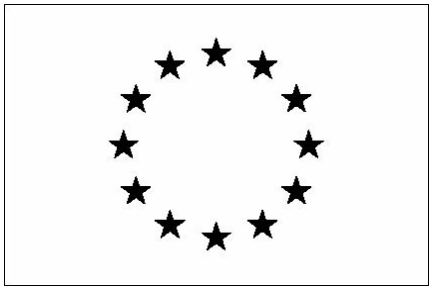

**FP7 – SEC- 2011-284725**
**SURVEILLE**
**Surveillance: Ethical issues, legal limitations, and efficiency**
Collaborative Project
*This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 284725*

# SURVEILLE Deliverable D2.9: Consolidated survey of surveillance technologies

Due date of Deliverable: 31.03.2015
Actual submission date: 08.04.2015

Start date of project: 1.2.2012 Duration: 41 months

SURVEILLE Work Package number and lead: WP2 Prof. Tom Sorell

Author(s):

The TU Delft team: Michelle Cayford and Coen van Gulijk

The Fraunhofer Team: Erik Krempel

The EUI team: Juha Lavapuro, Tuomas Ojanen, Martin Scheinin

The UW team: John Guelke; Helen McCabe and Tom Sorell

The EFUS team: Sebastian Sperber

| SURVEILLE: Project co-funded by the European Commission within the Seventh Framework Programme | | |
|---|---|---|
| **Dissemination Level** | | |
| **PU** | Public | **X** |
| **PP** | Restricted to other programme participants (including the Commission Services) | |
| **RE** | Restricted to a group specified by the consortium (including the Commission Services) | |
| **CO** | Confidential, only for members of the consortium (including the Commission Services) | |

# Table of contents:

## 1. Introduction

In this paper we build upon all earlier work in SURVEILLE Work Package 2 to present a consolidated 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 rights.

Although assessment 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 as a means of achieving a surveillance goal, but its use can nevertheless be morally problematic or intrude into 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 local authority. This scenario was constructed by the European Forum for Urban Security (a partner in the SURVEILLE project).

The technological assessment builds on previous SURVEILLE work: namely, Deliverable D2.1, which surveyed 43 technologies and introduced a range of considerations relevant to technological assessment. As work package 2 developed, the wide focus of D2.1 was narrowed down to look at technologies used in particular contexts. As well as narrowing down the focus to 14 technologies, D2.6 introduced the technique of surveying these in relation to a scenario of typical use, in D2.6 a serious crime investigation, and demonstrated how technological assessment can be summarised and related to normative assessment of actual dilemmas facing investigators and policy-makers. D2.8 extended this framework to Internet monitoring and other technologies used in a counter-terrorism context. In D2.9 we now turn to the use of surveillance technologies used by local authorities. D2.6, D2.8 and D2.9, while using the initial survey in D2.1 as a basis for technology selection have not been

restricted to the initial survey. In all three deliverables further technologies used in the contexts considered have been considered as well as technologies from the original list. In D2.9, five out of the 10 technologies analysed – the social media intelligence analysis, the CCTV, the Smart CCTV, the UAV (Unmanned Aerial Vehicle) and the thermal camera – either the technology or a similar technology featured in the D2.1 survey. To these five another five technologies not featured in D2.1 are added – a system for crime prediction, automatic number plate recognition, radio frequency identification (RFID), a system for automatic detection of abnormal behaviour, and a system for sharing CCTV images among police and businesses.

The ethical assessment builds on previous SURVEILLE work: namely Deliverable D2.2, 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 other things being equal – action that is *prima facie* morally objectionable. For example, the use of 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 way 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 taking moral risk unless the seriousness of the crime investigated merits it. In section 3.3.2, these considerations, outlined in Deliverable D2.2, are related to particular technologies and a realistic local authority use of surveillance for urban security and public order purposes.

The legal analysis builds upon previous SURVEILLE work in Deliverable D2.4 that outline the way in which surveillance technologies intrude on fundamental rights. Deliverable D2.9 applies this work, and the fundamental rights intrusion assessment methodology developed in D2.6 and D2.8 to specified uses of selected technologies in the context of the local authority scenario.

In section 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 sixteen for the intrusion into different fundamental rights represented by the use of the technology as proposed in the scenario. Usability assessments of the technology are scored out of ten, 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 local authority use for surveillance for urban security and public order purposes where a number of technologies surveyed in the matrix might be used for specific purposes. In 3.3 there is a detailed commentary on the technical, ethical and fundamental rights 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.

Section 4 constitutes a consolidated synthesis of SURVEILLE Work Package 2 as a whole.

## 2. A Matrix of Surveillance Technologies Resulting from the Third Scenario

### 2.1 Combined Matrix

There follows (on page 6) a matrix of surveillance technologies that reflects assessments of usability and of the risks of violating both ethical standards and fundamental rights. The fundamental rights assessments also differentiate the intrusion posed in the following

scenario to different individuals' rights, naming the different individuals whose rights are affected to different extents. For example in the case of CCTV, it is judged that Neil is subjected to a greater interference with his fundamental right to privacy than is the case with Kezia.

The assessments are represented by way of numerical scores awarded in the usability and fundamental rights assessments and by a red-amber-green 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 emphasised that this scenario-based assessment methodology addresses the use of specific surveillance technologies in the context of a fictional but realistic and complex scenario concerning surveillance usage by local authorities developed by the European Forum for Urban Security. The local authority surveillance-use scenario will be presented and discussed in Section 3.2 that follows. In total ten technologies are surveyed. These technologies feature as options for use by local authorities in the scenario.

| Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | HUMAN RIGHTS AND ETHICAL ISSUES | | | | |
| Technologie | Usability | 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)<br>Moral Risk of Intrusion | Other Fundamental Rights | Moral Risk to Trust and Chilling Effect |
| 1. Predpol | 5.5 | | | ¾ | 1½<br>*Non-Discrimination* | |
| 2. Cybels Intelligence | 6 | | 8 | 8 | 12<br>*Liberty* | |
| 3. ANPR | 6.5 | | 2 or 8 | 2 or 8 | | |
| 4. RFID in transport ticket | 6 | | 2 or 8 | 2 or 8 | | |
| 5. CCTV | 3 | | 0 (Niall), 2 (others) | 4 (Neil), 1 (Kezia) | 3 (Leonard) | |
| 6. Smart CCTV | 7 | | 2 | 1 | | |
| 7. Automatic detection of abnormal behaviour ADABTS | 2 | | 2 | 1 | 2<br>*Non-Discrimination* | |
| 8. UAV | 5 | | 8 (Wayne), 2 (others) | 8 (Wayne), 2 (others) | 4<br>*Association*<br>4<br>*Assembly* | |
| 9. Thermal camera | 7.5 | | 4 (Yuri), 0 (Xandra), 2 (Others) | 4 (Yuri), 2 (Xandra) | | |
| 10. Facewatch | 3.5 | | 8 | 4 | | |

Scores for **usability** run from 0-10, 0 representing the least usable, and 10 the most usable technology. Fundamental rights intrusion scores run from 0-16, 0 representing no interference with fundamental rights, 16 representing the most problematic intrusion. Whenever pertinent, the fundamental rights intrusion assessment has been performed separately in respect of persons situated differently in relation to a specific phase in the evolving scenario. Hence, it covers also issues of significant third-party intrusion. Ethical risk assessments are expressed via a colour-coding system. No colour is used where the ethical 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.

## 2.2 Methodologies

### 2.2.1 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 relied on three further factors, to give ten factor in total, each receiving a mark of 1, 0.5 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.[1] 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.

'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 it is reasonable to expect that success is achievable. In the absence of either, the technology scores '0'.

[1] '*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.

‘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 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 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, ‘1’ is scored. The score for these three factors are added together to a score for cost out of three.

The third category contributing to the overall score of 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 simply 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 in the case with iris-scans and DNA sampling for personal identification. Technologies qualifying as 'excellent' have 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, its 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 given the overall usability score out of 10.

### 2.2.2 Scoring Ethics

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

*The moral risk of intrusion* on this view involves penetration of one of three distinct 'zones' of privacy, discussed in SURVEILLE deliverable D2.2, and DETECTER deliverable D5.2.[3] These are bodily privacy, penetrated by close contact, touching or visual access to the naked body;

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

[3] 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

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.[4] 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

[4] 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.

be damaged by what is perceived as excessive, ethically problematic uses of technology.[5] The second category is, interpersonal social trust among the population – damage to this social trust is sometimes referred to as the 'chilling effect'.[6] 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 – 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.[7] 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.

### 2.2.3 Scoring Fundamental Rights

The scores for fundamental rights intrusion, given by the EUI team in SURVEILLE, follow the methodology developed in SURVEILLE deliverables D2.6 and D2.8. In those earlier papers intrusion scores between 0 and 16 were attributed to surveillance technologies or techniques used, respectively, in an organised crime scenario (D2.6) and a terrorism prevention scenario (D2.8). In the current deliverable the same scoring methodology is applied in the context of the urban security scenario. 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,[8] identification of attributes within a fundamental right in

[5] 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
[6] See, for example: DeCew, 1997, 64 on weakening of associational bonds, contributing to "wariness, self-consciousness, suspicion, tentativeness in relations with others".
[7] See for example Moeckli and Thurman DETECTER Deliverable D8.1. especially on the German Rasterfahndung: www.detecter.bham.ac.uk/pdfs/D8.1CounterTerrorismDataMining.doc
[8] Robert Alexy, (2002) *Theory of Constitutional Rights*

order to assess the weight of the rights in context,[9] 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.[10]

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 interpretation of its guarantees.[11] 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

[9] 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).
[10] 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.
[11] Pretty v. the UK (Application no. 2346/02), judgment of 29 April 2002, Reports of Judgments and Decisions 2002–III.

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.[12] Neither the right to the protection of private life nor the right to the protection of personal data are so-called absolute rights, i.e. rights that would not be subject to any limitations. For instance in the framework of the EU Charter of Fundamental rights the cumulative conditions for the permissibility of any restrictions is prescribed in Article 52 (1) as follows:
"Any limitation on the exercise of the rights and freedoms recognised by this Charter must be *provided for by law* and *respect the essence of those rights and freedoms*. Subject to the principle of *proportionality*, limitations may be made only if they are *necessary* and *genuinely meet objectives of general interest* recognised by the Union or the need to *protect the rights and freedoms of others*" (emphasis added).

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, the right to the liberty of the person, or the right to non-discrimination. As the assessments were made in relation to the ten different situations identified in the urban security scenario, a consideration of the impact on other fundamental rights beyond privacy and data protection was necessary only in a few cases. The right to non-discrimination was triggered in two situations, the right to the liberty of the person in two situations, and the freedoms of assembly of association on one situation. 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 for an identified fundamental rights intrusion was ¾ representing the best case or the least interference. In no case the maximum score of 16 was the outcome which would represent the worst case or the greatest intrusion. Notably,

[12] See e.g. Case T-194/04 *Bavarian Lager,* judgment of the Court of First Instance of 8 November 2007, paras 118-119.

that maximum score was assigned in some instances under the earlier scenarios (D2.6 and D2.8) but, as said, not in the context of the current urban security scenario. Any score above 10 would represent 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.[13] 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*[14], the ECtHR held that the disclosure to the media for broadcast use of video footage of the applicant whose suicide attempt was caught on closed 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.

[13] See for instance S. and Marper v. The United Kingdom (December 4, 2008), § 102
[14] Peck v. The United Kingdom (January 29, 2003), § 63.

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 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, 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 and the narrative of the scenario did not include references to the role of the judiciary, it could usually not be assessed whether the law would in each case require judicial authorization. Hence, the question of judicial authorization was left open, except in the two cases of deprivation of liberty (arrest), where it was assumed that the law of any EU Member State would secure prompt judicial review of the lawfulness of the arrest. 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' would be 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.[15] 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, in the assessments of the urban security scenario an effort was made to assess separately any 'third-party' or 'collateral' intrusion into the fundamental rights of individuals beyond the intended target. Therefore in several cases there are more than one outcome score, reflecting the different impact upon differently situated individuals. As such third-

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

party intrusion was assessed separately, there was no need to mark cases of significant risk for third party intrusion with an asterisk (*) as was earlier done in D2.6.

**2.3 Discussion of the Matrix**

As with D2.6 and D2.8, the matrix of technology used in D2.9 show a level of agreement between the ethical and legal assessments when it comes to assessing what the least problematic and most problematic technologies are. However, seeming agreement is limited by the fact that the technologies considered in D2.9 are overwhelmingly assessed as either posing moderate or intermediate ethical risks – both D2.6 and D2.8 represented a greater range of degree of 'moral riskiness' of the technology between no risk at all and severe risk.

Two issues need to be born in mind when comparing the fundamental rights and ethical assessments. Firstly the scoring and particularly the colour coding represent simplifications for the sake of providing a clear overview of a number of different uses of technology – more detailed and precise analysis is possible in sections 3.3.2 and 3.3.3, and in Annex 1 listing the Fundamental Rights assessments of each of the 10 technologies in full. Secondly the ethical and fundamental rights risks are all individually important and are non-additive – a technology doesn't 'compensate' for its riskiness in relation to one category by virtue of being very low risk with regard to another. And all risks individually raise a question about whether the technique ought to be used.

The ethics and the fundamental rights analyses both rank the Cybels social media analysis at the highest end of the range for riskiness among the sampled technologies. The ethics colour coding places the Facewatch system for sharing photographs among police and local businesses at an equivalent level, insofar as both systems raise intermediate risks of error, intrusion and damage to trust. The fundamental rights risks identified to privacy and data protection are assessed at '4' and '8' respectively. At least one of the uses of the Unmanned Aerial Vehicle (that directed against 'Wayne') was assessed as posing higher risks to the subject's fundamental right to privacy, scoring an '8' for this category as well as an '8' for the risk to the right to data protection, and '4' for a risk to fundamental rights to assembly and

association as well. The ethical analysis considered the Unmanned Aerial Vehicle to raise intermediate risks of damage to trust and intrusion and only moderate risks of error. At the lower end of the scale, the lowest risk technology by both the ethics and the fundamental rights analysis was the Predpol technology for predicting where crimes are likely to occur. This was considered to raise only low risks of error and damage to trust, and risks to fundamental rights to privacy and non-discrimination of ¾ and 1½ respectively.

There is no similar correlation between either ethics or fundamental rights and technical usability. The best technology from the point of view of usability is the thermal camera, which scores a '7.5', while being assessed as posing moderate ethical risks of error and damage to trust, intermediate risks of intrusion, and risks to fundamental rights to privacy and data protection (ranging between 0-4 and 2-4 respectively). The worst technology from the point of view of usability is the automatic detection of abnormal behaviour, which scores a '2'. This technology was assessed as posing intermediate risks of error and damage to trust, moderate risk of intrusion, and risks to fundamental rights to privacy, data protection and non-discrimination (assessed as '1', '2' and '2' respectively). Any claim that in the use of surveillance technology we always face a trade off between security and privacy (or ethics or human rights) is thus shown to be unsustainable.

## 3. Local Authority Surveillance-Use Scenario.

### 3.1 Introduction

SURVEILLE deliverable D2.9 provides an assessment of the use of surveillance technologies by local authorities in terms of usability and efficiency as well as ethical problems and fundamental rights intrusions. It builds on SURVEILLE deliverables D2.1, D2.3 and D2.7, which reviewed surveillance technologies, and on the matrix and scoring methods developed in D2.6. It provides a third scenario for the use of surveillance technologies: following a serious crime investigation scenario in D2.6 and a terrorism prevention scenario in D2.8, this paper looks at the use of surveillance technologies by local authorities for urban security and public order purposes.

In each case, the scenarios place the use of the technology in a specific context, which is important when considering the questions of efficiency as well as the ethical and fundamental rights challenges that this paper examines. The paper considers how technologies are used today by local authorities for security and public order purposes. It shows how towns and cities use a variety of technologies that can be used for surveillance and security applications. It gives insight into what exactly they are used for, which allows for the assessment of issues of usability and efficiency, as well as moral risk and infringements to fundamental rights.

The scenario is a fictional story aimed at illustrating the use of technologies for safety and security in a modern city – here simply named city X. While the events in the story are fictional, they are based on real world analogies, which are specified in footnotes.[16] This local authorities scenario is developed to underline that the reality of the use of these technologies is not limited to the police and to intelligence and law enforcement agencies.
For the purpose of the matrix of surveillance technologies above, 10 uses of technology are identified for further analysis. Possible applications of the technologies are stipulated in text boxes where uses of technologies against hypothetical subjects of surveillance are described. The uses against these people are then analysed in part 3.3.

[16] This scenario builds on and is an extension to the local authorities' paper for SURVEILLE, deliverable D2.3.

### 3.2 A scenario for the use of surveillance technologies by local authorities - 24 hours in city X.

The urban supervision centre of city X brings together all the available means that monitor, plan and manage security in the city. It is run by the municipality, bringing in all city departments that play a role in security issues, from local police to the cleaning service, but functions in very close cooperation with the national police. Algorithms can **mine the data** for patterns that were not previously revealed.[17] The police force in the city now uses new software that analyses this pool of information to make real-time **predictions** on where and when different types of crime are likely to occur.[18] The predictions are sufficiently detailed so as to facilitate the deployment of police forces.

Arnold, a citizen of the suburb of Wysteria in the city of X, has carried out a number of thefts of car radios over the previous two years in and around Wysteria and has not been caught. The thefts have been reported and are aggregated with similar crimes as data inputted into the PredPol system. The PredPol system predicts a higher likelihood of further car radio thefts in certain streets of Wysteria, and on this basis the decision is taken to deploy additional police to the area to look out for this type of crime. Bill, another citizen, is walking through Wysteria on his way to the city centre and stops when he hears the sound of breaking glass. He turns around and sees a parked car with a broken window. While looking into the car a deployed police officer, sent to the street on the basis of the PredPol data, arrives. The police officer sees Bill with his hand in the window of a car, whilst the car's radio is still in place in the vehicle.

On a Sunday morning, the city is calm, the squares are empty and only a few cars are on the main roads leading to the city centre, which are usually heavily congested. The few people going about their business and the city's cleaning units which appear in the field of vision of one of the **CCTV** cameras are easily detected against this almost static backdrop. However, a large demonstration is planned this Sunday to protest against the latest government

[17] Mayer-Schönberger, Viktor and Kenneth Cukier (2014): *Big Data : La révolution des données est en marche*. Paris. Robert Laffont.

[18] Several big data applications offer predicting scenarios. One of these services is PredPol, which is already used by several cities in California and Kent, UK. http://www.predpol.com/.

reforms. Tens of thousands of people are expected in the city centre, and this will obviously disrupt traffic and pose a threat to public order. In particular, it is feared that groups of extremists and other violent troublemakers might 'crash' the demonstration with the purpose of causing riots. Also, there have been incidents recently in which peaceful demonstrators were attacked and robbed by youth groups or gangs.

In order to obtain a better understanding of what to expect, the Urban Supervision Centre, in cooperation with the police, have also kept an eye on the Internet activities of extremist groups, some of which have indeed called their followers to go *en masse* to the demonstration. **Social media,** such as Twitter, provides important sources of publicly available information, which can be used to predict the development of crowds, and which can also give insights into what is going on within a crowd and how situations are developing.[19] Several companies offer **social media analysis software**.[20]

The Thales Cybels intelligence system continuously analyses the open-source social media postings of a number of individuals known to police as suspected of conspiring to cause disorder on previous occasions – Twitter postings and messages posted in places where they can be seen by anyone logging on to the relevant page. One of these is Celine, who the social networking analysis reveals is in regular contact with David on political topics, including on the subject of today's demonstration. A number of the messages between Celine and David include criticism of police management of this and similar demonstrations. All of these messages to David are flagged up as meriting attention. Today, for the first time, Celine uploads a message to a Facebook group suggesting that a number of people should try to break into the local party offices of the government party whose policies are being protested – this is an open Facebook group, potentially visible to anyone. David is one of ten others agreeing that this is a good idea, but without expressing any specific commitment to participating himself. Extra police are assigned to the route as it passes by the party headquarters. A group of about fifty people, including Celine, David and Emily gather near

[19] Kallus, Nathan (2014): Predicting Crowd Behavior with Big Public Data http://arxiv.org/pdf/1402.2308v1.pdf.
[20] See for example Cisco http://www.cisco.com/c/en/us/products/customer-collaboration/socialminer/index.html
[20] See for example, IBM http://www-03.ibm.com/software/products/fr/social-med'ia-analytics-saas/ or Thales https://www.thalesgroup.com/en/cybersecurity/what-we-do-products-gestion-de-la-securite-reaction-aux-incidents/cybels-intelligence.

the party headquarters. The police ask that they disperse or continue to the official site of the protest: the overwhelming majority of the fifty gathered near party-headquarters remain and the situation evolves into a confrontation with police. Eventually Frank tries to break through the police cordon and, although the protesters fail to get into the party headquarters, there are scuffles between the police and the protesters. All the protesters congregating outside the party headquarters are arrested.

In the Urban Supervision Centre one can observe the situation unfold. The square where the demonstration will start is filling up with people. **Automatic number plate recognition (ANPR)** cameras have been set up in the central part of City X to enforce the 'congestion zone', where non-residents have to pay a special tax. The ANPR system provides exhaustive lists of all the vehicles going through the zone. This information is correlated with information linked to the vehicle and its owner.[21] By now, large crowds have gathered not only in the streets and on the pavements, but also in the public transport system: the subway lines, tramways and buses calling at the demonstration gathering points are packed.

Another citizen, Gary, has his number plate logged and analysed by the ANPR system as he drives into the inner-city area where he lives. Helen, a citizen, is travelling from her home outside the city into the city-centre area to join the protest, and her number plate information is logged and analysed as well; some time later, she is charged the congestion tax. As with all ANPR records gathered in City X, the details of both Gary and Helen's journeys remain stored and accessible to police for a period of two years and are then deleted.

While the USC cannot directly access the **cameras located in the trains, trams and buses**, it can see the crowds from the CCTV cameras installed at the stops. Moreover, thanks to **RFID (radio frequency identification) chips** in transport tickets, they know which public transport lines and stations are registering an unusual number of passengers. This technology is also able to identify individual passengers because the chip includes information about the

[21] ANPR systems are being used in several cities in Europe. The particularity of the London congestion zone or the ANPR system set up in lower Manhattan as part of the domain awareness system is that they systematically monitor all the vehicles entering a given area.

identity of holders of monthly and season tickets (however, this information is currently only made available upon reasoned request).[22]

Ida travels by bus from her home in Wysteria to a coffee shop in West Heath, a suburb on the other side of town, where she meets John. Both then travel on the metro to the demonstration. All of Ida and John's travel is logged and automatically processed by software that provides the command centre with the information about public transport congestion. Ida's travel remains potentially attributable to her as she has used a season ticket registered to her name and address. John buys a new travel card on the day, which he retains for further use.

It is now midday and the central square is full of people. The **CCTV** operators of the urban supervision centre provide the police and other operational partners, such as civil protection, with overview shots of the crowd. The task of the operators has changed now, as they have to monitor a crowd of thousands of people. In addition to providing the overview, they have to identify problems and problematic behaviour. Is there congestion in the crowd? Are there people who show signs of being in need of help? Are there people showing signs of problematic, i.e. violent, behaviour? Are any of those who have recently attacked demonstrators detected in the area? Are any of the known troublemakers present? This task consists in watching individuals and their behaviour and is significantly more difficult than observing an empty space or monitoring an individual who is trespassing. As operators need to concentrate on only one or a few screens to perform their tasks in this new, more complex, situation, they therefore need help to monitor their usual, wider, sector of surveillance.

The CCTV records Kezia, who is walking to the event and stops to greet and talk with a number of friends she happens to meet along the way, some of whom are also going: Leonard, who is seen involved in a number of separate brief, violent scuffles (with Mary, Max and Melissa); and Neil, who closely resembles a 'known trouble-maker' by the name of Niall, who is reported to have taken part in violence and to often carry a knife. Niall has

[22] See for example the RFID based ticket systems in Paris (Pass Navigo) or London (Oyster Card).

previously engaged in fights at protests.

Kezia is watched fleetingly and occasionally by a series of different viewers keeping a general eye on the crowd. Leonard's initial scuffle draws the attention of an operator who watches him until a police officer arrives who has been directed to investigate the incident. The police officer arrests Leonard on suspicion of assault. Neil is watched by a third operator who mistakes him for Niall. The operator sends a policeman to investigate further when he sees 'Niall' congregating with a number of other 'known troublemakers'. The policeman questions Neil and searches him, suspecting he might be carrying a knife. When the search yields nothing Neil is free to go and continues on his journey.

The **CCTV** system of city X has several **smart features** that help them to focus on what is important in the vast amount of footage they receive. The system can, for example, trigger alerts when someone enters specific areas, like a property to which he or she is not allowed access;[23] goes the wrong way down a one-way passage; leaves an object in certain confined spaces; stands for a long time next to a car and might break into it or bends down next to parked trains as if to spray graffiti.[24]

The smart features flag up a number of individuals to the CCTV viewers as requiring attention. First Olivia tries to take a shortcut across the motorway while walking in to the city centre. The smart CCTV flags up her presence on the central reservation (where pedestrians are forbidden). A viewer notes her presence, and alerts a local traffic police officer, but Olivia has moved on by the time she could get there. No further action is taken.
Phillip is walking to the protest past an area with a parked train. He drops his keys, and consequently spends a period of time crouched down next to the train. The smart CCTV flags him up for attention because of the algorithm targeting graffiti. The CCTV viewer thinks he is probably a graffiti vandal and two police officers are sent to question Phillip.

However, **detecting problematic or suspicious behaviour** is another issue. As part of various research projects, experiments have been performed in city X and other European cities

[23] See for example the case of Genoa, Italy, in Efus (2009) *Citizens, Cities and Videosurveillance*.
[24] Such a system is used by the Munich transport authority (see Efus SURVEILLE end-user working group proceedings).

which aim, for example, automatically to detect abnormal behaviour and threats in crowded spaces[25] or to set up intelligent information systems supporting observation, searching and detection for the security of citizens in the urban environment (INDECT project).[26] However, these were still research projects with a testing phase and with no marked-ready solutions. Moreover, on several occasions the public even complained against the testing of these surveillance systems.[27]

The abnormal behaviour detection flags up three people as behaving in a manner of interest for the CCTV operators. Quentin has an argument where he suddenly raises his hand and strikes the person to whom he was speaking. Rebecca and Simon do not engage in wrongful action, but nevertheless separately trigger the alert. Rebecca is walking unusually. It is not clear why the smart CCTV categorises Simon's behaviour as unusual. The behaviour of all three is drawn to the attention of a CCTV operator. She sends an officer to investigate Quentin's violent scuffle. Watching Rebecca's unusual walk she concludes that this is what has led to the categorisation and concludes that no further action is needed. Confused by Simon's triggering of the system she asks an officer to investigate to see for himself if anything is wrong.

The flow of people demonstrating has now swollen over several kilometres and has reached an area of the city where there are not many fixed CCTV cameras. In order to monitor the demonstration in this area, two lamppost climbing mobile cameras have been set up as temporary extensions to the CCTV system.[28] In the context of such a large event, mobile CCTV cameras are an important additional tool. The latest tool of city X is an Unmanned

[25] Automatic Detection of Abnormal Behaviour and Threats in Crowded Spaces "ADABTS" is the title of a EU financed FP7 project. It explored the possibilities for automated operator support and tried to develop methods that can distinguish between 'may be interesting' and 'not interesting' imagery.

[26] Intelligent information system supporting observation, searching and detection for security of citizens in urban environment ("INDECT" is actually the name of an EU financed FP7 project).

[27] Both projects, especially INDECT, which received close to €11 million of EU funding, have been heavily criticised by the public, the media, citizens' rights organisations, data protection agencies and political parties. There have even been demonstrations in Brussels. There were rumours and fears about the system being tested at the 2012 UEFA European Championship and the 2012 Olympics in London.

[28] See the example of London, where these temporary cameras are used. Efus (2009): *Citizens, Cities and Video Surveillance.*

Aerial Vehicle (UAV) or **drone**, which can deliver live footage to the supervision centre.[29] It has been purchased by the municipality in cooperation with the police, who are its main user. It is also used by the fire brigade and for other civil protection purposes.[30] Drones can also be used as a show of force to those being surveyed, while also being so small and silent that they might go unnoticed. This afternoon, the weather is very good but parts of the crowd are more difficult to distinguish because of the shadows projected by buildings.

The drone briefly films Tina, a demonstrator; Ugo, a bystander who was not aware of the demonstration in advance and is walking in the other direction; Vanessa, who has been taking part in violent scuffles; and Wayne, who is sunbathing on his roof-terrace where he assumes he is not visible to view. In most of the footage they are unidentifiable, and none are scrutinised more than fleetingly. All four see and are aware of the drone.

While people can hardly be seen with the naked eye, they clearly appear on the thermal imaging camera. These cameras cannot see through walls, but they can see through a light cover, such as a tent. Thermal imaging cameras can also be used, for example, to see if buildings appear occupied (because they detect heat) or to identify illegal cannabis green-houses.[31]

The thermal camera films Xandra as part of the crowd, though she is not identifiable. In passing it also picks up the form of Yuri, who is inside his home, and has an illegal cannabis greenhouse. Neither sighting is acted upon in the command centre.

Businesses in city X have developed the use of facial recognition software – for business, but also for security purposes. In cooperation with the police, they set up a low-level crime reporting and image sharing system for businesses.[32] Their goal was, firstly, to help the police investigate incidents filmed with their CCTV system. Instead of having to send an

[29] The use of drones in events like this are currently tested (see for example the Efus interview with the president of the French National Commission on CCTV). However, there was debate in the SURVEILLE police end-user panel, if this was good police tactics (see minutes).
[30] As, for example, the fire brigade of Paris: http://lci.tf1.fr/france/societe/2009-06/un-mini-drone-experimente-par-les-pompiers-de-paris-4888941.html.
[31] The municipality of Rotterdam has provided the local police with a drone to spot illegal cannabis greenhouses.
[32] The system described here is the UK service Facewatch http://www.facewatch.co.uk/cms/.

officer to the scene, extract the video and watch hours of footage, the system allows business owners to directly upload relevant footage to the police and simultaneously to file a complaint. The police can then start their investigation directly. Their second goal was to create a watch list, which can alert security agents of other businesses, about persons who have committed a crime in another business.

Zara has carried out a number of wallet thefts in city centre shops, and has nearly been caught on a number of occasions, but there has not been sufficient evidence to press charges. Annwen, a business owner, has seen Zara in the area on a number of occasions when a wallet has been pickpocketed on her premises. Today a store security-guard tries to stop Zara to search her after a pickpocketing takes place, and Zara runs off. Annwen uploads Zara's image to the Facewatch system taken on the shop's CCTV.

Brendan is another business owner. He has recently had an argument with Ciara. Brendan maliciously uploads a photograph of Ciara in the hope of causing her inconvenience.
Both Zara and Ciara are spotted by shop-owners making use of the system which identifies them as troublemakers and who consequently subject them to additional scrutiny while they are there.

### 3.3 Stage-by-stage ethical, legal and technological assessment.

#### §3.3.1. Technical Analysis

| | | EFFICIENCY | | | COST | | | PRIVACY B-D | | | EX. |
|---|---|---|---|---|---|---|---|---|---|---|---|
| TECHNOLOGY AND USE | SCORE | #1 Delivery | #2 Context | #3 Sensitivity | #4 Initial cost | #5 Personnel | #6 Additional | #7 Data collection | #8 Access & use | #9 Protection | #10 Excellence |
| PredPol and car radio thefts | 5.5 | 0 | 1 | 0 | 1 | 1 | 0.5 | 1 | 0.5 | 0.5 | 0 |
| Thales Cybels intelligence system | 6 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0.5 | 0.5 | 0 |
| ANPR | 6.5 | 1 | 1 | 1 | 0 | 0.5 | 0 | 1 | 0.5 | 0.5 | 1 |
| RFID in transport tickets | 6 | 0.5 | 0.5 | 1 | 0 | 1 | 0 | 0.5 | 1 | 1 | 0.5 |
| CCTV for crowds | 3 | 0.5 | 0 | 0 | 0 | 0.5 | 0.5 | 0 | 0.5 | 0.5 | 0.5 |
| Smart CCTV | 7 | 1 | 1 | 1 | 0 | 0.5 | 0.5 | 1 | 0.5 | 0.5 | 1 |
| Smart CCTV detecting abnormal behaviour in crowds | 2 | 0 | 0 | 0 | 0 | 0.5 | 0 | 0.5 | 0.5 | 0.5 | 0 |
| UAV | 5 | 1 | 0 | 0.5 | 1 | 0 | 0.5 | 0.5 | 0.5 | 1 | 0 |
| Thermal camera on UAV | 7.5 | 1 | 0.5 | 0.5 | 0.5 | 1 | 1 | 0.5 | 0.5 | 1 | 1 |
| Facewatch | 3.5 | 0 | 0.5 | 0 | 1 | 1 | 0.5 | 0.5 | 0 | 0 | 0 |

The technologies in this scenario are scored based on the most recent version of scoring as presented in D3.8. Following D3.8 there was further discussion regarding the scoring of the Privacy-by-design (PbD) category. D3.3b had given a very detailed look and scoring for PbD. Ultimately, though, it was determined to be too complex to incorporate into the usability scoring. The usability scoring table is presented below to remind the reader how the scores are divided.

Several of the technologies in this scenario, namely, those related to cameras – are very similar to one another. Consequently, we have analyzed them consecutively, beginning with the basic CCTV camera and moving on to different smart cameras and then to the UAV that carries a camera. The order in which the technologies are analyzed and scored, therefore, varies slightly from the order in which they appear in the scenario.

One characteristic of this scenario is that several of the technologies used are new, meaning they are unproven and certain information about them is lacking. This automatically results in a lower score.

*Table 4: Usability scoring – second revision*

| Factor | Attribute | Sub-category | Sub-category yes/ no | Score |
|---|---|---|---|---|
| **Effectiveness** | | | | 0-3 |
| | Delivery | | | 0-1 |
| | Context | | | 0-1 |
| | Sensitivity | | | 0-1 |
| | | | | |
| **Cost** | | | | 0-3 |
| | Initial cost | | | 0-1 |
| | | Purchase price | y/n | |
| | | Installation cost | y/n | |
| | | Space requirement cost | y/n | |
| | Personnel requirements | | | 0-1 |
| | | Number of personnel | y/n | |
| | | Training required | y/n | |
| | | External partners | y/n | |
| | Additional running costs | | | 0-1 |
| | | Maintenance & sustainability | y/n | |
| | | False-positive rate | y/n | |
| | | Other (power, transport, etc.) | y/n | |
| | | | | |
| **Privacy-by-design** | | | | 0-3 |
| | Data collection | | | 0-1 |
| | | Selective | y/n | |
| | | Minimized | y/n | |
| | | Overt or covert | y/n | |
| | Data access & use | | | 0-1 |
| | | Who has access | y/n | |
| | | Clear regulations | y/n | |
| | | Protection against function creep | y/n | |
| | Data protection | | | 0-1 |
| | | Encryption or otherwise access protected | y/n | |
| | | Protected against manipulation | y/n | |
| | | Secure against theft | y/n | |
| | | | | |
| **Proven technology** | | | | 0-1 |

*Each attribute scores 0, 0.5, or 1. If only one sub-category scores 'y,' the attribute scores 0. If two sub-categories score 'y,' the attribute scores 0.5. And if all three sub-categories score 'y,' the attribute scores 1.*

## PredPol

PredPol is a software that predicts "the places and times that future crimes are most likely to occur." Using historical data together with earthquake after-shocks models, it processes

crime data to "assign probabilities of future crime events to regions of space and time."[33] It is, in effect, a risk analysis method. PredPol generates crime predictions on maps in boxes of 500 by 500 feet and updates them several times a day. It is run on a cloud-based software system. According to the PredPol website no personal data of any kind is used in making predictions. Based on the type of crime, the place of crime, and the time of crime, the algorithms predict various kinds of crime.

ATTRIBUTE #1 (EFFECTIVENESS): DELIVERY

"Delivery" refers to whether or not the equipment yields a useful outcome when used correctly. When there is evidence of prior successes or success is reasonably achievable this attribute scores 1; when there is evidence of some success it scores 0.5; otherwise it scores 0.

While there are some anecdotal success stories – testimonials from a few U.S. police departments – PredPol is new technology and does not yet have evidence of success. It scores 0.

ATTRIBUTE #2 (EFFECTIVENESS): CONTEXT

"Context" relates to the conditions of employment. Is the equipment being used in the context for which it was designed and in which it performs well? Or are the conditions such that it cannot perform optimally – i.e. weather inhibits its performance; it is being deployed in a context for which it was not originally intended or which challenges its functionality (e.g. a sound recording bug on a public transport bus is a poor context as it is designed for recording conversation among a few people, not multiple conversations at once with significant background noise).

The context in which PredPol is used in this scenario matches the what, where, and how of its intended design. It scores 1.

[33] http://www.predpol.com

ATTRIBUTE #3 (EFFECTIVENESS): SENSITIVITY

"Sensitivity" relates to the likelihood of error – information is open to interpretation or vague data enables wrong conclusions. It is certainly possible that PredPol could make errors in its prediction of where crime will occur. It scores 0 for sensitivity.

ATTRIBUTE #4 (COST): INITIAL COST

The initial cost is based on the purchase price, the installation cost and the space requirement cost.

According to the PredPol website there is an annual subscription cost based on the population the police department serves. A former crime analyst who has used PredPol stated that it costs about the cost of a crime analyst or less, regardless of the size of the police force.[34] These are low costs so it scores 1.

ATTRIBUTE #5 (COST): PERSONNEL REQUIREMENTS

"Personnel requirements" refers to the number of personnel and training required and any external partners necessary.

There are no additional personnel requirements and training to use the program is minimal. It scores 1.

ATTRIBUTE #6 (COST): ADDITIONAL RUNNING COSTS

"Additional running costs" refers to maintenance and sustainability, false-positive rate, and other (such as power, transport, insurance, etc.).

A possible additional running cost could be false-positives. False-positives would result in the misallocation of resources. The purpose of PredPol is to signal areas where crime is most likely to occur. The idea is that the mere presence of the officer will deter crime from occurring. Once on the scene the police officer still must make his own judgments. Therefore, one could argue that without the use of PredPol there could still easily be a misallocation of resources, with police deployed to areas not needing patrol. Thus, the misallocation of resources with PredPol is no worse than without. Because of this possibility

[34] https://www.youtube.com/watch?v=8uKor0nfsdQ

and yet the uncertainty of whether the false-positive rate would rise or not, the technology scores 0.5 for this attribute.

ATTRIBUTE #7 (PbD): DATA COLLECTION

“Data collection” refers to whether the collection of data is selective (i.e. only the subject is affected), if the collected data about the subject is minimized (i.e. only the data of interest is collected), and if the collection is done overtly or covertly.

The data collected by PredPol is not personal data and it is done overtly. It scores 1.

ATTRIBUTE #8 (PbD): DATA ACCESS & USE

“Data access and use” refers to who has access to the data, if there are clear regulations regarding who has access within an organization, and protection against function creep.

The PredPol facilities where the data is stored are access controlled. On the user side, only police officers have access to PredPol data. It is unknown whether PredPol has protections against function creep. It scores 0.5.

ATTRIBUTE #9 (PbD): DATA PROTECTION

“Data protection” is whether the collected data is encrypted or otherwise access protected, if it is protected against manipulation, and if the collection device is secure against data theft.

Access to PredPol’s data processing facilities is protected. It is unknown whether the data is protected against manipulation. PredPol does not have a collection device, making this point irrelevant. It scores 0.5 for data protection.

ATTRIBUTE #10: EXCELLENCE

“Excellence” refers to whether the excellence of the technology is proven beyond a shadow of a doubt. Although there are success stories of PredPol being used in several police departments in the U.S., the evidence is very limited. It has not yet proven its excellence beyond a shadow of a doubt. It scores 0.

**Thales CYBELS intelligence system**

According to the Thales website, CYBELS intelligence is an application that "provides the ability to analyse information from social media websites… by dynamically combining analysis of the content of conversations with detection and analysis of social communities."[35] It was developed particularly to prevent and anticipate cyber attacks. It follows and synthesizes discussions about threats and studies the behavioral and relational aspects of the hacker communities. It probably uses machine learning to recognize tagged words.

ATTRIBUTE #1 (EFFECTIVENESS): DELIVERY

Social media analysis is now a quite common tool for businesses to determine customer sentiment and thereby improve their marketing and business. They use it to follow what's being said about them, what kind of sentiment – positive, negative, neutral – is being expressed, across what demographics, etc.

Since social media websites are publically available, gathering data from them should not be difficult. Given that social media analytics is widely used in the business realm, it is assumed that it can successfully collect information and make relations between users. It is likely that CYBELS can analyze the publically available information and provide information on what subjects are saying and how they are related to one another. Therefore it scores 1 for delivery.

ATTRIBUTE #2 (EFFECTIVENESS): CONTEXT

CYBELS intelligence is employed in this scenario to analyze social media postings for signs of conspiring to create disorder during the demonstration. Used in this context and for this purpose, the technology functions well. It scores 1.

ATTRIBUTE #3 (EFFECTIVENESS): SENSITIVITY

One of social media analytics main functions is to monitor and analyze conversations. Conversations by nature can be interpreted differently by different people; even more so,

[35] https://www.thalesgroup.com/en/cybersecurity/cybels-intelligence

conversations that are written and that are in shorthand form. CYBELS scores 0 for sensitivity.

ATTRIBUTE #4 (COST): INITIAL COST

As CYBELS is a software application the initial cost would not be considerable. There would be no installation cost and no space requirement cost. It scores 1 for initial cost.

ATTRIBUTE #5 (COST): PERSONNEL REQUIREMENTS

The number of personnel and the training required to run such a software would both be reasonably low. During an event such as the demonstration probably no more than two personnel would be required, and their training would be typical to learning any new software. No external partners would be needed. It scores 1.

ATTRIBUTE #6 (COST): ADDITIONAL RUNNING COSTS

There would be no maintenance required, although there would presumably be software updates. We would assume, however, that as with most software updates, they would be free, and that if a new version eventually had to be purchased, it would be reasonably low for an existing customer.

It is certainly possible that CYBELS intelligence could yield false-positives. In this scenario that would mean incorrectly identifying someone or a conversation as being part of the disruptive community. The costs in this context would be minimal. At most it would cost the analyst some unnecessary time and/ or a few extra police officers deployed to the area of the party headquarters in question.

There would be no “other” costs involved. The category as a whole scores 1.

ATTRIBUTE #7 (PbD): DATA COLLECTION

There is some selectivity of data collected in that the technology is looking for certain kinds of discussions and relationships. However, there will inevitably be data collected from persons who are non-subjects. It is unknown whether the collected data is minimized. The collection is done covertly. The technology scores 0.

ATTRIBUTE #8 (PbD): DATA ACCESS & USE

It is unclear who exactly has access to the data, but it is clear that the technology is intended for the police and intelligence community. It is reasonable to assume that only members of this community, and perhaps those of first responders would have access to the data. It is unknown if there is regulation concerning who is allowed access under which circumstances or if there is protection against function creep. The technology scores 0.5.

ATTRIBUTE #9 (PbD): DATA PROTECTION

It is presumed that the data is access protected. Whether the data is protected against manipulation is unknown. The collection device is presumably in a secured building and therefore secure against theft. It scores 0.5.

ATTRIBUTE #10: EXCELLENCE

Social analytics is a somewhat new technology, particularly to the field of law enforcement. It appears to be widely used and somewhat proven in business. However, since it is not yet proven in law enforcement it scores 0.

**Radio Frequency Identification (RFID)**

Radio Frequency Identification (RFID) uses radio waves to automatically identify people or objects. RFID used in transportation tickets consists of a microchip with an antenna, a serial number and a limited amount of transaction data such as the money left on the card and the last 10 transactions. Via the antenna the chip transmits the identification number and transaction data to a reader using radio waves. The financial transaction is made between the reader and the card but feedback to a central computer is performed in batches, not real time.

ATTRIBUTE #1 (EFFECTIVENESS): DELIVERY

RFID in transportation tickets are unique to each ticket and therefore identify how many people are purchasing tickets and between which locations they are traveling. In the case of

season tickets it can also identify the ticket holders. Obtaining this information can yield the useful outcome of knowing which stations and routes experience high traffic volumes at which times, allowing the transportation company to run additional or longer trains. In the case of season tickets it could be useful in recovering a lost or stolen monthly pass. It is unclear in the present scenario, however, what this information would be used for. Since the data is not available in real-time the travel pattern of individuals can only be accessed after some time. In addition, information on season ticket holders is only made available upon reasonable request, which means it can only be used in ex-post investigations. RFID's usefulness for security purposes is limited. It scores 0.5.

ATTRIBUTE #2 (EFFECTIVENESS): CONTEXT

Although RFID in transportation tickets is a context in which the technology can be and is used, its best purpose in transportation tickets is to identify patterns of travel over a period of time. It is unclear what the purpose of RFID is in this scenario and whether using RFID for security purposes is an appropriate context for this technology. It scores 0.5.

ATTRIBUTE #3 (EFFECTIVENESS): SENSITIVITY

Since each chip has its own serial number there is no room for error or misinterpretation. RFID scores 1 for sensitivity.

ATTRIBUTE #4 (COST): INITIAL COST

The initial cost for installing RFID can be considerable. An RFID reader costs $1,000 or more. The read range for passive tags is only 20 feet, so installing a reader at each entrance/ exit is necessary.[36] Installing several readers at each station for various exits and entrances would typically be necessary. In the case of, for example, the Paris metro with over 300 stations this would mean a minimum of $600,000 if we assume that every station has at least 2 entrances/ exits. In many cases there are more than two entrances or exits so the initial cost would in reality be much higher. RFID scores 0 for initial cost.

ATTRIBUTE #5 (COST): PERSONNEL REQUIREMENTS

[36] http://www.rfidjournal.com/site/faqs

There does not appear to be additional personnel requirements for the use of RFID in this scenario. It scores 1.

ATTRIBUTE #6 (COST): ADDITIONAL RUNNING COSTS

In addition to maintaining the equipment, RFID has the running cost of the tags (the chip plus the antenna) in the product item, in this case, the transportation tickets. Day tickets use passive tags (it is unclear whether season tickets use passive or active tags, but it is likely that they also use passive tags). A passive tag cost 20-50 cents per tag. The RFID Journal states that this "makes them impractical for identifying millions of items that cost only a few dollars."[37] This would seem to indicate that using them for individual use tickets is a costly and impractical use of this technology. RFID in transportation tickets therefore scores 0.

ATTRIBUTE #7 (PbD): DATA COLLECTION

RFID collects data every time a person travels on public transport. On the one hand this is a specific scenario – travel – on the other hand every time a person travels the data is collected. In the context of security, this is not very selective, since everyone's travel data is collected. In the case of single journey tickets the data is minimized, as it is not associated with a person. In the case of season tickets it is not minimized. The collection is overt, although not all people may be aware that their ticket contains an RFID chip. It scores 0.5.

ATTRIBUTE #8 (PbD): DATA ACCESS & USE

Access to personal data is only allowed via court order. It scores 1.

ATTRIBUTE #9 (PbD): DATA PROTECTION

It is assumed that access to the central processing system is access protected, and since there are laws governing access to the data that it is protected against manipulation. The data is sent to the central processing center so there is no risk of theft from the collection device. It scores 1.

[37] Ibid.

ATTRIBUTE #10: EXCELLENCE

RFID is a proven technology that has existed since the 1970s. It uniquely identifies each product item and can have great advantages in closed-loop systems in which the item stays within a company's control. The use of RFID in transportation tickets, however, is a new application of this technology and its excellence in this domain is not yet proven. It scores 0.5 for this attribute.

**CCTV**

ATTRIBUTE #1 (EFFECTIVENESS): DELIVERY

CCTV is arguably one of the most controversial technologies when it comes to measuring success. There have been numerous studies done by various parties yielding results from opposite ends of the spectrum.[38] One of the reasons it is difficult to measure success is that upon installation of the camera its purpose is not stated (or is too large and vague to be realistically measured), it is given multiple purposes, or the purpose changes after it is installed (e.g. it was installed with the purpose of "deterring crime," but is then used to gather evidence for criminal cases).

There certainly are numerous cases of prior successes of CCTV use – footage used to successfully prosecute offenders in court, drops in car theft rates in car parks, etc.). There are also studies, however, that show that the installation of CCTV had absolutely no effect on crime rates in an area. The success varies widely depending on the intended purpose, the context of deployment, the area, etc. Therefore, CCTV scores 0.5.

ATTRIBUTE #2 (EFFECTIVENESS): CONTEXT

In this scenario in City X the CCTV is being used to monitor crowds of thousands of people. CCTV has potentially many uses, thus monitoring crowds for signs of disturbance can be one of them. However, the scenario states that the task of the CCTV operators has changed. It does not state what their previous or original task was, but presumably it is to monitor the

[38] According to discussions during a SURVEILLE meeting (25-26 March 2014) one possible explanation for these widely varying results is that all the studies performed in the UK have been funded by some interested party, and therefore have not been completely objective. See, also, SURVEILLE deliverable D4.6.

CCTV cameras which are filming small numbers of people rather than a crowd of thousands. Thus the system is being used in a context for which it was not originally intended. Further, using CCTV cameras for multiple purposes at the same time (identifying crowd congestion, problematic behavior, individuals in need of help), including identifying individual people, is not a context in which it can operate optimally and poses significant challenges to the system. CCTV scores 0 for context in this scenario.

ATTRIBUTE #3 (EFFECTIVENESS): SENSITIVITY

There is a high likelihood of error and misinterpretation in determining what is happening in the crowd and in misidentifying individuals. CCTV scores 0.

ATTRIBUTE #4 (COST): INITIAL COST

The initial cost of setting up a CCTV system can vary widely depending on the type of system and the number of cameras installed. In a report by Martin Gill evaluating fourteen different CCTV schemes in the UK,[39] the set-up cost per camera ranged from about £7,000 to nearly £34,000.[40] The minimum number of cameras installed was five and in this particular system the cost was £10,704 per camera, bringing the total above £50,000. While the cost varies widely, even with the less expensive systems the cost is considerable. Only in the case of installing a couple of cameras would the cost be less, and we assume that a municipality or police force would be installing more than this. CCTV scores 0 for initial cost.

ATTRIBUTE #5 (COST): PERSONNEL REQUIREMENTS

Based on the above-cited study, personnel requirements range from £53 to £116,215.[41] This very high cost, however, is exceptional, with all the other systems costing well below £50,000. CCTV, therefore, scores 0.5 for personnel requirements.

[39] Martin Gill and Angela Spriggs, "Assessing the impact of CCTV," Home Office Research, Development and Statistics Directorate, Feb. 2005.

[40] The set-up cost in this report includes figures, such as transport and advertising, not included in the "initial cost" category of our scoring system. However, these figures are not judged to significantly affect the overall set-up cost, as the highest figure by far is the equipment cost.

[41] These are ongoing personnel costs. Costs for set-up are included in the initial cost category.

ATTRIBUTE #6 (COST): ADDITIONAL RUNNING COSTS

The additional running costs are difficult to calculate based on the above-mentioned study, as the ongoing costs in the study include personnel costs. However, a rough estimation puts the costs at a range of £587 to £1021 per camera per year. Whether these are considered to be high costs or not depends on whether they are viewed per camera or per system. Per camera, these costs are not high; however 646 cameras at £587 each (as is the case for one of the systems studies) gives a considerable annual cost of £379,202. As it is impossible to evaluate on a system basis, since each scenario would involve a different number of cameras, we will consider them on a per camera basis. Based on this, CCTV would score 1 for additional running costs. However, the false-positive rate of CCTV used in monitoring a crowd would likely be high, bringing the score down to 0.5.

ATTRIBUTE #7 (PbD): DATA COLLECTION

The data being collected is of a whole crowd of people, not certain subjects. The whole crowd is being constantly monitored so more than just the data of interest is collected. The surveillance is overt. Because the technology only scores positively on one out of three criteria, it scores 0 as a whole for this category.

ATTRIBUTE #8 (PbD): DATA ACCESS & USE

Typically, data collected by CCTV systems is only available to a team of operators. Regulations regarding what the operators are allowed to do with the collected data exist and are required by law in most EU member states. There is, however, no protection against function creep. It scores 0.5.

ATTRIBUTE #9 (PbD): DATA PROTECTION

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

As the data is stored not on the collection device but at a remote surveillance centre, there is no risk of data extraction from the collection devices. CCTV scores 0.5 for data protection.

ATTRIBUTE #10: EXCELLENCE

CCTV has proven its excellence in that in many scenarios and contexts. Whether it has proven its success in monitoring crowds, however, is more questionable. It scores 0.5.

**Smart CCTV**

Smart CCTV is a technology that is programmed to recognize certain kinds of behavior and flag this behavior. The CCTV operator can then investigate the situation. This is a relatively basic form of smart CCTV motion detection. It works well in not-so crowded areas.

ATTRIBUTE #1 (EFFECTIVENESS): DELIVERY

Smart CCTV works well in areas with few people. It can easily detect intruders in areas where pedestrians are not allowed, such as on the highway or railway. It scores 1.

ATTRIBUTE #2 (EFFECTIVENESS): CONTEXT

In this scenario the smart CCTV is used in the context in which it was intended – that is, to flag a person's presence in a non-pedestrian zone and to alert lingering activity next to a train. It scores 1.

ATTRIBUTE #3 (EFFECTIVENESS): SENSITIVITY

Smart CCTV is programmed to flag certain kinds of activity. It does this well, with small likelihood of error. It is, of course, possible that that particular activity in a given instance is not errant, such as in the scenario of Philip looking for his keys next to the train. The system, however, is flagging that someone is lingering next to the train, which is, in fact, the case. To determine if this is suspicious activity requires further follow-up of someone investigating. The technology scores 1.

ATTRIBUTE #4 (COST): INITIAL COST

Smart CCTV has additional features to detect certain kinds of behavior, making it more expensive than a non-smart CCTV system. It scores 0 for initial cost.

ATTRIBUTE #5 (COST): PERSONNEL REQUIREMENTS

It is assumed that personnel requirements would be no different than that for a non-smart camera (see Attribute #5 under CCTV). It scores 0.5.

ATTRIBUTE #6 (COST): ADDITIONAL RUNNING COSTS

The maintenance costs are expected to be higher than for regular CCTV, since the system itself is more expensive. The maintenance costs for ANPR, a type of smart CCTV, are considerable (see below under the ANPR section). It is assumed that other kinds of smart CCTV systems would have similar costs. The false-positive rate would be similar to that of CCTV monitoring a crowd. Therefore, it scores 0.

ATTRIBUTE #7 (PbD): DATA COLLECTION

The collection of data is selective and minimized – only the subject is filmed and only when performing a certain action. The collection is overt. It scores 1.

ATTRIBUTE #8 (PbD): DATA ACCESS & USE

As with regular CCTV, the data collected by smart CCTV systems is only available to a team of operators and regulations exist regarding what operators are allowed to do with the collected data. There is no protection against function creep built into the technology. It scores 0.5.

ATTRIBUTE #9 (PbD): DATA PROTECTION

Smart CCTV is the same as regular CCTV with regard to data protection – the data is protected by access control, lack of protection against internal manipulation is assumed, and there is no risk of data theft from collection devices. It scores 0.5.

ATTRIBUTE #10: EXCELLENCE

Smart CCTV has proven its excellence. It scores 1.

**Automatic Number Plate Recognition (ANPR)**

ANPR is a type of smart CCTV technology.

ATTRIBUTE #1 (EFFECTIVENESS): DELIVERY

When ANPR is used correctly it captures the license plate numbers of passing vehicles and matches them with the vehicle owner's name and other vehicle information in an associated database. ANPR is known to be successful in recording vehicles' number plates for a variety of purposes such as locating stolen vehicles and identifying uninsured vehicles.[42] It is also successfully used in charging congestion tax as in this scenario. The technology scores 1.

ATTRIBUTE #2 (EFFECTIVENESS): CONTEXT

The purpose of the ANPR system in City X is to enforce the congestion zone tax. Although there is a demonstration going on in this scenario, the ANPR is still being used in the context of charging the congestion tax. It scores 1.

ATTRIBUTE #3 (EFFECTIVENESS): SENSITIVITY

Reading a number plate is quite straightforward and ANPR systems have developed significantly since their inception in the 1970s, always with improving accuracy. There is no need for interpretation in using ANPR. It scores 1.

ATTRIBUTE #4 (COST): INITIAL COST

The initial cost of implementing an ANPR system is expensive. In 2005 the Gloucestershire Constabulary was provided funds of £200,000 to implement an ANPR system around Gloucester. The proposal included the installation of 15 fixed cameras, routing an additional four CCTV cameras through the ANPR reader, and having a full time police ANPR intercept team.[43] It is not clear if these costs include the salaries of the intercept team, but the intercept team appears to consist of members already in the police force, not new hires. The

[42] http://www.police.uk/information-and-advice/automatic-number-plate-recognition/
[43] http://democracy.gloucester.gov.uk/committee/documents/s280/pt16115d-anpr.pdf

cost could be less if existing cameras are routed through the ANPR reader rather than new cameras being installed, however, there would still be the need to set up the system, including a central processing computer. ANPR scores 0 for initial cost.

ATTRIBUTE #5 (COST): PERSONNEL REQUIREMENTS

Training required for ANPR would be minimal as the system itself does most of the work. Whether or not additional personnel would be required depends on the individual police department or municipality and the extent to which they use ANPR. In the above case of Gloucester, ANPR was heavily implemented and required the hiring of an additional CCTV operator with an annual salary of £26,000. Due to this variation in personnel requirements, the technology scores 0.5.

ATTRIBUTE #6 (COST): ADDITIONAL RUNNING COSTS

The additional running costs of an ANPR system are considerable. Gloucester estimated a cost of £1,070 per camera per year (except the first year in which the cost was £770) plus £20,000 for the maintenance of the ANPR operating system at the control room.[44] There is also a cost of false-positive rate, which would probably not be high, but probably does exist. ANPR scores 0 for additional running costs.

ATTRIBUTE #7 (PbD): DATA COLLECTION

The collection of data is selective and minimized – only the license plate is detected and captured. The collection is overt. It scores 1.

ATTRIBUTE #8 (PbD): DATA ACCESS & USE

As with regular CCTV, the data collected by smart CCTV systems is only available to a team of operators and regulations exist regarding what operators are allowed to do with the collected data. As with other CCTV cameras, there is no protection against function creep. It scores 0.5.

[44] Ibid.

ATTRIBUTE #9 (PbD): DATA PROTECTION

ANPR scores the same as other kinds of smart CCTV for data protection – the data is protected by access control, lack of protection against internal manipulation is assumed, and there is no risk of data theft from collection devices. It scores 0.5.

ATTRIBUTE #10: EXCELLENCE

ANPR has proven its ability to record and analyze the number plates of passing vehicles and subsequently aid police forces and municipalities in identifying stolen vehicles, charging congestion tax, etc. It scores 1.

**Smart CCTV detecting problematic behaviour in crowds**

This is not actually a different technology than smart CCTV. The only difference is that it is flagging certain kinds of behaviour in crowds as opposed to the behaviour of individuals. This combines the difficulties of using CCTV on crowds and smart CCTV automatically detecting specific types of behaviour. The scores, therefore, are the same or worse as those for smart CCTV.

ATTRIBUTE #1 (EFFECTIVENESS): DELIVERY

Above it is stated that smart CCTV works well in areas with few people. This scenario is the exact opposite of that. Further, the scenario states that using smart CCTV in this way is still in the research phase. There is no evidence of success in smart CCTV detecting problematic behaviour in crowds. It scores 0.

ATTRIBUTE #2 (EFFECTIVENESS): CONTEXT

In this scenario the smart CCTV is used in the context in which it was intended – that is, to detect abnormal behaviour in crowds. However, this is experimental technology and it is not yet clear that this is a context in which smart CCTV can perform optimally, it scores 0.

ATTRIBUTE #3 (EFFECTIVENESS): SENSITIVITY

It seems probable that there would be a high likelihood of error and misinterpretation in attempting to detect problematic behaviour in crowds. It scores 0.

ATTRIBUTE #4 (COST): INITIAL COST

Smart CCTV has additional features to detect certain kinds of behaviour, making it more expensive than a non-smart CCTV system. It scores 0 for initial cost.

ATTRIBUTE #5 (COST): PERSONNEL REQUIREMENTS

It is assumed that personnel requirements would be no different than that for a non-smart camera (see Attribute #5 under CCTV). It scores 0.5.

ATTRIBUTE #6 (COST): ADDITIONAL RUNNING COSTS

As with other types of smart CCTV, the maintenance costs are expected to be higher than for regular CCTV, since the system itself is more expensive. The false-positive rate would be higher than regular CCTV or other smart CCTV systems. Many kinds of behaviour would be flagged, that were perhaps unusual, but not problematic. It scores 0.

ATTRIBUTE #7 (PbD): DATA COLLECTION

The collection of data is somewhat selective and minimized in that the system is triggered only when certain kinds of activity are detected. However, the camera is pointed at a crowd and will therefore collect data on non-subjects. The collection is overt. It scores 0.5.

ATTRIBUTE #8 (PbD): DATA ACCESS & USE

As with regular CCTV, the data collected by smart CCTV systems is only available to a team of operators and regulations exist regarding what operators are allowed to do with the collected data. There is no protection against function creep. It scores 0.5.

ATTRIBUTE #9 (PbD): DATA PROTECTION

This kind of smart CCTV scores the same as others for data protection – the data is protected by access control, lack of protection against internal manipulation is assumed, and there is no risk of data theft from collection devices. It scores 0.5.

ATTRIBUTE #10: EXCELLENCE

This technology has no proven excellence. It scores 0.

**Unmanned Aerial Vehicle (UAV)**

ATTRIBUTE #1 (EFFECTIVENESS): DELIVERY

Unmanned Aerial Vehicles (UAVs) or drones can yield a useful outcome. Typically they are outfitted with a camera and their purpose is to observe. In a civilian context this is usually their sole purpose. In a military context they can also be armed. Having a high vantage point they can transmit useful information about an event, in this case, the demonstration, to officers on the ground. At the same time they allow personnel to remain available on the ground and can maneuver to a closer proximity than, for example, a helicopter. They score 1.

ATTRIBUTE #2 (EFFECTIVENESS): CONTEXT

In this context a UAV is essentially a CCTV camera in the sky. The scenario is not clear what the purpose of using the UAV for the demonstration is. If it is to monitor crowd movement, this would be a context in which it would perform well. If it is to identify individuals, it would perform poorly, as it is nearly impossible to do so since the camera is pointed at the top of people's heads. As a whole, the SURVEILLE End User Panel found the use of UAVs in this context to be debatable. It scores 0.

ATTRIBUTE #3 (EFFECTIVENESS): SENSITIVITY

Depending on the distance of the drone from an object or person and the purpose of its use, the possibility of misinterpretation may or may not be more likely. For example, if the purpose is to identify mass movements of the demonstration crowd in one direction or another, misinterpretation is less likely. However, if the purpose is to identify possible instances of trouble or fighting among crowd members, the possibility of misinterpretation is higher. And if the purpose is to identify certain persons the possibility of error is even higher. Because of this wide range of sensitivity possibilities UAVs score 0.5 for this attribute.

ATTRIBUTE #4 (COST): INITIAL COST

The purchase price of a UAV for police or municipality purposes is considerably lower than for military purposes. The UAVs are smaller, which contributes to this lower cost. The Dutch UAV system costs 4,000€. This is a low cost. It scores 1.

ATTRIBUTE #5 (COST): PERSONNEL REQUIREMENTS

The additional personnel requirements are considerable as it is necessary to hire pilots to operate the UAVs.

ATTRIBUTE #6 (COST): ADDITIONAL RUNNING COSTS

There would certainly be maintenance costs, but as the initial cost of the UAV is not terribly high, the maintenance costs would be estimated to be reasonable. False-positives are possible, but again this depends on how the UAV is being used. It scores 0.5.

ATTRIBUTE #7 (PbD): DATA COLLECTION

UAVs are only deployed when special events occur. This makes the collection of data selective. However, as the system is flying and mobile it is nearly impossible to avoid filming private areas. Minimization is achieved due to the fact that the UAV has a top-down view of people and therefore not a good view of faces. Collection is done overtly, although at times the UAV could be difficult to spot, such as when it is quite high or in the near dark. It scores 0.5.

ATTRIBUTE #8 (PbD): DATA ACCESS & USE

A UAV with a camera is very similar to a conventional CCTV system. The data collected by typical systems is only available for a team of operators and in special cases, for law enforcement. Regulations what the operators are allowed to do with the collected data exist and are required by law in most member states of the EU. Nonetheless no technical measures protect against function creep, that is protect against an operator using the system to inappropriately look at people rather than monitoring the area for crime. It scores 0.5.

ATTRIBUTE #9 (PbD): DATA PROTECTION

Technical measures exist to protect the data transmitted from the UAV to the ground system from unauthorized access. Access control and protection from manipulation are also in place at the operation center. As the UAV is airborne, theft of internal storage is of no concern. It scores 1.

ATTRIBUTE #10: EXCELLENCE

UAVs have proven their excellence in the military realm. They are relatively new, however, in use by police forces. Their excellence is not yet proven. The technology scores 0.

**Thermal camera**

Thermal cameras detect heat sources such as people, animals, and cars, but they cannot be used for the identification of individuals.

ATTRIBUTE #1 (EFFECTIVENESS): DELIVERY

Thermal cameras yield a useful outcome and there is strong evidence of their success in detecting sources of heat. The technology scores 1.

ATTRIBUTE #2 (EFFECTIVENESS): CONTEXT

The thermal camera in this scenario is mounted on the UAV and is being used at night; it detects people and an illegal cannabis greenhouse. This is what the equipment is designed to do. The scenario, however, does not indicate what the purpose of using the thermal camera is. Is it being used to detect flows of people or to signal the presence of a person in a certain area? Is the goal to identify individuals or to signal problems in the crowd? In some of these contexts the thermal camera would not function well. Because the purpose is not stated, it is difficult to evaluate the context in full. Therefore it scores 0.5.

ATTRIBUTE #3 (EFFECTIVENESS): SENSITIVITY

The likelihood of error or misinterpretation depends on the context. In identifying cannabis houses there would be a very low likelihood of error. In assisting in crowd control the

likelihood of error or misinterpretation would be very high. Again, because the purpose of use is not stated in the scenario, the technology scores 0.5.

ATTRIBUTE #4 (COST): INITIAL COST

Thermal cameras are becoming less expensive. One vendor's web page quotes a cost of £2000-£3000 per camera.[45] In this scenario there is one camera mounted on a UAV. The cost is therefore low. On the other hand, a control center is also often used, which is not so cheap. It scores 0.5.

ATTRIBUTE #5 (COST): PERSONNEL REQUIREMENTS

Personnel and training costs are low. It scores 1.

ATTRIBUTE #6 (COST): ADDITIONAL RUNNING COSTS

As the cost per camera is reasonable, the maintenance costs are presumed to be relatively low. The false-positive rate is low since the camera's purpose is to detect heat sources. It scores 1.

ATTRIBUTE #7 (PbD): DATA COLLECTION

Thermal cameras are deployed for specific events or activity, making them selective. In this scenario, the camera is mounted on the UAV, which means that some private areas will inevitably be filmed. The data is minimized since the identification of individuals is not possible. The collection is overt, but the fact that the camera is used at night means that it is likely to be undetected. The technology scores 0.5.

ATTRIBUTE #8 (PbD): DATA ACCESS & USE

Data access and use for the thermal camera is the same as for a regular camera mounted on a UAV – access to the data is restricted and clear regulations exist. There is no technical protection against function creep (although the incentive to use the camera for other purposes would seem to be less since only heat sources are detected and the image is not clear). It scores 0.5.

[45] http://www.smartcctvltd.com/traffic-products-and-surveys/video-analytics/thermal/

ATTRIBUTE #9 (PbD): DATA PROTECTION

Again, the thermal camera scores the same as the regular camera mounted on the UAV (see Attribute #9 for UAV). It scores 1.

ATTRIBUTE #10: EXCELLENCE

Thermal cameras have proven their excellence in identifying heat sources. The technology scores 1.

**Facewatch**

Facewatch is a cloud-based resource that enables businesses to upload CCTV images and witness statements regarding offenders of low-level crime. The images can be shared with other businesses, while images and statements can be submitted to the police. Facewatch also has a Watch List where shop owners can post images of subjects who have been involved in incidents at their business. The purpose is both to prevent crime and to assist the police in solving crimes. The public can view images issued by the police and confidentially identify the individuals.

ATTRIBUTE #1 (EFFECTIVENESS): DELIVERY

Facewatch certainly could yield a useful outcome with shoplifters and other offenders of low-level crime being identified, aiding the police in arrests and shop owners in protecting their goods. There is, however, no evidence of success. It scores 0.

ATTRIBUTE #2 (EFFECTIVENESS): CONTEXT

In this scenario Facewatch is used both in the context for which it was intended and for malicious purposes. It scores 0.5.

ATTRIBUTE #3 (EFFECTIVENESS): SENSITIVITY

There is a high likelihood of error and misinterpretation in individuals being misidentified, as well as the possibility of misuse as in the scenario. It scores 0.

ATTRIBUTE #4 (COST): INITIAL COST

Facewatch is a free application. It scores 1.

ATTRIBUTE #5 (COST): PERSONNEL REQUIREMENTS

There are no additional personnel or training costs. It scores 1.

ATTRIBUTE #6 (COST): ADDITIONAL RUNNING COSTS

There are no maintenance costs, but there is the possibility of a high false-positive rate. It scores 0.5.

ATTRIBUTE #7 (PbD): DATA COLLECTION

It is difficult to score Facewatch for data collection because the data is collected from a CCTV camera in a specific location – the business – and purportedly for a specific incident – the crime committed in the shop. This would make it selective and minimized (the collection is also overt). However, there is the possibility that the shop owner could use data not related to an incident. Due to this ambiguity it scores 0.5.

ATTRIBUTE #8 (PbD): DATA ACCESS & USE

Potentially anyone could have access to Facewatch. There are no clear regulations governing its use and there is no protection against function creep. It scores 0.

ATTRIBUTE #9 (PbD): DATA PROTECTION

Facewatch is advertised as a secure reporting environment and is presumably access protected. But given that any shop owner and any member of the public can submit and comment on data, this seems a moot point. It is unknown if the data is protected against manipulation. Additionally, it is impossible to know if every CCTV system in every shop collecting data is secure against theft. It scores 0.

ATTRIBUTE #10: EXCELLENCE

The excellence of Facewatch is not proven. It scores 0.

### §3.3.2. Ethics Analysis

Arnold, a citizen of the suburb of Wysteria in the city of X, has carried out a number of thefts of car radios over the previous two years in and around Wysteria and has not been caught. The thefts have been reported and are aggregated with similar crimes as data inputted into the PredPol system. The PredPol system predicts a higher likelihood of further car radio thefts in certain streets of Wysteria, and on this basis the decision is taken to deploy additional police to the area to look out for this sort of crime. Bill is walking through Wysteria on his way to the city centre and stops when he hears the sound of breaking glass. He turns around and sees a parked car with a broken window. He is just looking into the car when a deployed policeman sent to the street on the basis of the PredPol data arrives around the corner and sees Bill with his hand in the window of a car with its radio still in its place, and arrests him on suspicion of attempted theft.

The data processing involved in the system is of non identifying data to begin with, so the intrusion involved is relatively slight before we even take into account the purpose for which the information is used.[46] The moral risk of intrusion is assessed as negligible. Improving crime prevention is a purpose that could legitimately justify privacy intrusions deeper than the data processing involved here.

More significant ethical issues can be identified, however. Profiling techniques are often highly error prone,[47] for a start, and even if the programme correctly identifies a raised risk of radio thefts the overwhelming majority of people in the area in the specified time window will have no criminal intentions. Two kinds of error ought to be considered: first that the technology incorrectly ascribes an increased risk of radio thefts to Wysteria incorrectly, and secondly that an individual police officer unnecessarily charges an innocent. We treat each in turn.

[46] On serious crime investigations morally justifying intrusion see SURVEILLE deliverable D2.2. For more general overviews of informational privacy see Tavani and Moor (2001) and Tavani (2007)
[47] On the moral risk of error and profiling see DETECTER deliverables D5.2. and D5.4. and SURVEILLE deliverable D2.2.

What are the consequences if a system like Predpol incorrectly ascribes a heightened risk of crime? There aren't any that follow necessarily. Indeed at first sight the possibility that an area might have additional police officers deployed to it seems benign. However there can be costs to being over policed.

Much of this question will turn on the matter of whether the police officer arresting Bill overreacted due to the Predpol data. This is very difficult to establish with any certainty – even the police officer themself might not be able to know for sure. The mistake is an understandable one given Bill's putting of his hand through the window, and one can conceive of similar examples where crime mapping had no involvement. We conclude that there is a moderate risk of error here.

Profiling techniques are often controversial because they can be highly error prone and discriminatory. However, the kind of profiling involved here – profiling of a time and place – is much less morally problematic than that which profiles a potential suspect. Profiling a potential suspect on the basis of personal characteristics, and in particular membership in a group, poses much greater risks of being discriminatory. Nevertheless, profiling an area is not morally neutral, as it could indirectly lead to behaviour akin to the profiling of individuals, if for example it led to crude stigmatising of all people associated with an area. We therefore conclude that there is a risk to trust, albeit a manageable one we rate as moderate. The mere deployment of additional police in response to a greater risk of a specified crime does not by any means amount to such a stigmatisation.

More importantly, the evidence of suspicion in the use of crime mapping technology is much less direct than in a case where, for example, police were looking for a suspect on the basis of an eye witness description. While Predpol might successfully identify an increased chance of a particular crime occurring in a particular place within a time range it is not clear how much more likely anybody found there will be intending to commit crime given such an assessment.

A similar error could take place without any technology having been used. The technology would have to make such errors more likely to raise significant moral risks of error. Police officers deployed in extra numbers because of such an assessment of higher risk simply need to bear in mind that they do not have evidence of anyone's involvement in crime, but ought to treat every case they encounter on its own merits. The relevant agent acting on the Predpol data is the superior who decides to provide additional officers – the officer themself should simply carry out their duties as usual.

The Thales Cybels intelligence system continuously analyses the open source social media postings of a number of individuals known to police as suspected of conspiring to cause disorder on previous occasions – Twitter postings and messages posted in places where they can be seen by anyone logging on to the relevant page. One of these is Celine, who the social networking analysis reveals is in regular contact with David on political topics, including on the subject of today's demonstration. A number of the messages between Celine and David include criticism of police management of this and similar demonstrations. All of these messages to David are flagged up as meriting attention. Today, for the first time Celine uploads a message to a Facebook group suggesting that a number of people should try to break into the local party offices of the government party whose policies are being protested – this is an open Facebook group, potentially visible to anyone. David is one of 10 others agreeing that this is a good idea, but without expressing any specific commitment to participating himself. Extra police are assigned to the route as it passes by the party headquarters. A group of about 50 people, including Celine, David and Emily gather near the party headquarters. The police ask that they disperse or continue to the official site of the protest, the overwhelming majority of the 50 gathered near party headquarters remain and the situation evolves into a confrontation with police. Eventually Frank tries to break through the police cordon and, although the protesters fail to get into the party headquarters, there are scuffles between the police and the protesters. All the protesters congregating outside the party headquarters are arrested.

This case involves significant invasions of privacy. There is an important difference between closed and open source communications insofar as the entitlement to privacy is concerned. Closed source communications are automatically regarded as normatively more private – that is to say that in one's closed source communications one is entitled to a much stronger degree of protection from anybody viewing the message other than the intended recipient. However, although it is weaker than in the case of closed source communications, open source communications are still entitled to a degree of privacy.

A relevant analogy is communication in public space,[48] where there is a broad understanding of a default entitlement to privacy. Because public space is by definition the space from which nobody is excluded, we can have no absolute entitlement not to be seen or heard. Associational life in public spaces thus often has the feature that one's interactions may be open to the observation of others. This is not some limitation or deficiency of public space, it is often valuable in itself. Public parks and town squares are often places where one hopes one will meet others – a place to see and be seen. A range of similar social spaces are in fact privately owned premises – bars, restaurants or shopping centres – where admission is ultimately at the owner's discretion. Each will vary in terms of the interests people have in having their behaviour, and particularly interactions, unobserved. Furthermore, the observation of the police could be considered more intrusive than that of the ordinary citizen, especially when covert.

Therefore while Celine and David have not made efforts to conceal their conversation with each other, carrying it out in a medium where others can see it, this does not mean it is fair game for observation. Reading all their conversations is like eavesdropping on people having a conversation in a public park or on a café terrace. They may be aware that there is a possibility of being listened to, but weigh that against their awareness of the widespread understanding of a presumption against eavesdropping, especially on an extended basis. And given that all the conversations in the week leading up to the demonstration are scrutinised, it is like eavesdropping over an extended period, following the speakers throughout different sites in public space – as well as anything pertinent to the policing of

[48] On the ethical right to privacy in different locations, including 'virtual' spaces, see SURVEILLE deliverable D4.8.

the demonstration, the conversations between Celine and David are bound to cover matters which are none of the police's business. We conclude that there is an intermediate risk of intrusion.

Such an invasion of privacy can be justified, but requires a higher justification than, for example, watching people in public space. Evidence of the plotting of violence meets this threshold, but that is not what is under consideration here. Celine and David discuss breaking and entering private premises, which involves at least some damage to property, and is quite likely to result in damage beyond just breaking in. This supplies a weaker justification, though one which would justify investigating further to find out the full details of the damage planned and likely consequences. However, even if it is justified to 'continue reading' once evidence of these plans is encountered, this does not retrospectively justify the reading of Celine and David's messages to begin with. This depends on intelligence of past involvement in violence. Again we must ask what the nature of this evidence is: who compiles it, how often it is updated, whether its assessments can ever be challenged? Past involvement in 'disorder', especially of non violent, does not meet the threshold. Furthermore, conversations on social media that appear to offer a strong justification for believing that a person is involved in violent plans can often on further inspection turn out to be far more innocuous. Given the possibility of mistakes here we conclude that there is also an intermediate risk of error.

Having advance information about a plausible plan to damage property shared among a number of people, police are justified and (consistent with other policing priorities) obliged to do what they can to prevent it – the same as any other plausible threat to public or private property. It is defensible for extra police to be deployed to protect the party headquarters (depending on relative priorities on the day) though police must bear in mind that they are policing a legitimate political protest, and have a duty to facilitate it as far as possible. In particular, while arresting Frank and others acting violently might be appropriate, arresting those simply failing to disperse seems disproportionate. Any unjustifiable arrest represents a serious moral cost. The genuine intrusiveness of monitoring any social media activity and the ease with which interactions on social media can be

misunderstood, we consider that there is a risk of damage to trust in authorities because the monitoring of social media activity is perceived as illegitimate and of risk of chill. We assess this risk as intermediate.

Gary's numberplate is logged and analysed by the ANPR system as he drives into the inner city area where he lives. Helen is travelling from her home outside the city in to the city centre area to join the protest and her numberplate information is logged and analysed as well, and some time later she is charged the congestion tax. As with all ANPR records gathered in City X, the details of Gary and Helen's journeys remain stored and accessible by police for a period of two years and then are deleted.

A numberplate uniquely identifies a vehicle, which in practice often uniquely identifies an owner. Information that tracks the movement of a vehicle with a particular numberplate thus in practice often tracks the movement of an individual.[49] At the same time, the existence of numberplates already represents a compromising of anonymity in public space, but one that is justifiable given the danger of road travel, and the ease with which heavy costs can be inflicted on others (however unintentionally). This use of ANPR technology here seems legitimate, and given secure data handling practices there are minimal costs to privacy. The invasiveness depends on the possibility of others being able to use the data to track one's movements (or find out other information linked to the numberplate). If the only purpose of the ANPR technology was enforcing the congestion tax quicker deletion would be preferable, because the risk incurred to the individual would seem unnecessary.
But this is not the only purpose. Police access to the data could be morally proportionate, given a serious enough purpose – namely investigating or preventing significantly welfare threatening crime. In a genuine such case – where there is specific evidence suggesting a particular vehicle or a particular vehicle owner is involved in a bombing plot, or an armed robbery, for example – the loss of privacy on the part of the suspect(s) is justified by the weight of the crime and the great potential for ANPR data to be useful to the investigation,

[49] On locational privacy see SURVEILLE deliverable D4.8.

precisely because it potentially reveals so much. However this justification will be contingent on a full range of safeguards to prevent abuse. This will include a legal framework specifying that such use is legal, and further specifying the regime governing its use. The existing position with regard to ANPR remains unsatisfactory in a number of jurisdictions. On this basis we conclude that there is an intermediate risk to privacy and damage to trust. We also conclude that there is a risk of error resulting from the use of the technology, largely due to misconceptions arising from what the ANPR data appears to show, albeit a low risk.

Ida travels by bus from his home in Wysteria to a coffee shop in West Heath, a suburb on the other side of town where she meets John. Both then travel on the metro to the demonstration. All of Ida and John's travel is logged and automatically processed by software which provides the command centre with the information about passenger congestion. Ida's travel remains potentially identifiable to her as she has used a season ticket registered to her name and address. John buys a new travel card on the day which he retains for further use.

This case of Radio Frequency Identification (RFID) technology is similar to the ANPR in that the main issue at stake is locational privacy. As in the ANPR case, the data can easily reveal quite a detailed picture of the subject's movement through public space. Also similar to the case of ANPR the profiling of anonymised data en masse to provide the city with useful information about passenger congestion is a kind of profiling technique, but again it does not impose risks on any particular individual.

Because more detailed data is taken about Ida when she registers it might well be easier to identify the travel data as hers, depending on how much information is stored and in what manner. The more that the collection of data potentially reveals the greater the moral duty to keep such data secure, and the better the reason needed for collecting it in the first place. There is still a range of ways in which John's data might be linkable with his own record if linked with other data. He may well have bought the travel ticket with a bank card, and this record might be linkable. A more remote possibility is that features of the journey patterns themselves might suggest a particular individual, if something unique about John's travel

patterns is known. Thus the longer John holds on to the same ticket (topping up on a pay as you go basis, for example) the more identifiable the data.

As with the ANPR data the travel information could be useful in the event of an investigation. However, the justification may be less weighty than in the case of ANPR. This is because it is easier to avoid the tracking functions than in the case of ANPR. Avoiding ANPR creating a record of one's movements in a city like X where cameras are equipped with this functionality seems to entail giving up the use of vehicles entirely, which for a range of crimes will not be practical. On the other hand, a forensically aware criminal wishing to avoid the creation of a record of his or her travel records in a city with a scheme like Pass Navigo or the Oyster card has a number of options. She might avoid transport on the public transport ticketed in this way, which does not incur the same disruption as in the case of avoiding vehicle travel. This city may have ticketing options which are not traceable, as is the case in the cities with the existing Navigo and Oyster systems (if one pays in cash, and for separate journeys). The ease with which one may avoid tracking if one wishes to do so weakens the likely usefulness of the data, and therefore the strength of the justification for storing the data for these investigative purposes.

Our assessment of moral risk also follows that of the case of ANPR: conclude that there is an intermediate risk to privacy and damage to trust. We also conclude that there is a risk of error resulting from the use of the technology, largely due to misconceptions arising from what the RFID data appears to show, albeit a low risk.

The CCTV records Kezia, who is walking to the event, and stops to greet and talk with a number of friends she happens to meet along the way, some of whom are also going; Leonard, who is seen involved in a number of separate brief, violent scuffles (with Mary, Max and Melissa); and Neil, who closely resembles a 'known trouble maker' by the name of Niall, who is reported to have taken part in violence and to often carry a knife. Niall has previously engaged in fights at protests before.

Kezia is watched fleetingly and occasionally by a series of different viewers keeping a general eye on the crowd. Leonard's initial scuffle draws the attention of an operator who watches him until a policeman arrives who has been directed to investigate the incident. The policeman arrests Leonard on suspicion of assault. Neil is watched by a third operator who mistakes him for Niall. The operator sends a policeman to investigate further when he sees 'Niall' congregating with a number of other 'known trouble makers'. The policeman questions Neil and searches him suspecting he might be carrying a knife. When the search yields nothing Neil is free to go and continues on his journey.

The privacy one is entitled to while walking through public space is weak, and does not rule out the cursory glances that are likely from a CCTV operator watching a busy street with a heavy throughput of traffic. We conclude that the risk of intrusion is low.[50] It would rule out extended watching without some good reason. However, in all these cases the operator has a good reason for watching Kezia, Mary, Max and Melissa, at least for the duration of the operator's involvement. In cases where attention is not even directed at individual people, such as the use of CCTV to monitor, for example, numbers of people travelling through a station, the intrusiveness is lower still.

The case is more complicated with Neil. Mistaken identity cases are fairly common in the use of CCTV, though they are of course perfectly possible without the involvement of technology at all. We conclude that there is a moderate risk of error. More important to the result of a false identification is the identification of individual's such as Niall as 'known trouble makers'. It is not specified exactly how this information is recorded, if at all. In the assessment of the scenario, it can be safely assumed that the false identification was simply an error by an individual CCTV operator, without any pre-existing record of 'troublemakers'. Independently of the scenario it may be added that if there had been an actual record, to which the CCTV operator could refer while scanning the video feeds, the situation would be much more complicated. For instance, what information is this intelligence based on? Any intelligence is easily subject to a great degree of error, as it is likely to consist of more provisional, limited and unreliable evidence than would be introduced according to the rules

[50] See for example the argument of Ryberg (2007)

of evidence in a court of law. Intelligence as a rule makes use of a wider range of less reliable sources of information. Obviously the worse the intelligence underwriting the assessment of Niall as a 'troublemaker' the worse the moral case for providing such intelligence to CCTV operators. Beyond this principle we may say that the further the intelligence assessments are from those that use them the harder it is for individual operators or officers to challenge their conclusions. In this case the consequences are not disastrous, but not insignificant either – a body search is likely to be felt as intrusive and may also be experienced as humiliating. As well as involving a significant sanction, the error could also prove discriminatory – mistakes will not necessarily be distributed fairly around the population, but often cluster around particular demographic groups.

Although we take the view that the intrusiveness and risk of significant mistakes resulting from the use of CCTV may be moderate, assessment of CCTV's risk to trust is also a matter of public perception. CCTV cameras remain one of the most prominent and visible surveillance technologies, particularly in urban areas. We therefore assess the risk to trust as intermediate.

The smart functions flag up a number of individuals to the CCTV viewers as requiring attention. First Olivia tries to take a shortcut across the motorway while walking in to the city centre. The smart CCTV flags up her presence on the central reservation (where pedestrians are forbidden). A viewer notes her presence, and alerts a local traffic policeman, but she has moved on by the time she could get there. No further action is taken.

Phillip is walking to the protest past an area with a parked train. He drops his keys, and consequently spends a period of time crouched down next to the train. The smart CCTV flags him up for attention because of the algorithm targeting graffiti. The CCTV viewer thinks he is probably a graffiti vandal and two policemen are sent to investigate, including by questioning Phillip.

As with the unassisted CCTV viewing, the privacy issues here are minor. Although Olivia and Phillip are entitled to a presumption against extended watching, both sets of behaviours involved in these cases meet the threshold for legitimate police watching. We again conclude that the risk of intrusion is moderate.

Smart camera functions may assist CCTV operators with focussing on the most important behaviours. Any risks of error here are likely to be mitigated by the fact that any decision on the basis of such a process will be mediated by the 'human in the loop' viewing the video feed.[51] Nevertheless, one might be concerned about overbroad categories of behaviour, or those which overlap with innocuous behaviour like looking for one's keys. Least problematic from the point of view of avoiding the infliction of unnecessary costs on individuals, will be algorithms that unambiguously capture behaviour most legitimately of interest to authorities. In practice many of the behaviours will resemble either the cases of Olivia or of Philip – either very cleanly identifying relatively unimportant behaviour like Olivia's, or behaviour that is a legitimate object of attention like Phillip's but about which it is easy to be mistaken. The possibility of both kinds of mistake lead us to conclude that there is an intermediate possibility of error.

For example it is important to avoid disproportionate attention on behaviours like Olivia's just because they are categories of behaviour that can be cleanly identified by algorithm. How important is trespass on areas of motorways, or on train tracks where people are (rightly) not permitted to walk? It may rank low in relative priority to more welfare threatening crimes, but trespass in these places can cause unnecessary danger (both to traffic as well as the trespassers), and slow down traffic. It might not rise to the levels of criminal activities we examine elsewhere, but is a legitimate object of police concern.
As in the case of ordinary CCTV, there is an intermediate risk of damage to trust.

| |
|---|
| The abnormal behaviour detection flags up three people as behaving in a manner of interest for the CCTV viewers. Quentin has an argument where he suddenly raises his hand and strikes someone he was speaking to. Rebecca and Simon do not engage in wrongful action, |

[51] On the intrusiveness of smart camera algorithms see Macnish (2012)

but nevertheless separately trigger the alert. Rebecca is walking unusually. It is not clear why the smart CCTV categorises Simon's behaviour as unusual. The behaviour of all three is drawn to the attention of a CCTV operator. She sends an officer to investigate Quentin's violent scuffle. Watching Rebecca's unusual walk she concludes that this is what has led to the categorisation and concludes that no further action is needed. Confused by Simon's triggering of the system she asks an officer to investigate to see for himself if anything is wrong.

What is abnormal behaviour? Arguably we all operate with a sense of what actions fall within norms of expected behaviour and are able to recognise that which falls short. This is also arguably what a person does when police scan a crowd for criminal activity – first look out for that which is unusual, and then establish whether there is any call to investigate further. This works ideally in the case of Quentin. His behaviour merits the additional scrutiny that results.

As with the other smart camera functions it is very significant ethically that the assessment is mediated by the judgment of the CCTV operator – the human in the loop. This is what prevents Rebecca from being subjected to unnecessary attention. And that which she faces because of the false alarm is so fleeting that it doesn't rise to the level of moral significance. Simon is less lucky, however. Simon is erroneously subjected to police attention. In isolation this may have a low moral cost, but it will be of greater moral significance if the error is discriminatory. A system which consistently ascribed 'abnormal behaviour' to South East Asian men or Somali women would be unacceptable even if it had a significant (and proven) security benefit. If 'abnormal behaviour' is solely determined by modelling majority behaviour, it is plausible that minorities could be disproportionately affected. Therefore it is morally important that the operator have more confidence in their own assessment than was demonstrated in the Simon case. We conclude that there is an intermediate risk of error. The algorithm is a tool for directing the attention of operators, not evidence of wrongdoing. When the operator cannot see anything wrong themselves they do not need to double check this assessment with an officer on the ground.

As with the other kinds of CCTV we conclude that the risk of intrusion is low, but that the risk to trust is intermediate.

| |
|---|
| The drone briefly films Tina, a demonstrator, Ugo, a bystander who was not aware of the demonstration in advance and is walking in the other direction, Vanessa, who has been taking part in violent scuffles, and Wayne, who is sunbathing on his roof terrace where he assumes he is not visible to view, are all filmed by the drone. In most of the footage they are unidentifiable, and none are scrutinised more than fleetingly. All four see and are aware of the drone. |

Drones raise all the privacy problems that arise in relation to CCTV, and then some further ones that are usually avoided due to the fixed location of a camera (the fixed location of a CCTV camera also means that those subject to surveillance can be notified through signs informing them that surveillance takes place in the area). A drone can film extensively throughout public space, capturing the behaviour of people as they go about day-to-day life there. We therefore conclude that there is an intermediate risk of intrusion. Neither Tina, Ugo nor Vanessa could make any great claim that their default entitlement to privacy is violated here. The case of the viewing of large crowds if anything represent a weaker intrusion because the attention of the operator is divided among so many people, and this viewing at least is analogous to the observation by countless anonymous others all three willingly submit to by being in public space. Tina arguably has a greater understanding that by joining in the demonstration she opens herself to at least fleeting observation. But even Ugo who is not there with the aim of taking part in a demonstration understands that a large concentration of people is incompatible with any interest he might have in not being observed. Only Vanessa faces any likelihood of being subjected to any kind of extended scrutiny, and this is for an entirely apt reason – her involvement in violence.

More problematically drones can also film people in a range of places not normally subject to scrutiny and where there is a good case for stronger entitlements to privacy, such as residential gardens. Wayne sunbathing on his roof terrace stands in a similar position. All the cases - even that of the greater degree of intrusion involved in filming Wayne – are

mitigated by the fact that any attention directed to any of them is likely to be highly fleeting – to the extent any are seen at all it is as one person in a crowd of many. They may not be unobserved, but they remain effectively anonymous. Even Wayne is very unlikely to draw much focus from those viewing the crowd – seen just as a person sunbathing rather than an individual of any interest at all.

Although the risk to privacy is greater than in the case of ordinary CCTV, the risks of error are rated as just as moderate (if not more so) as we have assumed no further use of smart camera applications. Of course, if smart camera applications were to be used, the use of the UAV would incur these risks as well. Although the public may be less able to see when they are being used as is the case in deployment of overt CCTV, their greater intrusiveness contributes to the assessment of an intermediate risk of damage to trust. Separately from the issues of privacy and data protection there is an ethical issue that has nothing to do with surveillance. Namely the fact that a drone, however small and lightweight, is still an aircraft. Flying one in an urban area entails a strong duty to prevent any risk to public safety from crashing or otherwise losing control of the vehicle.

The thermal camera films Xandra as part of the crowd, though she is not identifiable. In passing it also picks up the form of Yuri, who is inside his home, and has an illegal cannabis greenhouse. Neither sighting is acted upon in the command centre.

The filming of Xandra raises even lower privacy issues than in the case of the video camera filming the crowd, as she is not identifiable.

The case of Yuri is much more complicated. Yuri is entitled to strong protections against observation in his home. If the thermal cameras were able to reveal details of his movement about his house, then it would represent an intrusion only appropriate in the most serious criminal investigations, and be quite impermissible in this context. We therefore conclude that thermal cameras raise intermediate risks of intrusion. The growing of a cannabis plant is illegal in X, and thus this is arguably in a quite separate category. If the thermal cameras revealed details of behaviour within the home beyond this, the use of

thermal cameras would become inappropriate without a specific reason to justify the invasion of privacy (or possibly the use of thermal cameras in such a case should be accompanied by some kind of privacy masking). As it stands it is appropriate that Yuri's inadvertently spotted activity is not pursued as a result of this surveillance.

Although it is more intrusive than the use of cameras covering only public spaces the outputted information is judged to incur only a moderate risk of error. The use of the technology is also judged to incur only a moderate risk of damage to trust.

Zara has carried out a number of wallet thefts in city centre shops, and has nearly been caught on a number of occasions but there has not been sufficient evidence to press charges. Annwen, a business owner, has seen Zara in the area on a number of occasions when a wallet is pickpocketed on her premises. Today a store security guard tries to stop Zara to search her after a pickpocketing takes place and Zara runs off. Annwen uploads Zara's image to the Facewatch system taken on the shop's CCTV.

Brendan is another business owner. He has recently had an argument with Ciara. Brendan maliciously uploads a photograph of Ciara in the hope of causing her inconvenience.

Both Zara and Ciara are spotted by shop owners making use of the system which identifies them as troublemakers and consequently subject them to additional scrutiny while they are there.

Any hypothetical shared list of people suspected of criminal activity is ethically problematic. Such lists are problematic primarily because of the ease with which innocent people can find themselves entered on these lists without their knowledge and suffering significant costs unjustly. We therefore assess this technology as raising intermediate risks of error. As with the case of the CCTV operators working with intelligence that certain individuals are 'trouble makers' questions must be asked about how reliable this information is and what kinds of action could be taken on the basis of it. Annwen's use of it to draw attention to Zara

represents a case of the system working ideally and as intended. Here certainly Zara can have no complaint that her privacy is unfairly invaded – her behaviour merits the additional attention, even if she is subjected to it on occasions when she has no intention of carrying out thefts. Even this ideal case is not entirely free of problems, as it is entirely possible that at some stage somebody who looks similar to Zara may be mistaken for her (as in the Neil/Niall case), especially given that the system operates on the basis of recognising faces.

Ciara's privacy is invaded by the unwarranted scrutiny which will attend her throughout the businesses signed up to the scheme, whether or not she is aware of it. Much more serious than the interference with her anonymity is the possibility of further inconvenience and stigmatisation associated with the false identification of her as a criminal. The possibility of cases like this motivates the judgement that this technology incurs intermediate risks of intrusion and damage to trust. Brendan's malicious use of the system is obviously highly unethical, and exploits a range of others – police and fellow business people – to pursue his own vendetta. If the system fails to guard against this possibility, however, it is not just his moral failing that is implicated. While the privacy cost inflicted on Ciara in this case is not particularly weighty, it could have been higher. One can imagine a case where there is other misleading evidence of theft and thus her inclusion on Facewatch is decisive in her being searched. Both police and business owners need to bear in mind the highly provisional and limited nature of the intelligence. While it can be useful for directing attention amongst the large number of people making their way through a city, users of systems like Facewatch overwhelmingly ought to trust their own assessments of individuals in deciding whether actions like searches are warranted – if they cannot justify such an action on the basis of the evidence directly available to them they should not allow the fact that they appear on the Facewatch system to 'tip the balance'.

### §3.3.3. Fundamental Rights Analysis

SURVEILLE deliverable D2.6 was a scenario-based assessment of 14 surveillance technologies applied in 19 different situations in the context of the detection and investigation of serious organised crime. The resulting usability scores ranged from 3 to 9 on the scale of 0-10, where a higher score reflects better effectiveness and efficiency delivered by the use of a technology, towards a legitimate aim such as the investigation of crime. The same technologies were assessed as to their intrusiveness into fundamental rights, and these scores obtained varied from 0 (no intrusion) to 16, the latter representing the highest possible degree of fundamental rights intrusion. Further, the technologies were also reviewed for their ethical implications using three colours for different degrees of ethical risk: green for moderate, amber for intermediate and red for severe ethical risk.

Subsequent SURVEILLE deliverable D2.8 built upon the methodology developed for deliverable D2.6, now in the context of a terrorism prevention scenario and the use of six surveillance technologies or techniques. Deliverable D2.8 also included a discussion on a judgment delivered after the completion of D2.6 by the highest EU court, the Court of Justice of the European Union (CJEU), in *Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others*,[52] declaring invalid the EU data retention directive of 2006.[53] The CJEU's ruling was seen as supporting the SURVEILLE methodology developed for the fundamental rights assessments. In the assessments performed for deliverable D2.8, only the two traditional (non-technological) surveillance methods produced low fundamental rights intrusion scores (3/4), when using the same criteria that were used in deliverable D2.6. Three methods of electronic surveillance gave the highest possible fundamental rights intrusion score (16). Only one of the methods of electronic surveillance – targeted social network analysis – gave a medium-high score (8). The usability scores varied from 4 to 8, so that the lowest fundamental rights intrusion scores coincided with the highest usability (effectiveness and efficiency) scores.

[52] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communication et al* and *Kärtner Landesregierung et al*, judgment of 8 April 2014, nyr.

[53] 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 (OJ 2006 L105, p. 54).

In the current deliverable, the methodology developed in SURVEILLE deliverables D2.6 and D2.8 was used to assess the fundamental rights intrusion resulting from the use of ten surveillance technologies or techniques, as applied in the urban security scenario. As before, the assessments focused on the right to the protection of private life (or privacy) and the right to the protection of personal data. In some cases the possible intrusion into other fundamental rights, such as freedom of expression or freedom of association, was found to be derivative in nature, resulting from the first-order intrusion into privacy or data protection rights, and the scoring was conducted only in relation to the rights immediately impacted. However, in five out of the ten cases an independent assessment was made in relation to a third fundamental right which in two cases was the right not to be discriminated against, in two cases the right to the liberty of the person and in one case the freedoms of assembly and association. In the context of the urban security scenario independent impact upon the enjoyment of these rights was identified in those five cases, resulting in intrusion scores separate from the scores for privacy and data protection intrusion. Notably, the highest intrusion score (12) was this time obtained in relation to the right to the liberty of the person. As a word of caution it needs, however, to be pointed out that this assessment was based on the text of the scenario where a particular surveillance technique (social media analysis) resulted in the arrest of a number of persons on grounds that were assessed as arbitrary. Hence, the high intrusion score in this particular case was a causal but not an unavoidable outcome of the surveillance as such. It resulted of wrongful action taken by the authorities following the surveillance.

As in earlier deliverables D2.6 and D2.8, the fundamental rights intrusion scores 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 a fundamental right or, similarly, low, medium or high level of intrusion into that right. The two scores are then

multiplied with each other to give a combined score from 1 to 16 – or 0 where no fundamental rights impact could be identified.[54]

The primary source material used to assign the scores (low/medium/high) was found in existing case law by the European Court of Human Rights (ECtHR), complemented by the case law of the EU Court of Justice (including under the EU Charter of Fundamental Rights) and the United Nations Human Rights Committee acting under the International Covenant on Civil and Political Rights. The scoring is accompanied by detailed reference to this body of case law related to identical, similar or analogous situations, mostly the case-law by the ECtHR. The scoring has been verified collectively by the team of legal experts functioning as the EUI team in SURVEILLE. Where existing case law by the ECtHR and other relevant authorities was absent or ambiguous, the score has been corrected by multiplying it by a reliability factor of ¾. A similar reduction of the intrusion score by one fourth (i.e., multiplication by ¾) would be applied if the use of a surveillance method was authorised by a court. In practice, as none of the surveillance methods applied in the scenario had judicial authorization, no such reduction of the privacy or data protection scores was possible this time. However, in the two cases where a deprivation of liberty (arrest) resulted from the surveillance, it was assumed that such a measure would in any EU Member State be subject to prompt judicial review, and the multiplier of ¾ was therefore applied towards the final score.

As the text of the urban security scenario mentions several fictitious characters who often are differently situated in relation to a specific surveillance method, some of the assessments came to produce alternative scores for the same surveillance method, reflecting variation in how differently situated individuals were impacted.

The resulting scores are presented below on the following page. As can be seen, in four out of ten cases the assessments produced identical scores for privacy and data protection, while in two cases no impact upon data protection could be identified even if there was a privacy impact. As explained above, in five out of ten cases an autonomous impact upon a

[54] For a discussion of the methodology and its theoretical background, see SURVEILLE deliverable D2.6, section 2.3.3.

third fundamental right was identified and assessed. In general, the resulting intrusion scores were lower than in earlier deliverables D2.6 and D2.8. In particular, in only one case (social media analysis) there was an intrusion score higher than 8, and, as explained above, even there the score was not a direct result of surveillance itself but of arbitrary arrest wrongfully triggered by the surveillance. In four out of ten cases the outcome was the relatively high intrusion score of 8 in respect of at least one individual and at least one fundamental right. Only a very high usability score, i.e. security benefit, could possibly justify such a degree of fundamental rights intrusion.

| Technology or technique | Fundamental right to the protection of personal data | | | | Fundamental right to the protection of privacy | | | | Other fundamental rights | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Abstr. Weight | Intrus-iveness | Reliability of the law | Score | Abstr. weight | Intrus-iveness | Reliability of the law | Score | Abstr. weight | Intrus-iveness | Reliability Of the law | Score |
| 1. Predictive crime mapping (PredPol) | | | | | 1 | 1 | 3/4 | ¾ | 2 non-discr | 1 | 3/4 | 1,5 |
| 2. Social media analysis (Thales Cybles) | 2 | 4 | 1 | 8 | 2 | 4 | 1 | 8 | 4 liber-ty | 4 | 1 | 12 jud rev. |
| 3. ANPR | 2 | 1 or 4 | 1 | 2 or 8 | 2 | 1 or 4 | 1 | 2 or 8 | | | | |
| 4. RFID in transport ticket | 2 | 1 or 4 | 1 | 2 or 8 | 2 | 1 or 4 | 1 | 2 or 8 | | | | |
| 5. Traditional CCTV | 0 or 1 | 2 | 1 | 0 or 2 | 1 or 2 | 1 or 2 | 1 | 1 or 4 | 4 liber-ty | 1 | 1 | 3 jud rev. |
| 6. Smart CCTV | 1 | 2 | 1 | 2 | 1 | 1 | 1 | 1 | | | | |
| 7. Abnormal behaviour det. (ADABTS) | 1 | 2 | 1 | 2 | 1 | 1 | 1 | 1 | 2 non-discr | 1 | 1 | 2 |
| 8. UAV with videocamera | 1 or 4 | 2 | 1 | 2 or 8 | 1 or 4 | 2 | 1 | 2 or 8 | 2 assembly & assoc | 2 | 1 | 4 |
| 9. UAV with thermal camera | 1 or 2 | 2 | 1 | 2 or 4 | 1 or 2 | 2 | 1 | 2 or 4 | | | | |
| 10. Image sharing | 4 | 2 | 1 | 8 | 2 | 2 | 1 | 4 | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| (Facewatch) | | | | | | | | | | | | |

A brief account of the justification for these scores follows below. For the more detailed complete assessments and for the sources (case-law) used to verify each step of the assessments, see Annex 1 of this deliverable.

**§3.3.2.1 The PredPol system**

The suspected car radio thief (Arnold) is mentioned in the text of the scenario but apparently not impacted by the surveillance. Instead, the assessment focuses on a bystander (Bill) who out of curiosity ends up examining a broken car window. The use of the PredPol system results in increased police presence in the area, and as a consequence Bill gets arrested as a suspect.

There is no issue under the *right to the protection of personal data*, as the PredPol system does not collect any personal data (including images) of crime victims, offenders, or law enforcement. It nevertheless results in a heightened degree of police monitoring through non-intrusive means of certain public areas which is seen as impacting a low-importance (1) dimension of the *right to privacy* to a low (1) degree. As there is no clear ECtHR or CJEU case-law in the issue, the reliability of the assessment is medium (3/4) and the resulting privacy intrusion score therefore ¾.

Also the *right not to be discriminated against* is affected, as PredPol may result in tighter overall control of people residing in poor and segregated neighbourhoods, where crime rates are higher. PredPol may also lead to subconcious *de facto* (unregulated) profiling based on ethnicity or other group-based characteristics when a policeman sent to the area by PredPol sees an individual who behaves in a suspicious manner. The policeman's actions may be influenced by stereotypical assumptions related to the ethnicity or other group characteristics of the person. It is however assessed that as such *de facto* profiling can be countered through proper training of the police and as the scenario text does not suggest that Bill was targeted because of his membership in a group, the intrusion is assessed as low

(1) and as affecting a medium-weight dimension (2) of non-disrimination, namely membership in a group. Again, there is no authoritative case-law directly applicable, so the reliability factor is ¾ and the resulting score therefore 1,5.

Even though Bill was arrested at the crime scene, no assessment under the *right to liberty of the person* was conducted. This is because the surveillance had no bearing upon the arrest which plainly followed from the suspicious behaviour by Bill in the presence of the policeman.

**§3.3.2.2 Thales Cybels social media analysis**

The text of the scenario makes it clear that the Thales Cybels system collects and processes personal data, some of which, such as political opinion, is sensitive in nature. The importance of the fundamental *right to the protection of personal data* in the context at issue is therefore intermediate, even if the data is collected from publicly available sources (2).

The use of social network analysis as in the scenario interferes with the right to the protection of personal data. This technology affords scope for an agency to conduct systematic and widespread surveillance activity. The ECtHR has articulated in its prior judgments that the scope of covert intelligence gathering needs to have a clear and precise basis for it to be conducted in a lawful manner, else it risks abuse and arbitrary application. The database contains information innocent persons and their political opinions, as it is based on categories such as ‘suspected of conspiring to cause disorder’ or earlier criticism of the police. The intrusion in the right to the protection of personal data is serious (4).
In the light of clear case-law by the ECtHR and the CJEU (see Annex 1), these assessments are reliable and the resulting intrusion score for the right to the protection of personal data is 8.

An assessment under the *right to privacy* produces the same outcome. The social network analysis falls within the ambit of both ‘private life’ and ‘correspondence’ in relation to ECHR

Article 8. The importance of privacy in this context is intermediate (2). The social network analysis targets a wide range of communications between individuals. The systematic collection of the data and the fact that it subsequently used without the user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance. In this case, the intrusive aspect of surveillance is further intensified by the fact that surveillance is targeted at a group of individuals on the basis of their associations and political opinions. The intrusion is serious (4). As above, clear case-law exists and the assessment is reliable (1). The resulting intrusion score for the right to privacy is 8.

*Freedom of assembly, freedom of expression, freedom of association* are all affected by the use of Thales Cybels but this impact can be assessed through a full assessment of privacy and data protection, as no higher score would result in respect of these other rights.

The question about the *right to liberty of the person* is different, as the use of surveillance targeted a group and ultimately resulted in the arrest of a large number of members of the group. A deprivation of liberty is a severe interference with the right to liberty of the person. Any arrest affects the core area of the right to the liberty of the person. The importance of liberty in that context is high (4). The arrests of individuals who personally used violence against the police may be seen as triggered by their own unlawful conduct and therefore as a low-level intrusion (1). The fact that such arrests are triggered by individual unlawful actual conduct justifies the conclusion that they are not an outcome of the surveillance and can therefore be excluded from the assessment of Thales Cybles. However, the arrest of those demonstrators who have *not* used force to break through the police cordon and who have not engaged in violent scuffles, are without proper justification and hence arbitrary. In the context of the scenario they must be assessed as being a consequence of the surveillance targeting a group on the basis of their political opinion. Arbitrary arrest is a serious intrusion into the right to liberty of the person (4). In the light of clear case-law by the ECtHR (see Annex 1), these assessments are reliable (1). However, as the law of any EU Member State would secure prompt judicial review of the lawfulness of the arrest we can safely assume

that the measure is subject to judicial review and the score should be multiplied by ¾. The resulting intrusion score for the right to liberty of the person is 12.

#### §3.3.2.3 Automatic Number Plate Recognition (ANPR)

The text of the scenario makes it clear that City X uses automatic number plate recognition for the purpose of collecting a congestion tax from owners of vehicles that pass through the inner city. What, however, is not clear is whether the two-year access by the police to the recorded information is solely restricted to the enforcement of the congestion tax, or whether it could be used for other policing purposes as well. The fundamental rights assessments therefore produce two alternative scores for privacy and data protection intrusion.

According to the scenario, the ANPR system records at least the vehicle, its location and route, and the identity of the owner. This amounts to the collection and processing of personal data which, however, is not sensitive in nature, even if a person's identity and location data when combined with other data can reveal a significant amount of personal information and allow for inferences also in relation to sensitive data (such as religious affiliation or sexual orientation). The use of the ANPR system constitutes an interference with the *right to the protection of personal data* and affects a dimension of that right that is of medium importance (2). The level of intrusion into that right depends on whether the two-year access by the police is governed by the purpose limitation principle and hence only available for the purpose of enforcing the congestion tax, or whether the data is available also for other policing purposes. Location data as such is not sensitive personal information. However, if the police have unlimited access to the data, contrary to the purpose limitation principle, then their access to location data will represent a significant intrusion in the privacy rights of the individual and will affect his or her choices where to go (e.g. a mosque or a gay club). If police access to the data is limited to the enforcement of the congestion charge, the intrusion is assessed as low (1). If police access is unlimited, over a period of two years, the intrusion becomes severe (4). In the light of clear case-law by the ECtHR and the CJEU (see Annex 1), these assessments are reliable (1) and the resulting intrusion score for

the right to the protection of personal data is either 2 or 8, depending on whether access by the police is limited or unlimited.

An assessment under the *right to privacy* produces the same outcomes. According to established case law by 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. 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 the target's right to private life. Given that Art. 52 (3) CFREU stipulates that the ECHR is a minimum standard these considerations by the ECtHR also apply within the EU legal order. The importance of the right is medium (2). As with the right to the protection of personal data, if police access to the data is limited to the enforcement of the congestion charge, the intrusion is assessed as low (1) but if police access is unlimited, over a period of two years, the intrusion becomes severe (4). As above, these assessments are reliable (1) and the resulting intrusion score for the right to privacy is either 2 or 8, depending on whether access by the police is limited or unlimited.

Also *freedom of movement, freedom of religion,* and *freedom of association* are potentially affected by the use of the ANPR system but the privacy and data protection assessments are capable of capturing this impact, as no higher scores would result for these rights.

#### §3.3.2.4 Radio Frequency Identification (RFID)

City X also uses the RFID system to track users of public transport through an electronic chip inserted in their ticket. The following fundamental rights assessment is very similar to the previous one on ANPR, also in that it is not clear whether the accumulated data can only be used for its original purpose or whether it would be generally available to the police. The main difference compared to the RFID assessment is that here only one of two individuals (Ida) is identifiable as she uses a season ticket, whereas the other individual (John) remains anonymous because of using a one-day ticket.

In Ida's case, the RFID system records at least her identity, location and route. This amounts to the collection and processing of personal data which, however, is not sensitive in nature, even if a person's identity and location data when combined with other data can reveal a significant amount of personal information and allow for inferences also in relation to sensitive data (such as religious affiliation or sexual orientation). Even if John uses a single-day ticket and is therefore not immediately identified by the system, he will be potentially identifiable if his location data is connected with other personal information about him. Therefore a separate assessment is not conducted in respect of him and we can focus on Ida who is clearly identified at the outset. The use of the RFID system constitutes an interference with the *right to the protection of personal data* and affects a dimension of that right that is of medium importance (2). The level of intrusion into that right depends on whether the two-year access by the police is governed by the purpose limitation principle and hence only available for the purpose of enforcing the congestion tax, or whether the data is available also for other policing purposes. Location data as such is not sensitive personal information. However, if the police have unlimited access to the data, contrary to the purpose limitation principle, then their access to location data will represent a significant intrusion in the privacy rights of the individual and will affect his or her choices where to go (e.g. a mosque or a gay club). If the authorities' access to the data is limited to the monitoring of travel congestion, the intrusion is assessed as low (1). If police access is unlimited the intrusion becomes severe (4). In the light of clear case-law by the ECtHR and the CJEU (see Annex 1), these assessments are reliable and the resulting intrusion score for the right to the protection of personal data is either 2 or 8, depending on whether access by the police is limited or unlimited.

An assessment under the *right to privacy* produces the same outcomes. According to established case law by 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. 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. Given that Art. 52 (3) CFREU stipulates that ECHR is minimum standard these considerations by the ECtHR also apply within the EU legal order. The importance of the right is medium (2). As with the right to the protection of personal data, if the authorities' access to the data is limited to monitoring traffic congestion congestion, the intrusion is assessed as low (1) but if police has unlimited access is the intrusion becomes severe (4). As above, these assessments are reliable (1) and the resulting intrusion score for the right to privacy is either 2 or 8, depending on whether access by the police is limited or unlimited.

Also *freedom of movement* is affected but the privacy and data protection assessments are capable of capturing this impact, as so higher scores would result for this right.

**§3.3.2.5 CCTV**

The scenario includes the use of 'traditional' close-circuit television monitoring, distinguished from 'smart' CCTV and 'abnormal behaviour' detection which are subject to separate assessments. Against that background the fundamental rights assessment of plain CCTV is here based on the assumption that the CCTV system in question does not include any database on individual persons or any automated face recognition capacity. Hence, the reference to 'known troublemakers' in the text of the scenario is taken as referring to the coincidental possibility that an individual CCTV operator may recognise a person appearing on the screen and associate that person with his or her own previous knowledge about the person.

As the CCTV system, according to the assumption explained above, merely records individuals in a public place and does not use or produce a database of individually identifiable data, the importance of the fundamental *right to the protection of personal data* is low (1) in the given context (see, SURVEILLE deliverable D2.6, annex 3, p. 81). Even 'traditional' CCTV nevertheless falls within the ambit of the right, as persons will be identifiable on the TV screen and in the resulting recording. There is no data protection issue in respect of Niall who apparently is just by coincidence known to the individual CCTV operator but in fact is not even seen on CCTV. As the CCTV records individuals in a public

place and the data is used for police purposes, the level of the intrusion is assessed as medium (2), as established earlier in SURVEILLE deliverable D2.6 (Annex 3, p. 81). These assessments are based on clear case law by the ECtHR and are therefore reliable (1). The resulting intrusion score for the right to the protection of personal data is therefore 2 (except for Niall in respect of whom there was no intrusion).

The use of traditional CCTV in public space also falls within the ambit of the *right to privacy*. As it means surveillance by optical means (in contrast to sound recordings) in public space (in contrast to private or semi-private space), the weight of privacy in that context is assessed as low (1). Neil, however, is subjected to an external pat search of his clothes which interferes with a separate aspect of privacy which is of medium importance (2). Similarly, the use of CCTV constitutes a low-level (1) intrusion into privacy, and the pat search a medium-level (2) intrusion. These assessments are based on clear case law by the ECtHR and are therefore reliable (1). The resulting intrusion score for the right to privacy is therefore 1 for the individuals subject only to CCTV and 4 in respect of Neil who because of the CCTV surveillance was subsequently subjected to a pat search. (Again, there was no intrusion in respect of Niall even if he appears in the text of the scenario.)

The right to *liberty of the person* is at issue in respect of Leonard, as the CCTV surveillance results in the directing of the police to him, and subsequently to his arrest because of his violent behaviour towards other people. A deprivation of liberty is a severe interference with the right to liberty of the person. Any arrest affects the core area of the right to the liberty of the person. The importance of liberty in that context is high (4). The arrest of an individual who was on CCTV seen to use violence against others may be seen as triggered by their own unlawful conduct and therefore as a low-level intrusion (1). In the light of clear case-law by the ECtHR (see Annex 1), these assessments are reliable (1). However, as the law of any EU Member State would secure prompt judicial review of the lawfulness of the arrest we can safely assume that the measure is subject to judicial review and the score should be multiplied by ¾. The resulting intrusion score for the right to liberty of the person is therefore 3.

### §3.3.2.6 Smart CCTV

In the next stage of the scenario, two individuals are identified by smart CCTV as requiring attention by a human operator. There is no information of a pre-existing database of individuals warranting attention, or of facial recognition software that would produce such a database for further use. Instead, the only 'smart' function of the particular CCTV system appears to be an automated capacity to alert the human CCTV operator who perhaps is simultaneously monitoring too many screens to give them equal attention at every moment. The CCTV system identifies Olivia's presence in a forbidden place and conduct by Phillip that suggests he may be painting graffiti. In both cases the operator then alerts the police who will visit the scene.

As the CCTV system allows for the identification of individuals and as the images are presumably recorded, the fundamental *right to the protection of personal data* is at issue. As the CCTV system merely records through visual means individuals in a public place and there is no pre-existing database of identified individuals, the importance of the impacted dimension of the right to protection of personal data is low (1). (See, Deliverable 2.6, annex 3, p. 81.) As in the preceding case of traditional CCTV, the intrusion into data protection rights through the use of CCTV images for police purposes is of medium level (2). (See, Deliverable 2.6, annex 3, p. 81.) Due to the existence of clear ECtHR case-law (see Annex 1), the assessment is reliable (1). The resulting intrusion score is 2.

As in the preceding case of the use of traditional CCTV in public space, also smart CCTV falls within the ambit of the *right to privacy*. As it means surveillance by optical means (in contrast to sound recordings) in public space (in contrast to private or semi-private space), the weight of privacy in that context is assessed as low (1). Also here the use of CCTV constitutes a low-level (1) intrusion into privacy. Again, due to the existence of clear ECtHR case-law (see Annex 1), the assessment is reliable (1). The resulting intrusion score is 1.

No issue of the *right to liberty of the person* arises from merely questioning Phillip, as he is not arrested.

### §3.3.2.7 Smart CCTV detecting abnormal behaviour in crowds

Another variation of 'smart' CCTV surveillance technology is provided by the ADABTS abnormal behaviour detection system. In the scenario, the ADABTS algorithm flags up three people as behaving in a manner of interest for the CCTV viewers: Quentin who suddenly raises his hand and strikes someone he was speaking to, Rebecca who is walking unusually, and Simon without any clear reason. The behaviour of all three is drawn to the attention of a human CCTV operator who sends police officers to investigate Quentin's violent behaviour and the unexplained case of Simon but concludes that no further action is needed in respect of Rebecca. There is no information of a pre-existing database of individuals warranting attention, or of facial recognition software that would produce such a database for further use. Instead, the only 'smart' function of the particular CCTV system appears to be to alert the human CCTV operator.

The assessments are almost identical to the ones under the first version of smart CCTV. As the CCTV system allows for the identification of individuals and as the images are presumably recorded, the fundamental *right to the protection of personal data* is at issue. As the CCTV system merely records through visual means individuals in a public place and there is no pre-existing database of identified individuals, the importance of the right to protection of personal data is low (1). (See, Deliverable 2.6, annex 3, p. 81.) As in the preceding case of traditional CCTV, the intrusion into data protection rights through the use of CCTV images for police purposes is of medium level (2). (See, Deliverable 2.6, annex 3, p. 81.) Due to the existence of clear ECtHR case-law (see Annex 1), the assessment is reliable (1). The resulting intrusion score is 2.

As in the preceding case of the use of traditional CCTV in public space, also the ADABTS version of smart CCTV falls within the ambit of the *right to privacy*. As it means surveillance by optical means (in contrast to sound recordings) in public space (in contrast to private or semi-private space), the weight of privacy in that context is assessed as low (1). Once again, the use of CCTV constitutes a low-level (1) intrusion into privacy and, due to the existence of

clear ECtHR case-law (see Annex 1), the assessment is reliable (1). The resulting intrusion score is 1.

As there is no mention of Quentin being arrested, there is no issue concerning the *right to liberty of the person*.

The case of Rebecca, however, raises an additional issue about the *right to non-discrimination*. She is possibly targeted for more intensive observation because of an issue of health or disability which indirectly discriminates against her and affects a medium-important dimension of the right to non-discrimination (2). Since the system only alerts the operator about a potential target and no further action is taken, the resulting intrusion is Rebecca's equality rights is low (1). In the light of pre-existing case-law by the ECtHR, these assessments are reliable (1) (see Annex 1). The resulting intrusion score for the right to non-discrimination is 2.

**§3.3.2.8 UAV with optical camera**

In the next phase of the scenario, a video camera is mounted on a drone (UAV) that films people from above, irrespective of whether they are located in public or private space. There is no indication of such 'smart' functions of the system that would include a pre-existing database of identified individuals or the creation of such a database. The video images are nevertheless recorded and the persons appearing in them will at least in some cases be identifiable.

As the video camera merely records Tina, Ugo and Vanessa in a public place, the importance of the affected dimension of the *right to the protection of personal data* is low (1), even if the persons would be identifiable in the footage (see, Deliverable 2.6, annex 3, p. 81). The case of Wayne, however, is different as he is filmed while being in private space and sunbathing, possibly naked. The recording of an individual's (presumably) naked appearance in private premises entails processing of sensitive personal data, touching upon a high-

importance (4) dimension of data protection. The fact that the individuals in question happen not to notice the drone does not change the fact that effectively its use for video surveillance is covert in nature, compared to traditional CCTV cameras that represent overt surveillance due to their stationary location and the visible warning notices. Furthermore, the recordings are used for police purposes. The level of intrusion is assessed as medium (2). (See, Deliverable 2.6, annex 3, p. 81.) Due to the existence of clear case-law by the ECtHR (see Annex 1), these assessments are reliable (1). The resulting intrusion score for the right to the protection for personal data is 8 for Wayne and 2 for the other individuals.

The assessment under the *right to privacy* produces identical results. In the case of Wayne, the watching and recording of a (presumably) naked individual in a private place interferes with an aspect of private life which is close to the core of the right (4). Watching and recording of the other individuals in a public place affects a dimension of private life that is of low importance (1). Because of the covert nature of the type of surveillance, the degree of intrusion into privacy is intermediate (2) in respect of all affected individuals. Due to the existence of clear case-law by the ECtHR (see Annex 1), these assessments are reliable (1). The resulting intrusion score for the *right to privacy* is 8 for Wayne and 2 for the other individuals.

Using a drone with a video camera to observe and record a demonstration interferes with a medium-importance (2) dimension of the *freedom of association* and the *freedom of assembly*. As the intrusion takes place for policing purposes, it is of medium (2) intensity. Due to the existence of clear case-law by the ECtHR (see Annex 1), these assessments are reliable (1). The resulting intrusion score for the rights to freedom of assembly and association is 4 for Tina who was the affected individual mentioned in the scenario.

#### §3.3.2.9 UAV with thermal camera

As a modification of the previous phase of the scenario, a thermal camera is now mounted on the UAV. This allows for night-time surveillance – which is not relevant in the context of

the scenario – and for surveillance through light structures into private places where a person is shielded against conventional visual observation.

The use of a thermal camera mounted on a UAV raises limited issues under the *right to the protection of personal data*. As far as it records the crowd in a public place, entailing a very low level of capacity to identify individuals, and presuming the system does not use a pre-existing database of individually identifiable data, the importance of data protection rights at issue is at maximum low (1), (see Deliverable 2.6, annex 3, p. 81). The case of Yuri, however, is different, as he is in private space (at his home) and identifiable by combining the footage from the thermal camera with other data such as his home address. A medium-importance dimension of data protection rights is affected (2) in his case. As far as the system records individuals in a public place and the data is used for police purposes, the intrusion into data protection rights is of medium intensity (2) (see Deliverable 2.6, annex 3, p. 81). Even if Yuri is in a private place and the weight of his data protection rights is therefore higher, the intrusion is the same and on medium level (2). Due to the existence of clear ECtHR case-law (see Annex 1), these assessments are reliable (1). The resulting intrusion score is 4 in the case of Yuri and 2 in the case of members of the crowd (and 0 in the case of Xandra).

As to the *right to privacy*, covert watching of individuals in a public place interferes with a dimension of privacy that is of low importance (1), even if the use of a thermal camera at night time might make the assessment shift towards medium (2) importance due to the changes in human behaviour in public space when surrounded by darkness. With regard to Yuri, the watching of individuals at home interferes with an aspect of privacy rights which is of intermediate importance (2). As far as the system records individuals in a public place and the data is used for police purposes, the intrusion into data protection rights is of medium intensity (2) (see, Deliverable 2.6, annex 3, p. 81). Even if Yuri is in a private place and the weight of his privacy rights is therefore higher, the intrusion is the same and on medium level (2). Due to the existence of clear ECtHR case-law (see Annex 1), these assessments are reliable (1). The resulting intrusion score is 4 in the case of Yuri and 2 in the case of members of the crowd.

### §3.3.2.10 The Facewatch System

The last phase of the scenario relates to 'Facewatch', a system that allows private parties, such as shops, to share CCTV footage for instance of suspected shoplifters. Two individuals, Zara and Ciara, are affected by the system – the former apparently due to her own wrongful conduct and the latter through malicious application of the system by a shop-owner who has a grudge against her. As there is no information about the consequences for the two individuals of their identification through Facewatch, the fundamental rights assessment focuses on the actual surveillance. For that reason, the assessment produces the same outcome in respect of Zara and Ciara even if one of them presumably was involved in wrongdoing and the other one not.

As to the *right to the protection of personal data*, Facewatch produces a watch list of identified or identifiable persons created by and shared between private entities. The private nature of the surveillance entails that there is less regulation, monitoring and control over the surveillance than in the case of surveillance by public authorities. The surveillance takes place in semi-private space, namely shops, and possibly even in their dressing rooms or bathrooms. It interferes with an aspect of data protection rights which is close to the essential core of protection of personal data (4). The personal data processed does not necessarily contain sensitive information but does carry other personal data. The level of the intrusion is medium (2)(see, Deliverable 2.6, annex 3, p. 81). Due to the existence of clear ECtHR case-law (see Annex 1), these assessments are reliable (1). The resulting intrusion score is 8.

What comes to *the right to privacy*, the face recognition system allows for the identification of criminal suspects and other subjects of interest in the public space and private premises that are accessible to the public. It interferes with the right to privacy. This right has medium importance (2) in the context of the scenario, even without assuming that fitting room or bathroom footage was included. The recording and sharing of identifiable footage of Zara and Ciara occurred without their consent and would not be covered by standard warning signs about the use of CCTV. The intrusion is of at least medium severity (2). Due to the

existence of clear ECtHR case-law (see Annex 1), these assessments are reliable (1). The resulting intrusion score is 4.

## 4 Consolidated Summary and Conclusion

### 4.1. Consolidated Summary of Work Package 2 and Conclusion

This deliverable concludes and summarises the work in SURVEILLE Work Package 2 combining ethical, legal and technical assessment of surveillance technologies. Deliverables D2.1-D2.4 and D2.7 can be seen as laying the groundwork for the framework developed and applied in D2.6, D2.8 and the present D2.9.

Work Package 2 began with work by TU Delft overviewing 43 technologies in deliverable D2.1. These 43 technologies were selected with the objective of illustrating the variety of different kinds of technology that are accommodated under the label 'surveillance technology', to produce an information sheet summarising known information about the technology. As a piece of technical research it also began the process of exploring possible approaches for classification of different surveillance technologies, including by their cost effectiveness (this overview was then updated in deliverable D2.7). The next kind of analysis conducted in Work Package 2 was carried out with the ethics partners with input from the policing end users. The policing end users commented on the technology sheets outputted by D2.1, offering as feedback their own assessments as to the technology's effectiveness, and, for the specific purposes of D2.2, its 'intrusiveness' and any other ethical or legal issues. On the basis of this and further police end user input and the moral analysis in the previous DETECTER project, D2.2 outlines a framework identifying the moral risks of surveillance technology in the prevention of serious crime, and for justifying the taking of these moral risks, primarily based around the urgency of preventing threats to life and human welfare. D2.3 engaged a second and different kind of end-user partner, the European Forum for Urban Security, EFUS. This deliverable provided an overview of surveillance technologies used by local authorities, the reasons for using these technologies, and a brief discussion of the technologies' effectiveness, and the ethical and legal aspects of using them. D2.4 presented the initial legal analysis and began the process of developing means to categorise surveillance technologies by their risk to fundamental rights, by direct reference to the

Charter of Fundamental Rights of the European Union. This deliverable considered the potential intrusiveness of surveillance technology into a wide range of fundamental rights: non-discrimination, privacy, expression and information, data-protection, thought, conscience and religion, assembly and association, freedom of movement, human dignity, liberty and security, health, equality, fair working conditions, effective remedy and fair trial, and prohibition of torture, inhuman and degrading treatment.

The work of combining all ethical, technical and legal research was mainly carried out in the subsequent deliverables D2.6, D2.8 and D2.9. One very important device developed for the combining of the three assessments was the development of fictional but realistic scenarios of the use of surveillance technologies and other techniques in investigation of serious crime, in counter-terrorism and by local authorities. These scenarios narrowed down both the range of technologies considered and provided a specific context of use to analyse. First D2.6 developed the matrix technique for combining these assessments visually in a single table, a matrix of surveillance technologies. As outlined in sections 2.2.1-2.2.3 of that deliverable, means for summarising technical, legal and ethical assessments were set by TU DELFT, EUI and UW respectively.

The analysis of D2.6 focused on a fictional but realistic scenario involving serious organised crime. At different stages over time in the scenario a range of different surveillance technologies were used. Of the three matrix deliverables, the findings of D2.6 arguably showed the greatest degree of variation in usability, ethical riskiness and intrusiveness into fundamental rights amongst the different technologies surveyed. The use of a number of technologies used to detect specific substances were found to raise no ethical risks and rated low on their intrusiveness into fundamental rights. These 'unrisky' technologies included some of the best scoring technologies in relation to usability. At the other end of the scale the ethical and legal analysis agreed in finding the use of bugging equipment the 'worst' kind of surveillance, severely intrusive ethically and scoring the maximum score of '16' for its intrusions into the fundamental rights to data protection and privacy. The 'best' technologies from the point of view of technical usability varied between technologies of different levels of intrusiveness. The very best was judged to be the use of photography in

public places, scoring a '9', judged to raise intermediate risks of privacy and damage to trust, and risks to fundamental rights to privacy and data protection of '8' and '2' respectively. After photography, the next best technically rated technologies all scoring '8' were a mix of the very risky – bugging equipment and a mobile phone tap – and the very low risk – a gas chromatography drugs detector. Overall, the deliverable concluded by dividing up the uses of technologies between seven cases where the use of surveillance could be classified as 'justified', three cases where the use was classified as 'suspect', four cases where the use was judged 'highly suspect' and finally five cases judged to be 'legally impermissible'.

By contrast the findings of D2.8 were more critical, by all three measures. D2.8 concerned a counter-terrorism scenario largely involving surveillance of online communications. The scenario also included two instances of non-technological surveillance – a bag search at an airport and the deployment of a surveillance team. The use of these non-technological techniques were the only cases which could be considered 'justified' on the basis of the framework developed in D2.6. The range of technologies for monitoring online communications, however, was so problematic from the perspective of technical usability, ethical risk and fundamental rights intrusiveness that none were 'justified'. Three out of the four Internet monitoring technologies scored a '5', '5' and a '4' from the perspective of technical usability, were regarded as unjustifiable from the perspective of ethics, and were found 'legally impermissible'. The one Internet monitoring technology not considered impermissible – the social networking analysis – was 'highly suspect' going by the framework of D2.6.

### 4.2. Conclusion

Compared with D2.6, D2.9 does not cover such a wide range of technologies between very low risk and very risky technologies. Also the Local Authority scenario overwhelmingly consists of techniques and technologies of a less intrusive and risky nature than were examined in the counter-terrorism scenario. This is not to say that all the technologies across the board are less risky: in D2.8 the use of the baggage scanner was considered minimally intrusive, certainly much less intrusive than the social media analysis used above

in D2.9. However, the surveillance purposes of local authorities in general would justify far less in the way of intrusive techniques. This is not to say that they are less important, simply that the purposes are very different. The surveillance responsibilities of local authorities overwhelmingly concern public spaces – none of their requirements justify penetrating the privacy entitlements of the home, for example, as is the case, albeit still exceptionally, with serious crime and counter-terrorism.

The fundamental rights assessments conducted in this deliverable complement in important ways the work reported earlier in D2.6 and D2.8. In seven out of ten surveillance situations discussed in the current paper, the use of surveillance for urban security purposes could be regarded as *justified*, due to the absence of grave ethical concerns (red alerts) or very high fundamental rights intrusion scores. This would relate to items 1, 5, 6, 7 and 9, and also items 3 and 4 under the assumption that the purpose limitation principle was respected concerning police access to the data. Two surveillance methods, social media analysis (item 2) and the use of a video camera mounted on a drone (item 8) would be assessed as *highly suspect* due to the high levels of fundamental rights intrusion, resulting in higher scores than those given for usability. In one situation the assessments suggest that the surveillance in question is *legally impermissible*, namely the sharing of CCTV images between private businesses, recorded in their own semi-private premises (item 10). General observations of the urban security scenario are that both the ethical risks and the fundamental rights intrusions were lower than in the earlier two scenarios and that the usability scores also were often quite low. Even if the adverse consequences are less drastic, proper justification is nevertheless required for the use of surveillance technologies in the fairly low-key threat environment of urban security.

The most controversial aspects of local authority surveillance pertain to encroachments on the default entitlement to privacy in public, both ethical and legal. These entitlements were explored in greater depth in SURVEILLE deliverables D4.8 and D4.9. Three emerging technologies in particular raise important risks in relation to privacy in ostensibly 'public' spaces.

'Locational privacy' is arguably put at risk by the use of ANPR and travel data. This is not just a matter of the uses to which this data is put (although many uses such data are put to have a direct impact on privacy). However, simply by virtue of this information being collected, a risk that others will be able to use this data to invade a subject's privacy is established. This risk may be an entirely manageable one, but any city deciding to collect such data has a responsibility to do so. On top of this, certain uses are inevitably intrusive – police access for finding out a suspect's movements, for example. Such a use can be justified, but only within a legal framework controlling that use. This legal framework in many jurisdictions throughout Europe continues to be found wanting.

People use social networking services for a range of different communications purposes, often without a very sophisticated grasp of privacy settings, and how exposed their seemingly discreet conversation may be in reality. Those people still have an interest in and entitlement to privacy. Perhaps less of an entitlement than the person who does so having taken the step holding the conversation 'behind closed doors' in a closed source environment. Actually reading the content of conversations on social networks is not the only ethically risky use that can be made of this data. Software like the Cybels product considered above can mine the activity for useful information about social interaction. This information has a legitimate policing function in situations where criminal activity of a sufficiently serious level is being planned and carried out at great speed, such as in the case of the London riots of August 2011.

A third emerging surveillance technology used by local authorities which poses these kinds of dilemmas are unmanned aerial vehicles. The scenario use of these focuses on a case where persistent scrutiny of any one individual is unlikely because of the large numbers of people and the urgency of spotting security incidents. However, as established in SURVEILLE deliverable D2.6. which considered the use of UAVs in a targeted investigatory context, the use of these can be very intrusive indeed, effectively covert because they may be difficult to notice, and able to penetrate the privacy of areas like gardens and rooftops where people expect another's observation to be impossible.

In all these cases the ethical risks posed by the use of these technologies may appear to receive additional legitimation if citizens democratically endorse local government surveillance policy. However, as will be further discussed in deliverable D4.10, the privacy interests in not being covertly observed are very high, and cannot be considered to have been overridden by majority preference.

## ANNEX 1: Fundamental Rights Assessment Sheets

| A scenario for the use of surveillance technologies by local authorities as input for SURVEILLE deliverable D 2.9 "Assessment of surveillance technologies used by local authorities" | | | |
|---|---|---|---|
| | ***Surveillance technology: 1. The PredPol system*** | | |
| | Arnold has carried out a number of thefts of car radios over the previous two years in and around the suburb of Wysteria in the city of X and has not been apprehended by law enforcement. The thefts have been reported and are aggregated with similar crimes as data inputted into the PredPol system. The PredPol system predicts a higher likelihood of further car radio thefts in certain streets of Wysteria, and on this basis the decision is taken to deploy additional police to the area to look out for this type of crime. Bill, another citizen, is walking through Wysteria on his way to the city centre and stops when he hears the sound of breaking glass. He turns around and sees a parked car with a broken window. While looking into the car a deployed police officer, sent to the street on the basis of the PredPol data, arrives. The police officer sees Bill with his hand in the window of a car, whilst the car's radio is still in place in the vehicle. The police officer arrests him on suspicion of attempted theft. | | |
| **Affected individuals** | **a) all individuals in the targeted area and b) Bill in particular** | | |
| **Fundamental right involved** | **Privacy** | **Data protection** | **Other fundamental rights: Nondiscrimination** |
| **Importance of the right** | Interferes with periphery of the right to privacy due to the increased police presence (1) | No personal data of victims, offenders, or law enforcement is collected. Right to the protection of personal data does not apply. | Non-discrimination, 2 medium because it could lead to control more tightly people residing in poor and segregated neighbourhoods, where crime rates are higher, to be exposed to tighter controls. Predpol may also lead to subconcious de facto profiling based on ethnicity. |
| | ***Score 1*** | ***Score: 0*** | ***Score: 2*** |
| **Degree of intrusion** | Intrusion is weak (1) since the Predpol system influences privacy only indirectly. | No intrusion | Weak (1) since the argument concerning the possible profiling is merely a presumption and can be countered by proper training of the police force. |
| | ***Score: 1*** | ***Score: 0*** | ***Score: 1*** |
| **Relevant case law & certainty of law** | No case law strictly applicable | Not relevant | No case law strictly applicable |
| | ***Score 3/4*** | ***Score:0*** | ***Score:3/4*** |
| **Total Score** | **3/4** | **0** | **1,5** |
| Disclaimer: Judicial authorization would reduce all fundamental rights intrusion scores by a multiplier of 3/4 but is not applicable here, as there was no judicial authorisation. Any intrusion in fundamental rights, even where the score is low, would be deemed impermissible if there was no proper legal basis for it, meeting the requirements of clarity and precision. We are assuming that a proper legal basis exists for all the measures. | | | |

| A scenario for the use of surveillance technologies by local authorities as input for SURVEILLE deliverable D 2.9 "Assessment of surveillance technologies used by local authorities" | | | |
|---|---|---|---|
| | ***Surveillance technology: 2. Thales Cybels social media analysis*** | | |
| | The Thales Cybels intelligence system analyses the open source social media postings of a number of individuals known to police as suspected of conspiring to cause disorder on previous occasions. One of these is Celine, who the social networking analysis reveals is in regular contact with David on political topics, including on the subject of today's demonstration. A number of the messages between Celine and David include criticism of police management of this and similar demonstrations. All of these messages to David are flagged up as meriting attention. Today, for the first time Celine uploads a message to a Facebook group suggesting that a number of people should try to break into the local party offices of the government party whose policies are being protested – this is an open Facebook group, potentially visible to anyone. David is one of 10 others agreeing that this is a good idea, but without expressing any specific commitment to participating himself. Extra police are assigned to the route as it passes by the party headquarters. A group of about 50 people, including Celine, David and Emily gather near the party headquarters. The police ask that they disperse or continue to the official site of the protest, the overwhelming majority of the 50 gathered near party headquarters remain and the situation evolves into a confrontation with police. All the protesters congregating outside the party headquarters are arrested. | | |
| **Affected individuals** | **a) all individuals known to police as suspected of conspiring to cause disorder on previous occasion communicating via social media, b) all demonstrators c) Celine and David in particular** | | |
| **Fundamental right involved** | **Privacy** | **Data protection** | **Other fundamental rights: Liberty** |
| **Importance of the right** | Analysis social network site activity falls within the ambit of both 'private life' and 'correspondence' in relation to ECHR Article 8. The use of social network analysis interferes with the right to the protection of personal data. This technology affords scope for an agency to conduct systematic and widespread surveillance activity. The ECtHR has articulated in its prior judgments that the scope of covert intelligence gathering needs to have a clear and precise basis for it to be conducted in a lawful manner, else it risk abuse and arbitrary application. The importance of privacy in this context is intermediate (2) | As the individual concerned may be identified from the data collated, processed and analyzed, the social network analysis amounts to a processing of personal data. As the data includes sensitive personal data - such as political opinion, the importance of data protection is intermediate, even if the data is collected from publicly available sources (2). | Freedom of assembly, freedom of expression, freedom of association are all affected but this impact can be assessed through a full assessment of privacy and data protection as no higher score would result in respect of these other rights. The question about the right to liberty of a person is different, as there were arrests, i.e. deprivation of liberty which is a severe interference with the right to liberty of the person. Any arrest affects the core area of the right to the liberty of the person. The importance of liberty in that context is high (4). |
| | **Score: 2** | ***Score:2*** | ***Score: 4*** |
| **Degree of intrusion** | Utilization of social network analysis targets a wide range of communications between individuals. The systematic collection of this data and the fact that it subsequently used without the user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance. In this case, the intrusive aspect of surveillance is further intensified by the fact that surveillance is targeted to a group of individuals. The intrusion is serious (4) | The use of social network analysis interferes with the right to the protection of personal data. This technology affords scope for an agency to conduct systematic and widespread surveillance activity. The ECtHR has articulated in its prior judgments that the scope of covert intelligence gathering need have a clear and precise basis for it to be conducted in a lawful manner, else it risk abuse and arbitrary application.The databases contains information innocent persons and their political opinions. The intrusion is serious (4) | The arrests of those demonstrators who have not used force to break trhough the police cordon and who have not engaged in violent scuffles, are without proper justification and hence arbitrary. Arbitrary arrest is a serious intrusion into the right to liberty of the person. (4) |
| | **Score: 4** | ***Score:4*** | ***Score: 4*** |
| **Relevant case law & certainty of law** | Joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others. The assessment is reliable. | Joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others, Weber and Saravia v. Germany (dec.), no. 54934/00, ECHR 2006-XI. The assessment is reliable. | The key purpose of Article 5 of the ECHR is to prevent arbitrary or unjustified deprivations of liberty (McKay v. the United Kingdom [GC], § 30). Given that Art. 52 (3) CFREU stipulates that ECHR is minimum standard, these considerations by the ECtHR also apply within the EU legal order.The assessment is reliable. The score is multiplied by 3/4 because of judicial review. |
| | ***Score: 1*** | ***Score: 1*** | ***Score: 3/4*** |
| **Total Score** | **8** | **8** | **12** |
| Disclaimer: Judicial authorization would reduce all fundamental rights intrution scores by a multiplier of 3/4 but is not generally applicable here, as there was no judicial authorisation for surveillance. However, it is assumed that the arrests are subject to prompt judicial review. Any intrusion in fundamental rights, even where the score is low, would be deemed impermissible if there was no proper legal basis for it, meeting the requirements of clarity and precision. We are assuming that a proper legal basis exists for all the measures. | | | |

| A scenario for the use of surveillance technologies by local authorities as input for SURVEILLE deliverable D 2.9 "Assessment of surveillance technologies used by local authorities" | | | |
|---|---|---|---|
| | ***Surveillance technology: 3. Automatic number plate recognition (ANPR)*** | | |
| | Gary's numberplate is logged and analysed by the ANPR system as he drives into the inner city area where he lives. Helen is travelling from her home outside the city in to the city centre area to join the protest and her numberplate information is logged and analysed as well, and some time later she is charged the congestion tax. As with all ANPR records gathered in City X, the details of Gary and Helen's journeys remain stored and accessible by police for a period of two years and then are deleted. The ANPR system provides exhaustive lists of all the vehicles going through the zone. This information is crossed with information linked to the vehicle and its owner . | | |
| **Affexted individuals** | **a) all individuals moving with cars and b) Helen and Gary in particular** | | |
| **Fundamental right involved** | **Privacy** | **Data protection** | **Other fundamental rights** |
| **Importance of the right** | According to established case law by 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, 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. Given that Art. 52 (3) CFREU stipulates that ECHR is minimum standard these considerations by the ECtHR also apply within the EU legal order. The importance of the right is medium (2) | The access of the competent national authority to the licence plate data. As this entails the processing of personal data, it constitutes an interference with the protection of personal data. However, no sensitive data is involved. The importance is medium (2) | Freedom of movement, freedom of religion, freedom of association are affected but the privacy and data protection assessments are capable of capturing this impact, as no higher scores would result for these rights. |
| | ***Score: 2*** | ***Score: 2*** | ***Score:*** |
| **Degree of intrusion** | Location data as such is not sensitive personal information. However, if the police has unlimited access to the data, contrary to the purpose limitation principle, then their access to location data will represent a significant intrusion in the privacy rights of the individual and will affect his or her choices where to go (e.g. a mosque or a gay club). If police access to the data is limited to the enforcement of the congestion charge, the intrusion is low (1). If police access is unlimited, over a period of two years, the intrusion becomes severe (4). | Location data as such is not sensitive personal information. However, if the police has unlimited access to the data, contrary to the purpose limitation principle, then their access to location data will represent a significant intrusion in the privacy rights of the individual and will affect his or her choices where to go (e.g. a mosque or a gay club). If police access to the data is limited to the enforcement of the congestion charge, the intrusion is low (1). If police access is unlimited, over a period of two years, the intrusion becomes severe (4). | Impact upon freedom movement is included in privacy assessment. |
| | ***Score 1-4*** | ***Score: 1-4*** | ***Score:*** |
| **Relevant case law & certainty of law** | The existing case-law by the ECtHR (Uzun v. Germany , 35623/05) and other authoritative bodies, including the judgment of the CJEU on the invalidity of the data protection directive, provides a reliable basis for these assessments. See, Joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others; Uzun v. Germany , 35623/05. | The existing case-law by the ECtHR (Uzun v. Germany , 35623/05) and other authoritative bodies, including the judgment of the CJEU on the invalidity of the data protection directive, provides a reliable basis for these assessments. See, Joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others; Uzun v. Germany , 35623/05. | Impact upon freedom movement is included in the privacy assessment. |
| | ***Score: 1*** | ***Score:1*** | ***Score:*** |
| **Total Score** | **2 or 8** | **2 or 8** | |
| Disclaimer: Judicial authorization would reduce all fundamental rights intrusion scores by a multiplier of 3/4 but is not applicable here, as there was no judicial authorisation. Any intrusion in fundamental rights, even where the score is low, would be deemed impermissible if there was no proper legal basis for it, meeting the requirements of clarity and precision. We are assuming that a proper legal basis exists for all the measures. | | | |

| A scenario for the use of surveillance technologies by local authorities as input for SURVEILLE deliverable D 2.9 "Assessment of surveillance technologies used by local authorities" | | | |
|---|---|---|---|
| | ***Surveillance technology: 4. RFID*** | | |
| | Ida travels by bus from his home in Wysteria to a coffee shop in West Heath, a suburb on the other side of town where she meets John. Both then travel on the metro to the demonstration. All of Ida and John's travel is logged and automatically processed by software which provides the command centre with the information about passenger congestion. Ida's travel remains potentially identifiable to her as she has used a season ticket registered to her name and address. John buys a new travel card on the day which he retains for further use. | | |
| **Affected individuals** | **Ida & John** | | |
| **Fundamental right involved** | **Privacy** | **Data protection** | **Other fundamental rights** |
| **Importance of the right** | 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, 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. The importance of the right is medium (2) | The access of the competent national authority to the ticket data falls within the scope of the right to the protection of personal data. Personal data is processed but no sensitive data is involved. The importance of the fundamental right is medium (2) | Freedom of movement is affected but the privacy and data protection assessments are capable of capturing this impact, as no higher scores would result for this right. |
| | **Score: 2** | ***Score:2*** | |
| **Degree of intrusion** | If the police has unlimited access to the RFID data, contrary to the purpose limitation principle, then their access to location data will represent a significant intrusion in the privacy rights of the individual and will affect his or her choices where to go (e.g. a mosque or a gay club). If police access to the data is limited to monitoring of use of public transport, the intrusion is low (1). If police access is unlimited the intrusion becomes severe (4). | If the police has unlimited access to the RFID data, contrary to the purpose limitation principle, then their access to location data will represent a significant intrusion in the privacy rights of the individual and will affect his or her choices where to go (e.g. a mosque or a gay club). If police access to the data is limited to monitoring of use of public transport, the intrusion is low (1). If police access is unlimited the intrusion becomes severe (4). | Impact upon freedom movement is included in the privacy assessment. |
| | **Score: 1-4** | ***Score:1-4*** | ***Score:*** |
| **Relevant case law & certainty of law** | The existing case-law by the ECtHR and other authoritative bodies, including the judgment of the CJEU on the invalidity of the data protection directive, provides a reliable basis for these assessments. See, Joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others, Kennedy v. United Kingdom, Weber and Saravia v. Germany (dec.), no. 54934/00 | The existing case-law by the ECtHR (Uzun v. Germany , 35623/05) and other authoritative bodies, including the judgment of the CJEU on the invalidity of the data protection directive, provides a reliable basis for these assessments. See, joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others, Weber and Saravia v. Germany (dec.), no. 54934/00. | |
| | ***Score: 1*** | ***Score:1*** | ***Score:*** |
| **Total Score** | **2 or 8** | **2 or 8** | |
| Disclaimer: Judicial authorization would reduce all fundamental rights intrusion scores by a multiplier of 3/4 but is not applicable here, as there was no judicial authorisation. Any intrusion in fundamental rights, even where the score is low, would be deemed impermissible if there was no proper legal basis for it, meeting the requirements of clarity and precision. We are assuming that a proper legal basis exists for all the measures. | | | |

| A scenario for the use of surveillance technologies by local authorities as input for SURVEILLE deliverable D 2.9 "Assessment of surveillance technologies used by local authorities" | | | |
|---|---|---|---|
| | ***Surveillance technology: 5. CCTV*** | | |
| | The CCTV records Kezia, who is walking to the event, and stops to greet and talk with a number of friends she happens to meet along the way, some of whom are also going; Leonard, who is seen involved in a number of separate brief, violent scuffles (with Mary, Max and Melissa); and Neil, who closely resembles a 'known trouble maker' by the name of Niall, who is reported to have taken part in violence and to often carry a knife. Niall has previously engaged in fights at protests before.<br><br>Kezia is watched fleetingly and occasionally by a series of different viewers keeping a general eye on the crowd. Leonard's initial scuffle draws the attention of an operator who watches him until a policeman arrives who has been directed to investigate the incident. The policeman arrests Leonard on suspicion of assault. Neil is watched by a third operator who mistakes him for Niall. The operator sends a policeman to investigate further when he sees 'Niall' congregating with a number of other 'known trouble makers'. The policeman questions Neil and searches him suspecting he might be carrying a knife. When the search yields nothing Neil is free to go and continues on his journey. | | |
| **Affected individuals** | **Neil, Kezia, Leonard, Niall** | | |
| **Fundamental right involved** | **Privacy** | **Data protection** | **Other fundamental rights: Liberty** |
| **Importance of the right** | Neil: a pat search of Neil's clothes interferes with an aspect of privacy which is of medium importance (2) ; Watching of Kezia in public place interferes weakly with privacy (1) | CCTV merely records individuals in a public place. Presuming the system does not use a database of individually identifiable data, the importance of the fundamental right is weak (1) See, Deliverable 2.6, annex 3, p. 81. For the same reason, there is no data protection issue in respect of Niall who apparently is just by coincidence known to the individual CCTV operator, without the existence of any database on "trouble makers". | Leonard's liberty is deprived by arrest for a short period of time which affects a central dimension - the core - of the liberty of the person. (4). |
| | **Score: 2** | ***Score:1*** | ***Score: 4*** |
| **Degree of intrusion** | Searching of Neil constitutes medium (2) intrusion. Watching of Kezia and Neil intrudes weakly (1) on private life. | CCTV records individuals in a public place and the data is used for police purposes. The intrusion is medium (2) See, Deliverable 2.6, annex 3, p. 81. | As Leonard's arrest is based on his violent conduct that may constitute a crime, it is not an arbitrary deprivation of liberty. Hence, even if it touches a central dimension of the right to liberty of the person, the depth of the intrusion is light (1) |
| | **Score: 2** | ***Score:2*** | ***Score: 1*** |
| **Relevant case law & certainty of law** | Wainwright v. The United Kingdom, 12350/04; P. G. and J. H. v. The United Kingdom, n. 44787/98; Amann v. Switzerland, n. 27798/95 Rotaru v. Romania, n. 28341/95; Peck v. The United Kingdom, n. 44647/98. Given that Art. 52 (3) CFREU stipulates that ECHR is minimum standard, these considerations by the ECtHR also apply within the EU legal order. The assessments are reliable. | P. G. nd J. H. v. The United Kingdom, n. 44787/98; Amann v. Switzerland, n. 27798/95 Rotaru v. Romania, n. 28341/95; Peck v. The United Kingdom, n. 44647/98. Given that Art. 52 (3) CFREU stipulates that ECHR is minimum standard, these considerations by the ECtHR also apply within the EU legal order. The assessments are reliable. | The key purpose of Article 5 of the ECHR is to prevent arbitrary or unjustified deprivations of liberty, McKay v. the United Kingdom [GC], § 30, 543/03). Given that Art. 52 (3) CFREU stipulates that ECHR is minimum standard, these considerations by the ECtHR also apply within the EU legal order. The assessment is reliable. The score is multiplied by 3/4 because of judicial review. |
| | ***Score: 1*** | ***Score:1*** | ***Score:3/4*** |
| **Total Score** | **4 (Neil), 1 (Kezia)** | **0 (Niall), 2 (others)** | **3 (Leonard)** |
| Disclaimer: Judicial authorization would reduce all fundamental rights intrusion scores by a multiplier of 3/4 but is generally not applicable here, as there was no judicial authorisation for surveillance. However, it is assumed that the arrest of Leonard was subject to prompt judicial review. Any intrusion in fundamental rights, even where the score is low, would be deemed impermissible if there was no proper legal basis for it, meeting the requirements of clarity and precision. We are assuming that a proper legal basis exists for all the measures. | | | |

| A scenario for the use of surveillance technologies by local authorities as input for SURVEILLE deliverable D 2.9 "Assessment of surveillance technologies used by local authorities": Fundamental Rights Intrusion Assessment | | | |
|---|---|---|---|
| | ***Surveillance technology: 6. Smart CCTV*** | | |
| | The smart functions flag up a number of individuals to the CCTV viewers as requiring attention. First Olivia tries to take a shortcut across the motorway while walking in to the city centre. The smart CCTV flags up her presence on the central reservation (where pedestrians are forbidden). A viewer notes her presence, and alerts a local traffic policeman, but she has moved on by the time she could get there. No further action is taken.<br><br>Phillip is walking to the protest past an area with a parked train. He drops his keys, and consequently spends a period of time crouched down next to the train. The smart CCTV flags him up for attention because of the algorithm targeting graffiti. The CCTV viewer thinks he is probably a graffiti vandal and two policemen are sent to investigate, including by questioning Phillip. | | |
| **Affected individuals** | **Olivia, Phillip** | | |
| **Fundamental right involved** | **Privacy** | **Data protection** | **Other fundamental rights** |
| **Importance of the right** | Watching of Olivia and Phillip in the public place interferes with a weak aspect of right to private life. (1) | CCTV merely records individuals in a public place. The importance is of right to protection of personal data is weak (1) See, Deliverable 2.6, annex 3, p. 81. | No issue of deprivation liberty arise from merely questioning of Phillip |
| | **Score: 1** | ***Score:1*** | ***Score: 0*** |
| **Degree of intrusion** | Watching of Olivia and Philip intrudes weakly (1) on private life. | CCTV records individuals in a public place and the data is used for police purposes. The intrusion into data protection rights is medium (2) See, Deliverable 2.6, annex 3, p. 81. | |
| | **Score: 1** | ***Score: 2*** | ***Score: 0*** |
| **Relevant case law & certainty of law** | P. G. and J. H. v. The United Kingdom, 44787/98, Amann v. Switzerland, 27798/95; Rotaru v. Romania, 28341/95; Peck v. The United Kingdom, 44647/98. Given that Art. 52 (3) CFREU stipulates that ECHR is minimum standard, these considerations by the ECtHR also apply within the EU legal order.The assessment is reliable. | Peck v. The United Kingdom, 44647/98; P. G. and J. H. v. The United Kingdom, 44787/98, Amann v. Switzerland, 27798/9; Rotaru v. Romania, 28341/95; S. and Marper v. The United Kingdom, 30562/04 and 30566/04. Given that Art. 52 (3) CFREU stipulates that ECHR is minimum standard, these considerations by the ECtHR also apply within the EU legal order.The assessment is reliable. | |
| | ***Score: 1*** | ***Score:1*** | ***Score:*** |
| **Total Score** | **1** | **2** | **0** |
| Disclaimer: Judicial authorization would reduce all fundamental rights intrusion scores by a multiplier of 3/4 but is not applicable here, as there was no judicial authorisation. Any intrusion in fundamental rights, even where the score is low, would be deemed impermissible if there was no proper legal basis for it, meeting the requirements of clarity and precision. We are assuming that a proper legal basis exists for all the measures. | | | |

| A scenario for the use of surveillance technologies by local authorities as input for SURVEILLE deliverable D 2.9 "Assessment of surveillance technologies used by local authorities": Fundamental Rights Intrusion Assessment | | | |
|---|---|---|---|
| | ***Surveillance technology: 7. Abnormal behaviour CCTV*** | | |
| | The abnormal behaviour detection flags up three people as behaving in a manner of interest for the CCTV viewers. Quentin has an argument where he suddenly raises his hand and strikes someone he was speaking to. Rebecca and Simon do not engage in wrongful action, but nevertheless separately trigger the alert. Rebecca is walking unusually. It is not clear why the smart CCTV categorises Simon's behaviour as unusual. The behaviour of all three is drawn to the attention of a CCTV operator. She sends an officer to investigate Quentin's violent scuffle. Watching Rebecca's unusual walk she concludes that this is what has led to the categorisation and concludes that no further action is needed. Confused by Simon's triggering of the system she asks an officer to investigate to see for himself if anything is wrong. | | |
| **Affected individuals** | **Quentin, Rebecca, Simon** | | |
| **Fundamental right involved** | **Privacy** | **Data protection** | **Other fundamental rights: Nondiscrimination** |
| **Importance of the right** | Watching of Quentin, Rebecca and Simon in a public place interferes with a weak aspect of right to private life. (1) | CCTV merely records individuals in a public place. The importance is of the affected dimension of the right to protection of personal data is weak (1) See, Deliverable 2.6, annex 3, p. 81. | There was no deprivation of liberty in respect of Quentin (0). Rebecca is possibly targeted for more intensive observation because of a disability which indirectly discriminates her and affects a medium-important dimension of the right to non-discrimination (2). |
| | **Score: 1** | ***Score:1*** | ***Score: 2*** |
| **Degree of intrusion** | Watching of Quentin, Rebecca and Simon intrudes weakly (1) on private life. | CCTV records individuals in a public place and the data is used for police purposes. The intrusion is medium (2) See, Deliverable 2.6, annex 3, p. 81. This version of CCTV does not seem to include a pre-existing database of indentifiable individuals which would amount to a more severe intrusion to protection of personal data. | Since the system only alerts about the potential target, the resulting intrusion is Rebecca's equality rights is weak (1) |
| | **Score: 1** | ***Score:2*** | ***Score: 1*** |
| **Relevant case law & certainty of law** | Peck v. The United Kingdom, n. 44647/98, P. G. and J. H. v. The United Kingdom, 44787/98; Amann v. Switzerland, 27798/95 Rotaru v. Romania, n. 28341/95; S. and Marper v. The United Kingdom 30562/04 and 30566/04. Given that Art. 52 (3) CFREU stipulates that ECHR is minimum standard, these considerations by the ECtHR also apply within the EU legal order. The assessment is reliable. | Peck v. The United Kingdom, n. 44647/98; P. G. and J. H. v. The United Kingdom; 44787/98; Amann v. Switzerland, 27798/95 Rotaru v. Romania, 28341/95; S. and Marper v. The United Kingdom 30562/04 and 30566/04. Given that Art. 52 (3) CFREU stipulates that ECHR is minimum standard, these considerations by the ECtHR also apply within the EU legal order.The assessment is reliable. | Glor v. Switzerland, 13444/04; Horváth and Kiss v. Hungary, 11146/11. Given that Art. 52 (3) CFREU stipulates that ECHR is minimum standard, these considerations by the ECtHR also apply within the EU legal order.The assessment is reliable. |
| | ***Score: 1*** | ***Score:1*** | ***Score:1*** |
| **Total Score** | **1** | **2** | **2** |
| Disclaimer: Judicial authorization would reduce all fundamental rights intrusion scores by a multiplier of 3/4 but is not applicable here, as there was no judicial authorisation. Any intrusion in fundamental rights, even where the score is low, would be deemed impermissible if there was no proper legal basis for it, meeting the requirements of clarity and precision. We are assuming that a proper legal basis exists for all the measures. | | | |

| A scenario for the use of surveillance technologies by local authorities as input for SURVEILLE deliverable D 2.9 "Assessment of surveillance technologies used by local authorities": Fundamental Rights Intrusion Assessment | | | |
|---|---|---|---|
| | ***Surveillance technology: 8. UAV with videocamera*** | | |
| | The drone briefly films Tina, a demonstrator, Ugo, a bystander who was not aware of the demonstration in advance and is walking in the other direction, Vanessa, who has been taking part in violent scuffles, and Wayne, who is sunbathing on his roof terrace where he assumes he is not visible to view, are all filmed by the drone. In most of the footage they are unidentifiable, and none are scrutinised more than fleetingly. All four see and are aware of the drone. | | |
| **Affected individuals** | **Tina, Ugo, Vanessa and Wayne** | | |
| **Fundamental right involved** | **Privacy** | **Data protection** | **Other fundamental rights** |
| **Importance of the right** | Wayne: Watching of (presumably) naked individuals in a private place is interferes with an aspect of private life which is close to the core of the right (4). Tina, Ugo & Vanessa:: Watching of individuals in a public place affects dimension of private life that is of minor importance (1). | Tina, Ugo & Vanessa: camera merely records individuals in a public place. Presuming the system does not use a pre-existing database of individually identifiable data, the importance of data protection is weak (1) See, Deliverable 2.6, annex 3, p. 81. Wayne: Covert recording of an individual's (presumably) naked appearance in private premises entails processing of sensitive personal data (4) | Tina: The watching of demonstrations with drones interferes with the freedom of assembly and freedom of association. The importance of these fundamental rights in this context is medium (2) |
| | **Score: 4** | ***Score: 4*** | ***Score: 2*** |
| **Degree of intrusion** | Wayne, Tina, Ugo. Because of the covert surveillance, the degree of intrusion to privacy is intermediate. (2) | Camera records individuals in a public place and the data is used for police purposes. The intrusion is medium (2) See, Deliverable 2.6, annex 3, p. 81. | The intrusion is intermediate (2) |
| | **Score: 2** | ***Score:2*** | ***Score: 2*** |
| **Relevant case law & certainty of law** | Peck v. The United Kingdom, 44647/98; P. G. and J. H. v. The United Kingdom, 44787/98; Amann v. Switzerland, 27798/95 Rotaru v. Romania, 28341/95; S. and Marper v. The United Kingdom, 30562/04 and 30566/04. Given that Art. 52 (3) CFREU stipulates that ECHR is minimum standard, these considerations by the ECtHR also apply within the EU legal order.The asssessments are reliable. | Peck v. The United Kingdom, 44647/98; P. G. and J. H. v. The United Kingdom, 44787/98; Amann v. Switzerland, 27798/95; Rotaru v. Romania, 28341/95; S. and Marper v. The United Kingdom, 30562/04 and 30566/04. Given that Art. 52 (3) CFREU stipulates that ECHR is minimum standard, these considerations by the ECtHR also apply within the EU legal order.The assessments are reliable. | Djavit An v. Turkey, no. 20652/92, § 56; Oya Ataman v. Turkey no. 74552/01, §§ 7 and 3; Nosov and others v. Russia, 9117/04 10441/04.Given that Art. 52 (3) CFREU stipulates that ECHR is minimum standard, these considerations by the ECtHR also apply within the EU legal order.The assessments are reliable. |
| | ***Score: 1*** | ***Score:1*** | ***Score:1*** |
| **Total Score** | **8 (Wayne), 2 (others)** | **8 (Wayne), 2 (others)** | **4 (Tina)** |
| Disclaimer: Judicial authorization would reduce all fundamental rights intrusion scores by a multiplier of 3/4 but is not applicable here, as there was no judicial authorisation. Any intrusion in fundamental rights, even where the score is low, would be deemed impermissible if there was no proper legal basis for it, meeting the requirements of clarity and precision. We are assuming that a proper legal basis exists for all the measures. | | | |

| A scenario for the use of surveillance technologies by local authorities as input for SURVEILLE deliverable D 2.9 "Assessment of surveillance technologies used by local authorities" | | | |
|---|---|---|---|
| | ***Surveillance technology: 9. UAV with thermal camera*** | | |
| | The thermal camera films Xandra as part of the crowd, though she is not identifiable. In passing it also picks up the form of Yuri, who is inside his home, and has an illegal cannabis greenhouse. Neither sighting is acted upon in the command centre. | | |
| **Affected individuals** | **Xandra, Yuri** | | |
| **Fundamental right involved** | **Privacy** | **Data protection** | **Other fundamental rights** |
| **Importance of the right** | With regard to Xandra: Covert watching of individuals in a public place interferes with a weak aspect of private life. However, because of the use of thermal camera, the the interference is lightly heavier (1) ; with regard to Yuri; Watching of individuals in home is interferes with an aspect of private life which of intermediate importance. (2) | The thermal camera merely records the crowd in a public place. Presuming the system does not use a pre-existimg database of individually identifiable data, the importance of data protection rights at issue is weak (1) See, Deliverable 2.6, annex 3, p. 81.); With regard to Xandra, since there is no identifiable personal information collected, there is no issue about the protection of personal data (0).The case of Yuri is different, as he is in private space (at his home) and identifiable by combining the footage from the thermal camera with other data such as his home address. A medium-importance dimension of data protection rights is affected (2) | |
| | **Score: 1-2** | ***Score: 0,1 or 2*** | |
| **Degree of intrusion** | Yuri: Because of the covert surveillance of home, the degree of intrusion to privacy is intermediate. (2) | The thermal camera records individuals in a public place and the data is used for police purposes. The intrusion is medium (2) See, Deliverable 2.6, annex 3, p. 81. Even if Yuri is in a private place and the weight of his data protection rights is therefore higher, the intrusion is the same and on medium level (2) | |
| | **Score: 2** | ***Score:2*** | |
| **Relevant case law & certainty of law** | Peck v. The United Kingdom, 44647/98; P. G. and J. H. v. The United Kingdom, 44787/98, Amann v. Switzerland, 27798/95; Rotaru v. Romania, 28341/95; S. and Marper v. The United Kingdom, 30562/04 and 30566/04. Given that Art. 52 (3) CFREU stipulates that ECHR is minimum standard, these considerations by the ECtHR also apply within the EU legal order.The assessments are reliable. | Peck v. The United Kingdom, 44647/98; P. G. and J. H. v. The United Kingdom, 44787/98; Amann v. Switzerland, 27798/95; Rotaru v. Romania, 28341/95; S. and Marper v. The United Kingdom, 30562/04 and 30566/04. Given that Art. 52 (3) CFREU stipulates that ECHR is minimum standard, these considerations by the ECtHR also apply within the EU legal order.The asssessments are reliable. | |
| | ***Score: 1*** | ***Score:1*** | ***Score:*** |
| **Total Score** | **4 (Yuri), 2 (Xandra)** | **4 (Yuri), 0 (Xandra), 2 (others)** | **0** |
| Disclaimer: Judicial authorization would reduce all fundamental rights intrusion scores by a multiplier of 3/4 but is not applicable here, as there was no judicial authorisation. Any intrusion in fundamental rights, even where the score is low, would be deemed impermissible if there was no proper legal basis for it, meeting the requirements of clarity and precision. We are assuming that a proper legal basis exists for all the measures. | | | |

| A scenario for the use of surveillance technologies by local authorities as input for SURVEILLE deliverable D 2.9 "Assessment of surveillance technologies used by local authorities": Fundamental Rights Intrusion Assessment | | | |
|---|---|---|---|
| | ***Surveillance technology: 10. Facewatch image sharing*** | | |
| | Zara has carried out a number of wallet thefts in city centre shops, and has been nearly been caught on a number of occasions but there has not been sufficient evidence to press charges. Annwen, a business owner, has seen Zara in the area on a number of occasions when a wallet is pickpocketed on her premises. Today a store security guard tries to stop Zara to search her after a pickpocketing takes place and Zara runs off. Annwen uploads Zara's image to the Facewatch system taken on the shop's CCTV. | | |
| **Affected individuals** | **Zara, Ciara** | | |
| **Fundamental right involved** | **Privacy** | **Data protection** | **Other fundamental rights** |
| **Importance of the right** | The face recognition system allows for identification of criminal suspects in the public space and private premises accessible to the public. Use of facial recognition interferes with Zara's right to respect for private life. This right has medium importance in the scenario context. (2) | An identifiable watchlist created and shared by private entities over subjects of interest interferes with an aspect of data protection rights which is close to the essential core of protection of personal data. (4) | |
| | **Score: 2** | ***Score: 4*** | ***Score: 0*** |
| **Degree of intrusion** | The recording and sharing of identifiable footage of Zara occured without her consent and would not be covered by standard warning signs about the use of CCTV. The intrusion is of at least medium severity (2) | The personal data processed does not contain sensitive information but does carry other personal data. The level of the intrusion is medium (2) See, Deliverable 2.6, annex 3, p. 81. | |
| | **Score: 2** | ***Score: 2*** | ***Score: 0*** |
| **Relevant case law & certainty of law** | Perry v. United Kingdom, 63737/00; P. G. nd J. H. V. The United Kingdom, 44787/98; Amann V. Switzerland, 27798/95; Rotaru V. Romania, 28341/95; Peck V. The United Kingdom, 44647/98. Given that Art. 52 (3) CFREU stipulates that ECHR is minimum standard, these considerations by the ECtHR also apply within the EU legal order.The assessment is reliable. | Perry v. United Kingdom, 63737/00; P. G. nd J. H. V. The United Kingdom, 44787/98; Amann V. Switzerland, 27798/95; Rotaru V. Romania, 28341/95; Peck V. The United Kingdom, 44647/98. Given that Art. 52 (3) CFREU stipulates that ECHR is minimum standard, these considerations by the ECtHR also apply within the EU legal order.The assessment is reliable. | |
| | ***Score: 1*** | ***Score:1*** | ***Score:*** |
| **Total Score** | **4** | **8** | **0** |
| Disclaimer: Judicial authorization would reduce all fundamental rights intruston scores by a multiplier of 3/4 but is not applicable here, as there was no judicial authorisation. Any intrusion in fundamental rights, even where the score is low, would be deemed impermissible if there was no proper legal basis for it, meeting the requirements of clarity and precision. We are assuming that a proper legal basis exists for all the measures. | | | |