference with fundamental rights (in the abstract)

Since suspects X, Y and Z are 'neutral' individuals, that is not identified by any features exposing them to discrimination, and no coercive action is imposed upon them, the following rights are excluded: non-discrimination, freedom of expression and information, freedom of thought, conscience and religion, freedom of assembly and association and freedom of movement. Thus, the rights affected are data protection and privacy. Keeping in mind what was said above about the specificities of the software and the uncertainty on the screening of communications, the relevant attributes are:

- Data protection (article 8 EUCFR): data quality;
- Privacy (article 7 EUCFR, 8 ECHR): Social identity and relations.[292]

16.2.1 Preliminary remarks on the legal meaning of open data

The European courts have not assessed yet the issue as to whether information published on social media and websites constitutes 'communications' within the meaning of article 7 EUCFR and 8 ECHR (correspondence). However, the Article 29 Data Protection Working Party (WP29) recalled that social media/networking services are not electronic communication services providers,[293] but Information Society Services Providers.[294] It could be argued that data published on the Web and meant to be available to the general public do not constitute (private) communications within the meaning of article 7 EUCFR and 8 ECHR.

In Lindqvist,[295] the Court of Justice of the European Union (CJEU) clarified that publishing personal information (about oneself or a third party) on the Web in such a way as to make it accessible by the general public constitutes processing of personal data within the meaning of article 2 of Directive 95/46/EC[296], regardless whether

[291] Profiling is defined in the Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, article 1 letter as "an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."

[292] A description of the two rights is contained in Porcedda (2013).

[293] Article 2, letter c) of Directive 2002/21/Ec of the European Parliament and of the Council of 7 March 2002 on a Common Regulatory Framework for Electronic Communications Networks and Services (Framework Directive), p. 33–50, 24 April 2002.

[294] Article 1 paragraph 2 of Directive 98/34/EC as amended by Directive 98/48/EC.

[295] Case C-101/01, Bodil Lindqvist, n. Court of Justice of the European Union, 6 November 2003 at § 27.

[296] Data Protection Directive.

such information is eventually accessed. Moreover, posting information on the Web is an action that does not fall in the household exemption laid down by article 3(2) of the Data Protection Directive.[297] The WP29 noted in this respect:

> "When access to profile information extends beyond self-selected contacts, such as when access to a profile is provided to all members within the SNS or the data is indexable by search engines, access goes beyond the personal or household sphere. Equally, if a user takes an informed decision to extend access beyond self-selected 'friends' data controller responsibilities come into force. Effectively, the same legal regime will then apply as when any person uses other technology platforms to publish personal data on the web. In several Member States, the lack of access restrictions (thus the public character) means the Data Protection Directive applies in terms of the internet user acquiring data controller responsibilities."[298]

It could be concluded that information published on the Web about personally identifiable individuals, such as one's contacts and friends, does not amount to communications, but is personal data controlled by the publisher pursuant to article 2 of the Data Protection Directive. In turn, this excludes the attribute 'confidential communications', which is closer to the core of privacy, and allows focusing on 'Social identity and relations' (unchecked social relations).

16.2.2 Privacy

The European Courts have not judged on the matter of data analysis tools applied to open data, but several existing judgments offer useful insights on the subject matter. The European Court of Human Rights (ECtHR) interprets the notion of private life broadly, and states that:

> "Article 8 is not limited to the protection of an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. It also protects the right to establish and develop relationships with other human beings and the outside world (…). There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"."[299]

Moreover, such a broad interpretation:

> "[C]orresponds with that of the Council of Europe's Convention of 28 January 1981 (…) whose purpose is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data

[297] C-101/01 - Lindqvist at §§ 46 47. See also Case C-73/07, Tietosuojavaltuutettu V Satakunnan Markkinapörssi Oy and Satamedia Oy, n. Court of Justice of the European Union, 16 December 2011 at § 44.

[298] Article 29 Data Protection Working Party, 'Opinion 5/2009 on Online Social Networking (Wp 163) ', Brussels, (2009) at 6.

[299] Shimovolos V. Russia at § 64. The Court referred to Rotaru V. Romania at § 59; Perry V. The United Kingdom at § 36., and S. And Marper V. The United Kingdom at §§ 95 96.

relating to him" (Article 1), such personal data being defined as "any information relating to an identified or identifiable individual" (Article 2)."[300]

Collecting and storing data relating to the private life of an individual fall within the application of article 8 § 1 ECHR.[301] The ECtHR clarified that "the storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8"[302] and that "to establish the existence of such an interference, it does not matter whether the information communicated is of a sensitive character or whether the persons concerned have been inconvenienced in any way."[303] Insufficient knowledge of the collection appears as an important factor to appraise the existence of an interference with one's private life.[304]

In *Shimovolos v. Russia*, the ECtHR went further and said that an interference with a person's private life persists when the data are collected and stored systematically "by security services on particular individuals (…) even if that data was collected in a public place." [305] Data publicly available on the Internet may be regarded as information available in the public place.

Thus, it could be said that the open data collection and processing of data on several persons' social relationships (with or without the knowledge of the individual) amount to an intrusion into private life within the meaning of article 8 § 1 ECHR.

16.2.3 Data protection

If the posting of data on the Web to the effect of making it publicly available constitutes processing, than the collection of such data by the police amounts to secondary processing.

As acknowledged by the CJEU in *Osterreichischer*, "Under Directive 95/46, subject to the exceptions permitted under Article 13, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, second, with one of the criteria for making data processing legitimate listed in Article 7."[306]

The exception of article 13 applies to the case at hand, as the police collection is, "An activity of the State or of State authorities unrelated to the fields of activity of individuals" pursuant to article 3(2) of the Directive 95/46/EC.[307]

The exception laid down by article 13 does not absolve the state from the obligation of complying with the principle of legality. Since the mere collection of personally identifiable data concerning the private life of an individual constitute an

[300] Peck V. The United Kingdom at § 57.
[301] P. G. And J. H. V. The United Kingdom at § 56.
[302] Amann V. Switzerland at § 65.
[303] ibid.; C-465/00 - Österreichischer Rundfunk and Others at § 75.
[304] Copland V. The United Kingdom at § 42.
[305] Shimovolos V. Russia at § 65. See also Amann V. Switzerland at § 69.
[306] C-465/00 - Österreichischer Rundfunk and Others at § 65.
[307] *C-101/01 - Lindqvist at §§ 43 44; C-73/07 - Satakunnan Markkinapörssi and Satamedia at § 42.*

interference of data protection (informational privacy in the meaning of Convention 108 as reminded above), such interference must be justified even in the case of activities of the state. A discussion on legitimate grounds for personally identifiable data collection is discussed in section 4 below.

Having excluded most data protection attributes from the analysis (see section 2 above), the only dimension that could be infringed is that of data quality. Although article 13 allows States to derogate partly from the requirements of article 6 of Directive 95/46, the importance of data quality is recognized by the ECtHR in the case of Rotaru v. Romania,[308] and in several *leges speciales*:

- Council Framework Decision 2008/977/JHA refers to data quality in recitals 11, 16 and 39, and article 7.[309]
- Council of Europe Data Protection Convention refers to it in article 5 (quality of data), which can only be limited under the conditions set in article 9.[310]
- Recommendation 15(87) which established derogations pursuant to article 9 of the Data Protection Convention, in particular Principles Principle 5 (Communication of data) and 7 – (Length of storage and updating of data).[311]

We could argue that a secondary processing represents an interference with the right to data protection and could in particular impact on its attribute of data quality, which cannot be verified by data subjects and is in turn relevant for the correct identification of suspects.

16.3 Limitations to the rights and level of intrusion

16.3.1 Limitations

Neither data protection nor privacy is configured as an absolute right.[312] Moreover, the attribute of private life analysed, 'social identity and relations' (unchecked social relations), is not close to the core, it should have weight 1. *D*ata quality is not an attribute close to the core, but in the context of investigations, where it could lead to substantive and procedural errors, it should weigh 2.

Thus, the permissibility of the intrusion is subject to an assessment of legality, necessity and proportionality. Establishing whether the intrusion is "in accordance with the law" within the meaning of article 8.2 ECHR and "provided for by the law"[313] is not possible, due to the fact that the scenario is jurisdiction-neutral. Our assessment is based on the assumption that proper legal basis exists for the operation.

[308] Rotaru V. Romania at § 36.
[309] Council Framework Decision 2008/977/Jha.
[310] Convention 108.
[311] Police Recommendation) R (87) 15.
[312] For more details, see Porcedda (2013).
[313] Article 52.1 Eucfr.

16.4 Level of intrusion

Based on the discussion on the two rights, and with a view to provide an assessment, it could be said that:

- *Since individuals X, Y and Z are aware about the possibility of some third-party access when developing one's social life in social media, the value of intrusion into the attribute of privacy should be 2.*

In fact, the ECtHR even said that "an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him."[314]

- *Since automatic individual decisions and other potential sources of problems were excluded from the scenario, but data subjects cannot access the data to rectify possible inaccuracies, the value of the interference into data quality is 2.*

The ECtHR further noted "both the storing of (…) information and the use of it, *which were coupled with a refusal to allow the applicant an opportunity to refute it*, amounted to interference with his right to respect for his private life as guaranteed by Article 8 § 1"[315] and understood as the collection of personal data.

16.4.1 Considerations on the permissibility of open data analysis tools

It should be reminded that the expressions "in accordance with the law" and "provided for by the law" are two-fold.[316] Not only should there be a legal basis in domestic law, but such law should also respect certain features in terms of quality. Inter alia, it should be accessible and enable its readers to foresee the consequences it has upon them. However, as the ECtHR recalled:

> "The Court reiterates in this connection that in the special context of secret measures of surveillance the above requirements cannot mean that an individual should be able to foresee when the authorities are likely to resort to secret surveillance so that he can adapt his conduct accordingly."[317]

It could be argued that performing analysis on *open data* (and only open data) is akin to the police patrolling the roads, and should thus not amount to a secret measure of surveillance. As a result, rules relating to such actions should be "foreseeable", namely "formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct."[318] In particular, with a view to

[314] Rotaru V. Romania at § 35.
[315] Ibid., at § 46.
[316] See, *inter alia*, Perry V. The United Kingdom at § 45; Shimovolos V. Russia at § 67.
[317] Shimovolos V. Russia at § 68.
[318] Case of Yildirim V. Turkey at § 57.

prevent abuses, "the law must indicate with sufficient clarity the scope of any such discretion and the manner of its exercise."[319] Social media and Web users should be thus fully informed about their vulnerability to police checks.
It should be noted that the lack of adequate rules in this respect would have an impact on two rights that have not been considered so far. As noted in SURVEILLE D2.4[320], an excessive use of covert technology negatively affects the exercise of one's right to access information (freedom of expression and information) and to participation in public policy (non-discrimination), which are thus potential secondary effects of the intrusion.

Covert investigations on specific individuals, instead, would amount to secret measures of (individual) surveillance, which carries evident risks of arbitrariness. In this case:

> "The law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any measures of secret surveillance and collection of data. In addition, because of the lack of public scrutiny and the risk of abuse intrinsic to any system of secret surveillance, the following minimum safeguards should be set out in statute law to avoid abuses: the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law."[321]

As noted in Rotaru v. Romania:

> "In order for systems of secret surveillance to be compatible with Article 8 of the Convention, they must contain safeguards established by law which apply to the supervision of the relevant services' activities. Supervision procedures must follow the values of a democratic society as faithfully as possible, in particular the rule of law, which is expressly referred to in the Preamble to the Convention. The rule of law implies, inter alia, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure (see the Klass and Others judgment cited above, pp. 25-26, § 55)."[322]

Thus, secret measures of (individual) surveillance should be carried out with judicial supervision, preferably in the form of a court order.

16.5 Quantification

The reliability of the above considerations must be assessed.

[319] Ibid., at § 59.
[320] Porcedda (2013).
[321] Shimovolos V. Russia at § 68.
[322] Rotaru V. Romania at § 59.

Data protection: the state of the law is of medium (3/4) reliability, especially with regard to law enforcement access of personal data; no direct case law on data quality in police matters exists.

Private life: although no directly applicable case exists, there are analogously applicable legal materials that are relevant for the case under analysis. The reliability of the analysis of intrusiveness is high (1).

Lawful collection of open data and covert measures of individual surveillance

	Abstract weight[323]	***Intrusiveness***[324]	***Reliability of the state of law***[325]	***Value***[326]
Data protection	***2***	***2***	***¾***	***3***
Right to private life	***1***	***2***	***1***	***2***

16.6 Further considerations

This assessment does not include the right to a fair trial. Hence, the possible use of the recordings as evidence in the trial has not been addressed.

This assessment provides a focus solely in respect of the rights of the individual targeted for surveillance; therefore, as we are assuming the somewhat uncharacteristic targeted use of data analysis tools, no significant issues of third-party intrusion arise. However, other uses of such tools could apply to third party individuals that are not the target of investigations, and may therefore interfere with their fundamental rights to privacy, personal data, thought conscience and religion, association and assembly (etc.).

In the above assessment, we are assuming that the condition of being prescribed by law is met; otherwise, the measure would be impermissible. Furthermore, we are not assuming judicial authorization. But we add a caveat that judicial authorization results in a multiplier of ¾ in the quantification scheme.

[323] Scale: 1 low, 2 medium, 4 high.
[324] Scale: as above.
[325] Scale: ½ low (lay person), ¾ medium (expert team), 1 high (expert team with reference to clear case law).
[326] Scale: when used by expert team, from ¾ to 16. All values above 10 (i.e., either 12 or 16) will mean that no security benefit from the use of the technology as described can legitimise its use due to fundamental rights consequences.

17 Data analysis tools/ data crawlers SCIIMS and OMNIFIND (MGP)

17.1 Descriptions readapted from TU Delft

17.1.1 SCIIMS

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.[327]

I. A 'smart' search engine is built for crawling through the Internet;
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 data-bases: 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.

17.1.2 OMNIFIND

OMNIFIND is a 'big data' gathering and analysis tool for business purposes.[328] 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,

[327] See at: http://www.sciims.co.uk/Publications_Links.html .
[328] See at: http://www-03.ibm.com/software/products/us/en/contentanalyticssearch.

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.[329]

17.1.3 Common features

These shallow descriptions seem to suggest that the two programs have similar functionalities, the only difference being that OMNIFIND looks at publicly available data only, whereas SCIIMS fuses open data with private sources. In turn, OMNIFIND is different from the generic data tools already analysed in that it does more than reconstructing the social network of the individual, but gathers all available data, based on search words. The descriptions hint at the application of profiling[330] operations, but in the absence of specific information, and given the complex and yet unclear features of such tools, I shall analyse them in the context of the scenario only.

17.1.4 Scenario-based use of SCIIMS and OMNIFIND

Data crawlers *may* appear in steps one to four of the scenario. Based on low-grade intelligence, the police consider performing research and analysis (including on open data) on X, and, after discovering association with Y and Z, a covert Internet investigation (steps 3 and 4), including 'friending' the suspects on social media. 'Open data' are data posted on the Web and freely available and accessible to any users browsing. It is clear that OMNIFIND could be used for the open data research, and SCIIMS for the covert investigation that makes use of other, unspecified sources. As discussed in the case of generic tools performing social network analysis based on open data, the scenario describes operations based on officers' lawful conduct and *bona fides*. At this stage, we must assume that the code is written in such a way that the software:

- Is not used for 'fishing expeditions', in that its use needs to be authorised;

---

[329] See at: http://www-03.ibm.com/software/products/us/en/contentanalyticssearch.

[330] Profiling is defined in the Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, article 1 letter as "an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."

- Does not retain (or it automatically deletes) irrelevant data sieved in the process, that is data relating to innocent 'bystanders' or the private life of the suspect (i.e. family and private relations etc.);[331]
- Is controlled by police officers, so that any risks of automation are eliminated;
- No databases containing biometrics are consulted (as suggested in the scenario);
- No monitoring (as understood in EU law) or interception of data in transit occurs.

Yet, differently from the generic data analysis tool, both systems fuse data, and as such could build databases of suspects. Whereas the covert Internet investigation is only initiated in the last step, the investigation would appear as covert to most people. The nature of the private databases is unknown, and this unfortunately seriously limits the depth of the assessment.
The purpose is to gather as much information as possible on suspects X, Y and Z, who are neutral individuals, that is, they do not have any particular features susceptible of causing discrimination.

17.2 Interference with fundamental rights (in the abstract)

Since suspects X, Y and Z are 'neutral' individuals, that is not identified by any features exposing them to discrimination, and no coercive action is imposed upon them, then non-discrimination, freedom of expression and information, and freedom of movement are not intruded upon. Thus, the rights affected are data protection and privacy. However, the indiscriminate collection may affect some attributes of, at least, freedom of thought, conscience and religion.
Keeping in mind what was said above about the specificities of the software and the uncertainty on the screening of communications, the relevant attributes are:

- Data protection (article 8 EUCFR): sensitive data; data minimization; data quality (open data);
- Privacy (article 7 EUCFR, article 8 ECHR): confidential communications (if at least metadata); social identity and relations (if information about social network); and autonomy and participation (if information about one's activities).[332]

17.2.1 Preliminary remarks on the information gathered

Data crawlers fuse data collected in different circumstances. The European Courts have not judged directly on matter of data crawlers,[333] but several existing judgments and legislation offer useful insights into the subject matter. Although the information we have on the two pieces of software is scant, the data collected relates to X, Y and Z, identified individuals, as laid down by the article 2, letter a of

[331] See the case following case on data minimization (proportionality) in case of search and seizure of electronic data: Robathin V. Austria.
[332] A description of the two rights is contained in Porcedda (2013).
[333] But see the Opinion of Advovate General Jaaskinen, Case C-131/12 Google Spain Sl, Google Inc. V Agencia Española De Protección De Datos (Aepd), Mario Costeja González, n. C-131/12, 25 June 2013.

Directive 95/46/EC[334]. Thus, the databases derived from them are 'personal data file systems' within the meaning of article 2 letter c of Directive 95/46, wherein data are processed within the meaning of said article 2 letter b.

All types of data may be collected, including data produced in the course of communications and disciplined by Directive 2002/58[335] as modified by Directive 2006/24. [336] Directive 2006/24 harmonizes the obligation for communications providers to retain the data that they produce for billing purposes. Pursuant to articles 1.2 and 5.2, the *content* of electronic communications, including information consulted using an electronic communications network (i.e. searches), should not be retained.
'Communication' is defined in article 2 letter d of the E-privacy Directive as "any information exchanged or conveyed between a finite number of parties by means of a *publicly available electronic communications service*."
A private database storing content data within the meaning of article 2 of Directive 58/2002 on identifiable individuals would be unlawful. Only a police database resulting from the *temporary* aggregation of lawfully intercepted content could be legal. For the sake of simplicity, I should thus exclude the analysis of content in the sense discussed. Information 'published' online does not constitute 'communications' but is tantamount to processed personal data. Its collection by police officers can be regarded as secondary processing (see the assessment of the generic data analysis tool for details).
Traffic data and location data (metadata) relating to the use of the Internet, within the meaning of article 2 letters b and c respectively of the E-privacy Directive, could be processed instead.

Yet, such metadata[337] constitutes 'communication' within the meaning of article 7 EUCFR (correspondence in article 8 ECHR). The European Court of Human Rights (ECtHR) clarified that "information relating to the date and length of telephone conversations and in particular the numbers dialled can give rise to an issue under Article 8 as such information constitutes an "integral element of the communications made by telephone. The mere fact that these data may have been legitimately obtained by the College, in the form of telephone bills, is no bar to finding an interference with rights guaranteed under Article 8.""[338] The Court further declared that the person has a reasonable expectation of privacy if there is no warning about the monitoring of 'correspondence'.[339]

[334] Data Protection Directive.
[335] E-Privacy Directive.
[336] Data Retention Directive.
[337] While such data still weigh 4 for the information it can reveal, the level of intrusion could be considered lower.
[338] Copland V. The United Kingdom at § 43.
[339] Ibid., at § 42.

Moreover, it should be recalled that the ECtHR interprets the notion of private life broadly, and state that:

> "Article 8 is not limited to the protection of an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. It also protects the right to establish and develop relationships with other human beings and the outside world (…). There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life."[340]

Such definition,

> "[C]orresponds with that of the Council of Europe's Convention of 28 January 1981 (…) whose purpose is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined as "any information relating to an identified or identifiable individual" (Article 2)."[341]

The information above should indicate with sufficient clarity that the use of SCIIMS and OMNIFIND is susceptible of interfering with both the fundamental rights to data protection (article 8 EUCFR) and private and family life (article 7 EUCFR as interpreted by the ECtHR under ECHR article 8).

17.2.2 Data Protection: sensitive data, data quality & data minimization

The collection of personal data represents an interference with the right to data protection, unless it fulfils one of the conditions of legitimacy, as addressed in section 4. The attributes that are likely to be affected by the use of both tools are sensitive data, data minimization and data quality.

17.2.2.1 Sensitive data

It can be safely assumed that the wide variety of data collected by SCIIMS and OMNIFIND could *reveal* sensitive information about the data subject pursuant to article 8 of Directive 95/46. Article 6 of Council Framework Decision 2008/977/JHA (which would ideally apply to the present case as the police exchanges information with other member states' authorities) lays down that "The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of data concerning health or sex life shall be permitted only when this is strictly necessary and when the national law provides adequate safeguards."

Thus, the processing of big data is likely to intrude upon the protection of sensitive data, unless the law provides for appropriate safeguards.

---

[340] Shimovolos V. Russia at § 64. The Court referred to Perry V. The United Kingdom at § 36; S. And Marper V. The United Kingdom at §§ 95 96.

[341] S. And Marper V. The United Kingdom at §§ 95 96.

17.2.2.2 Data minimization

The wide collection raises also issues of data minimization, i.e. the use of the minimum amount of data necessary. The ECtHR acknowledged that "The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards (…). The need for such safeguards is higher where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that *such data are relevant* and *not excessive in relation to the purposes* for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored".[342] The ECtHR further noted that, "The core principles of data protection require the retention of data to be proportionate in relation to the purpose of collection and insist on limited periods of storage (see paragraphs 41-44 above). These principles appear to have been consistently applied by the Contracting States in the police sector in accordance with the Data Protection Convention and subsequent Recommendations of the Committee of Ministers (see paragraphs 45-49 above)."[343]

The fusion of data from different sources is likely to infringe upon data minimization; the assessment of proportionality, though, can only be made by the courts in relation to the purpose of the data collection (legitimate aim).

17.2.2.3 Data quality (open data)

If the posting of data on the Web to the effect of making it publicly available constitutes processing, then the collection of such data by the police constitutes secondary processing, for which data quality is crucial.

As acknowledged by the Court of Justice of the European Union (CJEU) in *Osterreichischer*, "Under Directive 95/46, subject to the exceptions permitted under Article 13, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, second, with one of the criteria for making data processing legitimate listed in Article 7."[344]

The exception of article 13 applies to the case at hand, as the police collection is, "An activity of the State or of State authorities unrelated to the fields of activity of individuals" pursuant to article 3(2) of the Directive 95/46.[345]

The exception laid down by article 13 does not absolve the state from the obligation of complying with the principle of legality. Since the mere collection of personally identifiable data concerning the private life of an individual constitute an interference of data protection (informational privacy in the meaning of Convention 108 as reminded above), such interference must be justified even in the case of

---

[342] Malone V. The United Kingdom at § 103.

[343] Ibid., at § 107.

[344] C-465/00 - Österreichischer Rundfunk and Others at § 65.

[345] *C-101/01 - Lindqvist at § 43 44; C-73/07 - Satakunnan Markkinapörssi and Satamedia at § 42.*

activities of the state. A discussion on legitimate grounds for personally identifiable data collection is discussed in section 4 below.
Although article 13 allows States to derogate partly from the requirements of article 6 of the Data Protection Directive, the importance of data quality is recognized by the ECtHR,[346] and in several *leges speciales*:

- Council Framework Decision 2008/977 refers to data quality in recitals 11, 16 and 39, and article 7.
- Council of Europe Data Protection Convention (Convention 108) refers to it in article 5 (quality of data), which can only be limited under the conditions set in article 9.
- Recommendation 15(87) which established derogations pursuant to article 9 of the Data Protection Convention, in particular Principles Principle 5 (Communication of data) and 7 – (Length of storage and updating of data).

We could argue that a secondary processing represents an interference with the right to data protection and could in particular impact on its attribute of data quality, which cannot be verified by data subjects and is in turn relevant for the correct identification of suspects.

17.2.3 Secondary effect of the processing of sensitive data

In the context of the scenario, the processing of information revealing sensitive data that relate to X, Y and Z's participation in society (autonomy and participation, social identity and relations), could affect at least the right to freedom of thought, conscience and religion (article 10 EUCFR), The fused data may reveal one's religion or political preferences (*forum internum*).

17.2.4 Privacy

Collecting and storing data relating to the private life of an individual fall within the application of article 8 § 1 ECHR.[347] The ECtHR clarified that "the storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8"[348] and that "to establish the existence of such an interference, it does not matter whether the information communicated is of a sensitive character or whether the persons concerned have been inconvenienced in any way."[349] *A fortiori*, the ECtHR stressed that the storage and use of the information, coupled with refusing the applicant an opportunity to challenge it, amount to an interference.[350]
Moreover, insufficient knowledge of the collection appears as an important factor to appraise the existence of an interference with one's private life.[351] Indeed, a person

[346] Rotaru V. Romania at § 36.
[347] P. G. And J. H. V. The United Kingdom; Peck V. The United Kingdom at § 57.
[348] Amann V. Switzerland at § 65.
[349] ibid.; C-465/00 - Österreichischer Rundfunk and Others at § 75.
[350] Rotaru V. Romania at § 46.
[351] Copland V. The United Kingdom at § 44.

has a reasonable expectation of privacy if there is no warning about the monitoring of 'correspondence'.[352]
The fusion of private and open data intrudes upon the following attributes: confidential communications; autonomy and participation; and social relations and identity.

17.3 Limitations to the rights and level of intrusion

Neither data protection nor privacy nor freedom of thought, conscience and religion are (fully) configured as absolute rights (see D2.4 for more details). The attribute of private life analysed have different impacts. *Since the confidentiality of personal communications and physical integrity are very close to the core, the value given to the attributes is 4. The attributes autonomy and participation, and social relations and identity, are not close to the core, and should weigh 1.*
As for data protection, since sensitive data *are very close to the core, the value given to the attribute is 4. Data minimization in the context of police operations should have a medium weight of 2. Data quality in the context of secondary processing by the police should also weight 2, as the control by the data subject is substituted by that of a supervisory authority.*
As for freedom of thought, conscience and religion, the *forum internum* is very close to the core (thus would weight 4 in other circumstances), but since the scenario is based on the assumption of non-discrimination, it weighs 2.
Thus, the permissibility of the intrusion is subject to an assessment of legality, necessity and proportionality. Establishing whether the intrusion is "in accordance with the law" within the meaning of article 8.2 ECHR and "provided for by the law" (article 52.1 EUFCR) is not possible, due to the fact that the scenario is jurisdiction-neutral.

17.4 Level/intensity of intrusion

Based on the discussion on the 3 rights, and with a view to provide an assessment, it could be said that, in the context of the scenario where only the information of the suspects is obtained (the assessment would be different for SCIIMS and OMNIFIND as such), and where proper safeguards are in place, the intensity of the intrusion is not as such as to impede the enjoyment of the right. *In the cases of privacy and data protection, the intensity of the intrusion should weigh 2. In the case of freedom of thought, conscience and religion, since it is a secondary effect, we assume a mild intrusion weighing 1.*

17.4.1 Considerations on the permissibility of SCIIMS and OMNIFIND

The considerations made for the assessment of data analysis tools (sheet # 16) and HEMOLIA (sheet # 15) apply here too.

[352] Ibid., at § 42.

17.5 Quantification

The reliability of the above considerations must be assessed.

Data protection: the state of the law is clear, especially with regards to sensitive data and data minimization; moreover, case law on both attributes exists. The reliability of the analysis of intrusiveness is 1.

Private life: either directly applicable case law exists, or analogously applicable legal materials that are relevant for the case under analysis. The reliability of the analysis of intrusiveness is 1.

Freedom of thought, conscience and religion: the right was considered in terms of secondary effects, and relied on the analysis of a team member based on previous study of case law. Reliability is thus ¾.

SCIIMS and OMNIFIND together

	Abstract weight[353]	***Intrusiveness***[354]	***Reliability of the state of law***[355]	***Value***[356]
Data protection – sensitive data	***4***	***2***	***1***	***8***
Data protection – minimization (SCIIMS)	***2***	***2***	***1***	***4***
Data protection – data quality (open data)	***2***	***2***	***1***	***4***
Right to private life – communications (metadata) (SCIIMS)	***4***	***2***	***1***	***8***
Right to private life – autonomy and participation/ social identity and relations	***1***	***2***	***1***	***2***

[353] Scale: 1 low, 2 medium, 4 high.
[354] Scale: as above.
[355] Scale: ½ low (lay person), ¾ medium (expert team), 1 high (expert team with reference to clear case law).
[356] Scale: when used by expert team, from ¾ to 16. All values above 10 (i.e., either 12 or 16) will mean that no security benefit from the use of the technology as described can legitimise its use due to fundamental rights consequences.

Freedom of thought, conscience and religion (forum internum)	***2***	***1***	***¾***	***1,5***

17.6 Further considerations

This assessment does not include the right to a fair trial. Hence, the possible use of the data as evidence in the trial has not been addressed.

This assessment provides a focus solely in respect of the rights of the individual targeted for surveillance; therefore, as we are assuming the somewhat uncharacteristic targeted use of SCIIMS and OMNIFIND, no significant issues of third-party intrusion arise. However, SCIIMS and OMNIFIND could also be used in ways that affect third party individuals that are not the target of investigations, and would therefore interfere with their fundamental rights to privacy, personal data, thought conscience and religion, and association and assembly (etc.).

In the above assessment, we are assuming that the condition of being prescribed by law is met; otherwise, the measure would be impermissible. Furthermore, we are not assuming judicial authorization. But we add a caveat that judicial authorization results in a multiplier of ¾, so that, e.g. value 8 becomes 6 and therefore potentially permissible when strong security interests are being served effectively and efficiently.

18 Cellular Phone Location Tracking (JA)

18.1 Description of the surveillance technology

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."[357]

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.

18.1.1 Scenario

The scenario does not identify a specific instance in which the use of cellular phone location tracking may prove an appropriate method of surveillance. The outline does however indicate that law enforcement may wish to monitor movement of suspects; thus the technology could prove of value where, for example, in the latter stage of the investigation officers wish to ascertain the likely route for importation of illicit substances or firearms. As such, monitoring of individuals may render useful intelligence that allows law enforcement to discern likely routes for the trafficking of contraband, based in part on patterns of movement of those suspected to be involved in criminal activity.

18.2 Fundamental rights affected

[357] Ian J. Samuel, 'Warrantless Location Tracking', New York University Law Review, 4:83 (2008) at 1327. Available at SSRN: http://ssrn.com/abstract=1092293.

18.2.1 Fundamental right to privacy or private and family life (Article 8 ECHR, Article 7 EUCFR, Article 17 ICCPR)

The protections afforded by the right to privacy require consideration in the case of the use of a location tracking of cellular phones for surveillance purposes by law enforcement. Location tracking of this nature is necessarily covert.

In the context of "private life", the European Court of Human Rights (hereafter *ECtHR*) has recalled that the notion is a broad one, which is not susceptible to exhaustive definition.[358] Of relevance too within the context of location tracking is the ECtHR having asserted that: "Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities."[359]

In the *P.G. and J.H. v. United Kingdom* case the ECtHR further noted as follows:

> "There are a number of elements relevant to a consideration of whether a person's private life is concerned in measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities, which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, though not necessarily conclusive factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (e.g. a security guard viewing through close circuit television) is of a similar character. Private life considerations may arise however once any systematic or permanent record comes into existence of such material from the public domain."[360]

With regard to the above, in the context of location tracking it may be held that, where such surveillance is covert, the monitoring would not be strictly analogous to the scenarios described by the Court (whereas locality may be immediately observed in an instant, patterns of movement would be intrinsically more complex to determine by a bystander). In this way one cannot draw the same inferences affirmed in the case of *Herbecq* where the observations of activities is "[I]dentical to that which he or she could have obtained by being on the spot in person."[361]

A further consideration is whether the equipment records data, or where there exists a systematic or permanent nature of the record this may give rise to consideration as to whether their has been an interference in the protection

[358] Niemietz V. Germany at § 29.
[359] Amann V. Switzerland at § 69.
[360] Ibid., at § 70.
[361] Case of Herbecq and the Association "Ligue Des Droits De L'homme" V. Belgium at 92.

guaranteed by Article 8 of the Convention.[362] ECtHR jurisprudence provides further guidance as to whether locality in the context of surveillance proves relevant to whether location tracking constitutes an interference in the right to privacy: "The Court reiterates that the storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding…"[363]

The ECtHR held in the case of *Copland v. United Kingdom*[364] that information of a less than notionally private nature (in this case, phone bills freely available to other parties which provide information as to another's conduct) did not infer that Article 8 guarantees to the right to privacy did not apply, rather: "The mere fact that these data may have been legitimately obtained… in the form of telephone bills, is no bar to finding an interference with rights guaranteed under Article 8 (ibid.). Moreover, storing of personal data relating to the private life of an individual also falls within the application of Article 8 § 1."[365] As such, while location data is 'freely made available' (to the telecommunications operator) by the individual carrying the cellular phone whilst switched on, nonetheless the person still enjoys the guarantees enshrined within Article 8.

The ECtHR has affirmed that the monitoring of movement, and the subsequent processing of the data obtained thereby, amounts to an interference in one's private life protected by Article 8 of the Convention.[366]

As evidenced by the above-cited case law, the purpose for which surveillance is conducted by law enforcement, and the use made of the data collected are the significant factors in determining whether an interference has occurred in the right to privacy.

18.2.2 Fundamental right to the protection of personal data (Article 8 ECHR, Article 8 EUCFR)

The EUCFR establishes a distinct right to the protection of personal data in Article 8, which states: "Everyone has the right to the protection of personal data concerning him or her."[367] The ECHR's Article 8's guarantees to a right to privacy have also been

[362] "Accordingly, in both the Rotaru and Amann judgments (to which the P.G. and J.H. judgment referred) the compilation of data by security services on particular individuals even without the use of covert surveillance methods constituted an interference with the applicants' private lives (Rotaru V. Romania at § 43.)." P. G. And J. H. V. The United Kingdom at § 57.
[363] Amann V. Switzerland at §§ 65-67; Rotaru V. Romania at §§ 43 44.
[364] Copland V. The United Kingdom.
[365] Ibid., at § 43.
[366] Uzun V. Germany at § 52.
[367] Article 8 Eucfr.

interpreted to cover the protection of personal data.[368] Article 17 of the ICCPR has been held to cover the protection of personal data.[369] The ECtHR has reiterated in its most recent cases[370] of the necessity of there being clear and sufficiently detailed guidelines as to the use of surveillance measures, in addition to minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.[371]

Also relevant in the European context is the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[372] (hereafter Convention 108). The provisions with the Convention 108 apply to any information relating to an identified or identifiable individual (personal data) processed wholly or partly by automatic means, and both by public and private parties. Of particular note in Convention 108 is Article 6, which states with respect to 'Special categories of data': "Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards."[373] Location tracking may engage this provision where, for example, a person visits a particular healthcare facility or place of worship. In this respect location may act as a proxy or indicator for other forms of sensitive personal data. Also relevant in the context of crime prevention activities vis-à-vis data protection is Recommendation No. R(87)15 on regulating the use of personal data in the police sector places on the collection of personal data. The appendix to the recommendation asserts that this activity should be limited to reflect the intention of suppressing a specific criminal offence, rather than reflect a broader preventative mandate of an unspecified description.[374]

The Council Framework Decision 2008/977/JHA[375] applies to and provides for the protection of personal data processed in the framework of police and judicial cooperation in order to prevent, investigate, detect or prosecute a criminal offence or execute a criminal penalty. However, in the context of the given scenario it must be taken into account that the Framework Decision has limited effect in respect of

[368] *See*, for example Leander V. Sweden at § 48; Peck V. The United Kingdom at § 59.
[369] *See*, for example, La Rue (2011) at 16, § 58. Available at: http://www2.ohchr.org/english/ bodies/hrcouncil/docs (accessed on 22 May 2013).
[370] See, for example, M. M. V. The United Kingdom at § 195.
[371] Amann V. Switzerland at § 68.
[372] Convention 108.
[373] Ibid., at article 6.
[374] Police Recommendation) R (87) 15.
[375] Council Framework Decision 2008/977/Jha.

the domestic setting; where data originates and is processed within a Member State its provisions do not apply.[376]

18.2.3 Freedom of movement and residence (Protocol 4 - Article 2 to ECHR, Article 45 EUCFR, Article 12 ICCPR)

Surveillance conducted by the location tracking of cellular phones may interfere in the enjoyment of the right to freedom of movement. The UN Human Rights Committee has noted with respect to Article 12 of the ICCPR: "Liberty of movement is an indispensable condition for the free development of a person" and that: "The permissible limitations which may be imposed on the rights protected under article 12 must not nullify the principle of liberty of movement, and are governed by the requirement of necessity provided for in article 12, paragraph 3, and by the need for consistency with the other rights recognized in the Covenant."[377] As mentioned earlier with respect to the right to the protection of personal data, an individual's locality or their pattern of movement can prove a contextual indication of other attributes of personal conduct that is of a sensitive nature. Knowledge of an individual's location may render detectable a person's political opinions, religious or other beliefs (when visiting a place of worship or political assembly, for example).

18.3 Permissible limitations to the fundamental rights that are engaged by the use of the technology for surveillance purposes

The rights engaged in respect of the use of location tracking by law enforcement for the purposes of monitoring a suspect are not absolute; the provisions within the ECHR, ECUCFR and ICCPR pertaining to the rights to privacy, the protection of personal data, and freedom of movement are all qualified by the permissibility of limitations placed upon them where such restrictions serve a legitimate aim, are necessary and proportionate.

The criteria by which such limitations may be deemed lawful interferences are articulated in, *inter alia*, ECHR Articles 8(2), Prot. 4 – Art. 10(2), EUCFR Article 52, ICCPR Articles 12(3) and 19(3). The intrusion into fundamental rights by a law enforcement agency's use of location tracking for the purpose of the detection or the prevention of crime may prove permissible where it can be shown to constitute a proportionate interference. As the review here does not concern a specific jurisdiction, questions as to the foreseeability of the intrusion and whether it be 'prescribed by law' are outwith the scope of this assessment. That said, in the context of a specific event, prior to placing a phone tap, a public authority would need to meet the condition that the impugned measure have some basis in domestic

[376] Preamble (ibid.), recital 7 states: The scope of this Framework Decision is limited to the processing of personal data transmitted or made available between Member States."
[377] Human Rights Committee (1999) at §§ 1, 2.

law i.e. be 'prescribed by law'. The ECtHR has reiterated the importance is places on the obligations incumbent upon the law enforcement agencies for the proper safeguard of fundamental rights in the context of surveillance activity, whereby it: "[F]urther observes that concerns which prompted the elaboration of the Data Protection Convention in regard to the increasing recourse to automation in all sectors are most acutely felt in the police sector, for it is in this domain that the consequences of a violation of the basic principles laid down in the Convention could weigh most heavily on the individual."[378]

18.4 Level of intrusiveness

The use of location tracking of a suspect by law enforcement may constitute an intrusion into several distinct fundamental rights. In each instance the severity of each interference is dependent upon a number of distinct criteria.

- With respect to the right to privacy, the level of intrusiveness of the use of location tracking can be considered to be significant where the monitoring activity can provide authorities with detailed information not just to movement, but also in respect of daily interactions and choices that can build a detailed pattern of behaviour. Locality therefore reflects more than simply one's physical location, but also a broader range of attributes that provide a high level of granularity pertaining to, for example, an individual's associations with others. Where cellular phones are frequently carried by an individual their tracking may provide the party conducting the monitoring with a extremely nuanced understanding of an individual's daily routine in both in public and notionally private areas (such as the home). Thus the interference may be qualified as of a 'high' weighting.

- The protection of personal data in accordance with the guarantees furnished by Article 8 of the ECHR has been considered pivotal to an individual's enjoyment of their private life: "[T]he Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained."[379] As has been already been noted, the collation and analysis of location tracking data carries particular risks pertaining to its capacity to furnish highly nuanced inferences – it might thus be constituted to fall within the ambit of 'Special categories of data' where, specifically, data pertaining to time and location of an individual provides a public authority with information of a highly sensitive nature. Furthermore, the ECtHR has stated that the need for such safeguards is all the more necessary where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes.[380]

[378] Rotaru V. Romania at § 43. For further elaboration see M. M. V. The United Kingdom at § 126. *See* also ibid., at §§ 121-41.
[379] *See* S. And Marper V. The United Kingdom at § 99.
[380] Ibid., at § 103.

- The ECtHR case law has affirmed that the notion of being "necessary in a democratic society" in respect of a surveillance activity must be considered to infer that the interference corresponds to a pressing social need and is proportionate to the legitimate aim pursued.[381] Thus, in assessing the proportionality of the use of location tracking one must consider whether other methods of investigation that are comparatively less intrusive could prove to sufficiently effective while constituting a lesser interference in the fundamental rights of the individual.

18.5 Qualifying the intrusion on the basis of a scale

	Abstract weight[382]	***Intrusiveness***[383]	***Reliability of the state of law***[384]	***Value***[385]
Right to privacy	***2***	***4***	***3/4***	***6***
Data protection	***2***	***4***	***3/4***	***6***
Freedom of Movement	***2***	***2***	***1/2***	***2***

18.6 Further considerations

This assessment does not include the right to a fair trial. Hence, the possible use of the recordings as evidence in the trial has not been addressed.

This assessment provides a focus solely in respect of the rights of the individual targeted for surveillance. However, the use of location tracking of an individual by a cellular phone device may subject other persons to monitoring (where another party makes use of the phone, for example) and may therefore also constitute interferences in respect of their fundamental rights, particularly as regards the rights to privacy and the protection of personal data. The monitoring of locality may also implicate others where indication of an individual's whereabouts infers an association with another party e.g. where one visits another person's home or business premises.

---

[381] Uzun V. Germany at § 78.
[382] Scale: 1 low, 2 medium, 4 high.
[383] Scale: as above.
[384] Scale: ½ low (lay person), ¾ medium (expert team), 1 high (expert team with reference to clear case law).
[385] Scale: when used by expert team, from ¾ to 16. All values above 10 (i.e., either 12 or 16) will mean that no security benefit from the use of the technology as described can legitimise its use due to fundamental rights consequences.

In the above assessment, the weight of the fundamental rights in question has been assessed in relation to surveillance without judicial authorization. If the surveillance measure is authorised by the judiciary, the weight (and the overall score) should be multiplied by 3/4.

19 Mobile Phone Tapping (JA)

19.1 Description of the surveillance technology

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.

19.1.1 Scenario

The scenario does not identify a specific instance in which the use of cellular phone tap may prove an appropriate method of surveillance. The outline does however indicate that law enforcement may wish to identify contact between suspects and other parties, thus the technology could prove of value where, for example, in the latter stage of the investigation officers wish to discern the scope of criminal activities and collect information related to other parties' possible involvement in their facilitation.

19.2 Fundamental rights affected

19.2.1 Fundamental right to privacy or private and family life (Article 8 ECHR, Article 7 EUCFR, Article 17 ICCPR)

The covert monitoring of cellular phone communications by law enforcement engages the protections guaranteed by the right to privacy. The ECtHR has recalled that 'private life' is a broad notion, "not susceptible to exhaustive definition."[386] Further, telephone communications are covered by the notions of "private life" and "correspondence" within the meaning of Article 8, and that the freedom of communication between users of the telecommunications services is of particular concern: "The Court recalls its findings in previous cases to the effect that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation

[386] Niemietz V. Germany at § 29.

may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them."[387]

A further consideration is whether the equipment records data, or where there exists a systematic or permanent nature of the record this may give rise to consideration as to whether their has been an interference in the protection guaranteed by Article 8 of the Convention.[388] ECtHR jurisprudence provides further guidance where the Court has determined: "[T]he storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding…"[389]

The ECtHR held in the case of *Copland v. United Kingdom*[390] that information of a less than notionally private nature (in this case, phone bills freely available to other parties which provide information as to another's conduct) did not infer that Article 8 guarantees to the right to privacy did not apply, rather: "The mere fact that these data may have been legitimately obtained… in the form of telephone bills, is no bar to finding an interference with rights guaranteed under Article 8 (ibid.). Moreover, storing of personal data relating to the private life of an individual also falls within the application of Article 8 § 1."[391]

The ECtHR has also affirmed that where the transmission of data to and its use by other authorities enlarges the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned, this constitutes a further separate interference with the applicants' rights under Article 8.[392]

As evidenced by the above-cited case law, the purpose for which surveillance is conducted by law enforcement, and the use made of the data collected are the significant factors in determining whether an interference has occurred in the right to privacy.

---

[387] Liberty and Others V. The United Kingdom at § 56.

[388] "Accordingly, in both the Rotaru and Amann judgments (to which the P.G. and J.H. judgment referred) the compilation of data by security services on particular individuals even without the use of covert surveillance methods constituted an interference with the applicants' private lives (Peck V. The United Kingdom at § 59.)." S. And Marper V. The United Kingdom at § 105.

[389] Amann V. Switzerland at §§ 65-67; Rotaru V. Romania at §§ 43 44.

[390] Copland V. The United Kingdom.

[391] Ibid., at § 43.

[392] Peck V. The United Kingdom at § 59.

19.2.2 Fundamental right to the protection of personal data (Article 8 ECHR, Article 8 EUCFR)

The EUCFR establishes a distinct right to the protection of personal data in Article 8, which states: "Everyone has the right to the protection of personal data concerning him or her."[393] The ECHR's Article 8's guarantees to a right to privacy have also been interpreted to cover the protection of personal data.[394] Article 17 of the ICCPR has been held to cover the protection of personal data.[395] The ECtHR has reiterated in its most recent cases[396] of the necessity of there being clear and sufficiently detailed guidelines as to the use of surveillance measures, in addition to minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.[397]

Also relevant in the European context is the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[398] (hereafter Convention 108). The provisions with the Convention 108 apply to any information relating to an identified or identifiable individual (personal data) processed wholly or partly by automatic means, and both by public and private parties. Of particular note in Convention 108 is Article 6, which states with respect to 'Special categories of data': "Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards."[399] Location tracking may engage this provision where, for example, a person visits a particular healthcare facility. In this respect location may act as a proxy or indicator for other forms of sensitive personal data. Also relevant in the context of crime prevention activities vis-à-vis data protection is Recommendation No. R(87)15 on regulating the use of personal data in the police sector places on the collection of personal data. The appendix to the recommendation asserts that this activity should be limited to reflect the intention of suppressing a specific criminal offence, rather than reflect a broader preventative mandate of an unspecified description.[400]

---

[393] Article 8 Eucfr.

[394] *See*, for example, Leander V. Sweden at § 48; Weber and Saravia V. Germany at § 79.

[395] *See*, for example La Rue (2011) at 16, § 58. Available at: http://www2.ohchr.org/english/ bodies/hrcouncil/docs (accessed on 22 May 2013).

[396] See, for example, M. M. V. The United Kingdom at § 195.

[397] Amann V. Switzerland at § 68.

[398] Convention 108.

[399] Ibid., at Article 6.

[400] Police Recommendation) R (87) 15.

The Council Framework Decision 2008/977/JHA[401] applies to and provides for the protection of personal data processed in the framework of police and judicial cooperation in order to prevent, investigate, detect or prosecute a criminal offence or execute a criminal penalty. However, in the context of the given scenario it must be taken into account that the Framework Decision has limited effect in respect of the domestic setting; where data originates and is processed within a Member State its provisions do not apply.[402]

19.3 Permissible limitations to the fundamental rights that are engaged by the use of the technology for surveillance purposes

The rights engaged in respect of the use of location tracking by law enforcement for the purposes of monitoring a suspect are not absolute; the provisions within the ECHR, ECUCFR and ICCPR pertaining to the rights to privacy, the protection of personal data, and freedom of movement are all qualified by the permissibility of limitations placed upon them where such restrictions serve a legitimate aim, are necessary and proportionate.

The criteria by which such limitations may be deemed lawful interferences are articulated in, *inter alia*, ECHR Articles 8(2), EUCFR Article 52. The intrusion into fundamental rights by a law enforcement agency's use of cellular phone tap for the purpose of the detection or the prevention of crime may prove permissible where it can be shown to constitute a proportionate interference. As the review here does not concern a specific jurisdiction, questions as to the foreseeability of the intrusion and whether it be 'prescribed by law' are outwith the scope of this assessment. Nevertheless, in the context of a specific event, prior to deploying a tap on a cellular phone, a public authority would need to meet the condition that the impugned measure have some basis in domestic law i.e. be 'prescribed by law'. The ECtHR has reiterated the importance is places on the obligations incumbent upon the law enforcement agencies for the proper safeguard of fundamental rights in the context of surveillance activity, whereby it: "[F]urther observes that concerns which prompted the elaboration of the Data Protection Convention in regard to the increasing recourse to automation in all sectors are most acutely felt in the police sector, for it is in this domain that the consequences of a violation of the basic principles laid down in the Convention could weigh most heavily on the individual."[403]

[401] Council Framework Decision 2008/977/Jha.

[402] Preamble (ibid.), recital 7 states: "The scope of this Framework Decision is limited to the processing of personal data transmitted or made available between Member States."

[403] Rotaru V. Romania at §§ 43 44. For further elaboration see M. M. V. The United Kingdom at § 126. *See* also ibid., at §§ 121-41.

19.4 Level of intrusiveness

The content of confidential communications, including discussions by telephone, fall within the core area of the right to privacy, or at least close to that core. In contrast, contact-related data, which furnishes information only in respect of the identities of the parties with whom a suspect communicates, falls outwith the core area of the confidentiality of communications and represents a medium weight of the affected right.

- With respect to the right to privacy, the use of a cellular phone tap can be considered to be an intrusion on a high level, where the monitoring activity may disclose to law enforcement a large volume of information pertaining to a person's private life.

- Access to the records of the use of a cellular phone also provides a party with detailed insight into the individual's patterns of association with others, constituting therefore a further interference in the right to privacy. Thus, the interference as a whole with regard to the right to privacy may be qualified as of a 'high' weighting.

- The protection of personal data in accordance with the guarantees furnished by Article 8 of the ECHR has been considered pivotal to an individual's enjoyment of their private life.[404] Collecting and analysing the data provided by a cellular phone tap inheres a capacity to furnish information pertaining to many facets of an individual's private life. Elements of the phone tap procedure will constitute automated processing and, as such, the ECtHR has stated that the need for safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes.[405]

- Considering the high level of intrusiveness of a cellular phone tap, the reader should consider that where an interference caused by a surveillance activity may be justified as being necessary in a democratic society it must correspond to a pressing social need and, furthermore, must be proportionate to the legitimate aim pursued.[406] Thus, in assessing the proportionality of the use of a cellular phone tap one must duly consider whether other comparatively less intrusive methods of investigation could prove sufficient while constituting a lesser interference in the fundamental rights of the individual.

19.5 Qualifying the intrusion on the basis of a scale

[404] *See* S. And Marper V. The United Kingdom at § 99.
[405] Ibid., at § 103.
[406] Uzun V. Germany at § 78.

	Abstract weight[407]	*Intrusiveness*[408]	*Reliability of the state of law*[409]	*Value*[410]
Right to privacy	***2***	***4***	***1***	***8***
Data protection	***2***	***2***	***3/4***	***3***

19.6 Further considerations

This assessment does not include the right to a fair trial. Hence, the possible use of the recordings as evidence in the trial has not been addressed.

This assessment provides a focus solely in respect of the rights of the individual targeted for surveillance. However, the use of cellular phone tap may subject other persons to a form of monitoring in that another party may also utilise the phone, constituting therefore an interference in respect of their fundamental rights. A cellular phone tap also proves an interference into others' fundamental rights as it necessarily furnishes personal data pertaining to those parties in association with the subject of the monitoring.

In the above assessment, the weight of the fundamental rights in question has been assessed in relation to surveillance without judicial authorization. If the surveillance measure is authorised by the judiciary, the weight (and the overall score) should be multiplied by 3/4.

[407] Scale: 1 low, 2 medium, 4 high.
[408] Scale: as above.
[409] Scale: ½ low (lay person), ¾ medium (expert team), 1 high (expert team with reference to clear case law).
[410] Scale: when used by expert team, from ¾ to 16. All values above 10 (i.e., either 12 or 16) will mean that no security benefit from the use of the technology as described can legitimise its use due to fundamental rights consequences.

20 Bibliography

'1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08', Judgment: Bundesverfassungsgericht (German Federal Constitutional Court) (2 March 2010).

'Opinion of Advovate General Jääskinen, Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González', C-131/12, Reference for a preliminary ruling from the Audiencia Nacional (Spain): (25 June 2013).

Article 29 Data Protection Working Party (2009), 'Opinion 5/2009 on online social networking (WP 163) ', (Brussels).

'Case C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy', Judgment of the Court (Grand Chamber): Court of Justice of the European Union (16 December 2011).

'Case C-101/01, Bodil Lindqvist', Reference for a preliminary ruling - Judgment: Court of Justice of the European Union (6 November 2003).

'Case C-275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU', Judgment: Court of Justice of the European Union (29 January 2008).

'Case C-301/06, Ireland v European Parliament and Council ', Judgment of the Court (Grand Chamber): Court of Justice of the European Union (10 February 2009).

'Case C-369/98, The Queen v Minister of Agriculture, Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher', Reference for a preliminary ruling, Judgment: Court of Justice of the European Union (14 September 2000).

'Case of Amann v. Switzerland', 27798/95, Judgment: European Court of Human Rights (16 February 2000).

'Case of Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria', 62540/00, Judgment: European Court of Human Rights.

'Case of Buckley v. the United Kingdom', 20348/92, Judgment: European Court of Human Rights (25 September 1996).

'Case of Bykov v. Russia', 4378/02, Judgment: European Court of Human Rights (10 March 2009).

'Case of Copland v. the United Kingdom', 62617/00, Judgment: European Court of Human Rights (3 April 2007).

'Case of Demades v. Turkey', 16219/90, Judgment: European Court of Human Rights (31 July 2003).

'Case of Friedl v. Austria', 15225/89, Judgment: European Court of Human Rights (31 January 1995).

'Case of Golder v. the United Kingdom', Judgment: European Court of Human Rights (21 February 1975).

'Case of Herbecq and the association “Ligue des droits de l'homme” v. Belgium', 32200/96 and 32201/96, Commission Decision: European Court of Human Rights (14 January 1998).

'Case of Hirst v. the United Kingdom', 74025/01, Judgment: European Court of Human Rights (6 October 2005).

'Case of Iordachi v. Moldova', 25198/02, Judgment: European Court of Human Rights (10 February 2009).

'Case of Kennedy v. The United Kingdom', 26839/05, Judgment: European Court of Human Rights (18 August 2010).

'Case of Khan v. the United Kingdom', 35394/97, Judgment: European Court of Human Rights (12 May 2000).

'Case of Klass and others v. Germany ', 5029/71, European Court of Human Rights (6 September 1968).

'Case of Kopp v. Switzerland', 23224/94, Judgment: European Court of Human Rights (25 March 1998).

'Case of Kruslin v. France', 11801/85, Judgment: European Court of Human Rights (24 April 1990).

'Case of Leander v. Sweden', 9248/81, Judgment: European Court of Human Rights (26 March 1987).

'Case of Liberty and Others v. the United Kingdom', 58243/00, Judgment: European Court of Human Rights (01 July 2008).

'Case of Lupker and Others v. the Netherlands', 18395/91, Decision of Admissibility: European Court of Human Rights (7 December 1992).

'Case of M. M. v. the United Kingdom', 24029/07 Judgment: European Court of Human Rights (29 April 2013).

'Case of Mentes and Others v. Turkey', 23186/94, Judgment: European Court of Human Rights (28 November 1997).

'Case of Niemietz v. Germany', 13710/88, Judgment: European Court of Human Rights (16 December 1992).

'Case of P. G. and J. H. v. the United Kingdom', 44787/98, Judgment: European Court of Human Rights (25 December 2001).

'Case of Peck v. the United Kingdom', 44647/98, European Court of Human Rights (28 January 2003).

'Case of Perry v. the United Kingdom', 63737/00, Judgment: European Court of Human Rights (17 July 2003).

'Case of Robathin v. Austria', 30457/06, Judgment: European Court of Human Rights (3 July 2012).

'Case of Rotaru v. Romania', 28341/95, Judgment: European Court of Human Rights (4 May 2000).

'Case of S. and Marper v. the United Kingdom', 30562/04 and 30566/04, 4 December 2008: European Court of Human Rights.

'Case of Shimovolos v. Russia', 30194/09, Judgment: European Court of Human Rights (21 June 2011).

'Case of Silver and Others v. the United Kingdom', 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, Judgment European Court of Human Rights (24 October 1983).

'Case of Stes Colas Est and others v. France', 37971/97, Judgment: European Court of Human Rights (16 April 2002).

'Case of Taylor-Sabori v. the United Kingdom', 47114/99, Judgment: European Court of Human Rights (22 January 2003).

'Case of Uzun v. Germany', 35623/05, Judgment: European Court of Human Rights (2 September 2010).

'Case of Vetter v. France', 59842/00, Judgment: European Court of Human Rights (31 May 2005).

'Case of Von Hannover v. Germany', 59320/00, Judgment: European Court of Human Rights (24 June 2004).

'Case of Weber and Saravia v. Germany', 54934/00, European Court of Human Rights (29 June 2006).

'Case of Yildirim v. Turkey', 3111/10, Judgment: European Court of Human Rights (18 December 2012).

'Charter of Fundamental Rights of the European Union', (2007), (Official Journal C 303/1), 1–22.

'Consolidated versions of the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU)', (Official Journal C 83/01).

'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data', (1981), in Council of Europe (ed.), (CETS No. 108; Strasbourg).

Council (2008), 'Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters', (OJ L 350), 60 –71.

Council of Europe (1950), 'Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No 11 and 14', (CETS n° 005; Rome).

European Parliament and Council (1995), 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive)', (OJ L 281), 31-50.

--- (2002), 'Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)', 33–50.

--- (2006), 'Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive)', (Brussels), 54–63.

European Parliament and European Council (2002), 'Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (e-Privacy Directive)', 37-47.

Human Rights Committee (1999), 'General Comment No. 27. Freedom of movement (Article 12)'.

'Joined Cases C-465/00, C-138/01 and C-139/01, K Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk', References for a preliminary ruling, Judgment: Court of Justice of the European Union (20 May 2003).

La Rue, Frank (2011), 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,' (United Nations Human Rights Council).

'Malone v. the United Kingdom', 8691/79, European Court of Human Rights (2 August 1984).

Party, Article 29 Data Protection Working (2011), 'Advice paper on special categories of data ("sensitive data")', (Brussels).

Porcedda, Maria Grazia (2013), 'Paper Establishing Classification of Technologies on the Basis of their Intrusiveness into Fundamental Rights. SURVEILLE deliverable D2.4', (Florence: European University Institute).

'Recommendation of the Committee of Ministers regulating the use of personal data in the police sector (Police Recommendation) R (87) 15', (1987), in Council of Europe (ed.), (Strasbourg).

Samuel, Ian J. (2008), 'Warrantless Location Tracking', *New York University Law Review,* 83 (4).

Simitis, Spiros (1999), 'Revisiting sensitive data', (Council of Europe).

'Volkszählungsurteil', 1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1, Judgment: German Bundesverfassungsgericht (Federal Constitutional Court) (15 December 1983).