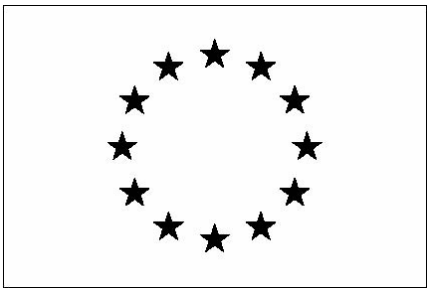


FP7 – SEC- 2011-284725

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 D4.10
Synthesis report from WP4, merging the ethics and law analysis and discussing their outcomes

Due date of deliverable: 28.02.2015
Actual submission date: 07.04.2015

Start date of project: 1.2.2012 Duration: 41 months

SURVEILLE Work Package number and lead: WP04 Martin Scheinin (European University Institute, Florence)

Author(s): Martin Scheinin (European University Institute, Florence) Tom Sorell (University of Warwick)

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

Executive Summary

A. Law

1. The right to privacy (or to a private life) is the human or fundamental right most often and most directly affected by modern surveillance technologies. This right is enshrined, inter alia, in the Universal Declaration of Human Rights (article 12), the European Convention on Human Rights (article 8) and the European Union Charter of Fundamental Rights (article 7).

2. The right to the protection of personal data has emerged from the family of privacy rights and is now recognised either as an attribute of privacy or, as in the EU Charter of Fundamental Rights (article 8), as an independent fundamental right. SURVEILLE work demonstrates that the right to the protection of personal data has added value when assessing the impact of surveillance and needs to be addressed separately from other privacy rights.

3. The use of surveillance technologies may impact upon a whole range of other fundamental rights, including freedom of expression, freedom of association, freedom of assembly, freedom of movement, freedom of religion and the right of non-discrimination. However, SURVEILLE analysis indicates that the right to privacy and its 'sibling right', the right to the protection of personal data, usually are the immediately and directly affected fundamental rights and an assessment under them, when conducted in a holistic manner, can serve as a good proxy for a general fundamental rights assessment.

4. The legal assessment of the use of surveillance technologies must address also so-called collateral impact or third party intrusion, i.e. how other people besides the original target of the surveillance are impacted by surveillance.

5. Surveillance that impacts upon fundamental rights can only be lawful if it is prescribed by law, i.e. if it has a legal basis in European or domestic law that meets the qualitative requirements of any law that interferes with human or fundamental rights, including public nature, precision and foreseeability of application.

6. The impact of the use of a particular surveillance technology upon a fundamental right can be assessed through two main factors: the weight or importance of a fundamental right (or its specific dimension) in a given context, and the depth of the intrusion into that right. The outcome (an initial score) can then be subject to corrections related to: a) the reliability of the assessment, based on the existence of earlier case-law by the highest European courts in the same or similar matters, and b) the question of whether the measure was judicially authorised or subject to judicial review. In SURVEILLE, the outcome is called the 'fundamental rights intrusion score'.

7. A legal assessment of surveillance technologies cannot shy away from the conclusion that some methods of surveillance will be legally impermissible because of the very high degree of fundamental rights intrusion.

8. In other situations, the SURVEILLE methodology takes the outcome of the parallel technology assessment (the usability score) as demonstration of the existence of a legitimate aim that in principle makes surveillance justified. The score itself represents the contribution made by surveillance towards the achievement of the legitimate aim in question. A comparison between the usability score and the fundamental rights intrusion score is then the proper place for a proportionality assessment between the two. This discussion needs to be informed of the outcomes of the parallel ethics assessment and will need to address possibilities of Privacy by Design and other methods to improve the usability score and/or reduce the fundamental rights intrusion score.

9. The SURVEILLE assessment methodology, including the place reserved in it for a proportionality assessment can be applied in a wide range of situations, including when drafting *legislation* on surveillance, when deciding about the *development or deployment* of new surveillance technologies, when deciding about the *authorization* of using a particular surveillance technology, and also in a practical situation of *actual usage* of a technology.

B. Ethics

1. Surveillance is in principle justified by the protection of citizens' vital interests if those interests are genuinely threatened.

2. Citizens have a vital interest in e.g. survival, in being pain-free, in being free of debilitating addiction, and other interests in many other goods that can be distributed to them.

3. Counter-terrorism and the fight against serious crime correspond to vital interests, but the justifiability of a given choice of measures to protect those interests depends on the size and imminence of the threat against them.

4. Preventive operations against terrorism and organized crime involving surveillance need greater justification than prosecutorial operations and investigations.

5. Democracy requires justified surveillance to be as public as possible: there is a presumption against covert surveillance in public places and any surveillance in private places.

6. There are very big tensions between the norms of democracy and the large-scale surveillance of citizenries (as in the NSA programme) even as part of counter-terrorism.

7. There are moral objections against large-scale surveillance in democracies also from considerations of privacy and a heightened threat of loss of liberty.
8. Various political agendas at the level of urban jurisdictions encourage different kinds of surveillance of a local population for the protection of non-vital

interests. These agendas include the devolution of federal power, and the pursuit of greater efficiencies and security through "smart city" technology.

9. Some software that promotes a "smart cities" agenda is potentially very intrusive.

10. There is a risk that technology-based security policies pursued by local government, including various kinds of surveillance, can become disconnected from human rights commitments entered into at a federal level.

Introduction

This paper summarizes a major part of the work done within the FP7 project SURVEILLE (Surveillance: Ethical Issues, Legal Limitations, and Efficiency),[1] the focus here being on the main ethical and legal dimension of the project, the analysis of surveillance techniques or technologies as to the resulting ethical risks and fundamental rights intrusion. The SURVEILLE project itself is multidisciplinary in nature. Most of its consortium partners are universities responsible for the three pillars of academic work represented in the name of the consortium: ethics, law and technology assessment, the last-mentioned pillar being itself multidisciplinary as it utilises the methodologies of engineering sciences, economics and sociology. The consortium also includes two end-user partners, bringing in the experience and expertise of local authorities and the police in the use of surveillance technologies. The project seeks to answer the question whether surveillance technologies, and which ones of them, and in what circumstances, can simultaneously be (a) effective and efficient by delivering better security at an acceptable financial cost, (b) ethically acceptable and (c) legally permissible, in particular in relation to the fundamental rights intrusion that results from surveillance.

In the original project proposal submitted to the European Commission in November 2010, surveillance was defined as "the targeted or systematic monitoring of persons, places, items, means of transport or flows of information, in order to detect specific, usually criminal, forms of conduct, or other hazards, and enable, typically, a preventive, protective or reactive response, or the collection of data for preparing such a response in the future."[2] Geared to a specific topic in the Security Research call of FP7, this definition clearly is intended to relate to surveillance technologies as used in the prevention, investigation and prosecution of terrorism and other crime.

The Annexes represent SURVEILLE background research in Work Package 4, towards this synthesis report.

---

[1] SURVEILLE (Surveillance: Ethical Issues, Legal Limitations, and Efficiency) is a Security Research project coordinated by the EUI in 2012-2015 that has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 284725. See, http://www.surveille.eu

[2] SURVEILLE Description of Work, November 2010.

1. The Law of Surveillance: SURVEILLE Fundamental Rights Intrusion Analysis

1.1 Setting the Scene

1.1.2 Affected human or fundamental rights

Surveillance often affects a number of human rights, constitutional rights or fundamental rights – whatever is the terminology used in a given legal order. To name just a few examples, this is the case with the use of closed-circuit television (CCTV) in public spaces or private premises, traditional interception of telephone calls[3] or the placement of listening devices to monitor suspected criminals, and electronic mass surveillance as disclosed through the revelations by former CIA contractor Edward Snowden.[4]

The immediately and most commonly affected fundamental right is *the right to privacy*, or the right to the protection of private life as it is named in the European Convention on Human Rights (ECHR). The formulations of this right often explicitly refer to 'correspondence' or 'communications' and to 'home', in addition to the notions of 'privacy' or 'private life'. Reference is made to article 12 of the Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights (ICCPR), and article 7 of the EU Charter of Fundamental Rights (EUCFR). Much of the public discourse on surveillance and human rights has on good grounds been formulated as a tension or tradeoff between *privacy vs. security*.[5]

The right to the protection of personal data belongs to the family of privacy rights but has gradually emerged as an independent fundamental right, as is confirmed by its inclusion as a separate article 8 in the EUCFR.[6] To provide a more fine-

[3] For SURVEILLE research on the topic, see Céline Cocq, The impact of terrorism on States with a recent authoritarian past. Analysis of Germany and Spain through the use of interception of telecommunications (submitted for publication); Annex C.

[4] See e.g. Céline Cocq and Francesca Galli, "The use of surveillance technologies for the prevention and investigation of serious crimes" Deliverable 4.1, SURVEILLE project, 31 October 2012; Jonathan Andrew, "Paper on legal issues related to the use of surveillance data for profiling" Deliverable 4.2 SURVEILLE project, 30 April 2014; Michelle Cayford, "Mass Surveillance by the National Security Agency (NSA) of the United States" Deliverable 2.8 SURVEILLE project, 29 May 2014; Mathias Vermeulen, "the scope of the right to private life in public places" Deliverable 4.7, SURVEILLE project, 27 July 2014.

[5] For SURVEILLE research on the challenges new technologies pose to the right to privacy, see, Mathias Vermeulen, New technological challenges to the right to privacy; Annex G.

[6] SURVEILLE project, "Matrix of Surveillance Technologies" Deliverable 2.6, Tom Sorell (leader), 31 July 2013, p. 14 et seq.; see also *e.g.* DLA Piper," The future of online privacy and data protection", *in* the *EU Study on the Legal analysis of a Single Market for the Information Society, New rules for a new age?* November 2009, p. 3; Serge Gutwirth, Ronald Leenes, Paul De Hert and Yves Poullet (eds.), *European Data Protection: Coming from age*, (Dordrecht: Springer, 2013), p. 76 and ff.; Antonella Galetta and Paul De Hert, "A European Perspective on Data Protection and Access Rights" IRISS project, Clive

grained assessment, SURVEILLE research has addressed the right to the protection of personal data separately from the broader right to privacy.

Many other fundamental rights may, depending on the circumstances, be affected by surveillance – either directly or through a 'chilling effect' resulting from a first-order intrusion into privacy rights that also affects peoples' enjoyment or exercise of their other rights. With no intention to be exhaustive, the following human or fundamental rights can be mentioned: *freedom of movement, freedom of association, freedom of assembly, freedom of expression, freedom of thought, conscience and religion, the right not to be discriminated against* (e.g., through surveillance-based profiling), and *the right to liberty of the person.* All of these rights have been consistently recognised as human or fundamental rights in the same instruments that were mentioned above under privacy.

1.1.3 Permissible limitations

The human rights affected by surveillance tend not to be 'absolute' rights, i.e. those that would allow for no restrictions, nor be subject to derogation during a state of emergency threatening the life of the nation, or which constitute norms of *jus cogens*.[7]

As we have shown earlier,[8] states have not in practice resorted to formal derogation, treaty reservations or withdrawal from human rights treaties to legalise or justify their intrusions into privacy rights. Instead, the regime of permissible limitations to human rights appears to be the prevailing paradigm for justifying surveillance that affects privacy rights. Some states, notably the United States,[9] have also resorted to the denial of the extraterritorial effect of human rights treaties when seeking to justify a distinction between 'internal' and 'foreign' communications or interference with submarine fiber-optic cables that carry cross-border telephone and internet traffic.

Norris and Xavier L'Hoiry (leaders), Deliverable 5, Exercising Democratic Rights Under Surveillance Regimes.

[7] When 'profiling' through surveillance constitutes racial discrimination, this would be an exception. Further, we should not rule out the possibility that every human right may contain an inviolable 'essential core' that is absolute in one of the above meanings.

[8] Martin Scheinin and Mathias Vermeulen, 'Unilateral Exceptions to International Law: Systematic Legal Analysis and Critique of Doctrines to Deny or Reduce the Applicability of Human Rights Norms in the Fight against Terrorism, Essex Human Rights Review, vol. 8 (2011) 27-75; Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (Martin Scheinin), UN document A/HRC/13/37.

[9] On this debate, see Scheinin and Vermeulen 2011 (previous footnote); "Electronic Frontier Foundation, "Necessary & Proportionality. International Principles on the application of Human rights Law to Communications Surveillance" May 2014, http://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf (accessed 26 February 2015), p. 2 et seq.

SURVEILLE has focused on surveillance occurring within one nation state or across borders within the EU and therefore safely assumes that fundamental rights, including those included in the EUCFR or those defined in the ECHR as human rights that are legally binding upon all EU Member States even when acting outside EU law, will be applicable as the proper legal framework, which therefore is to be addressed through the paradigm of permissible limitations.

Within that paradigm, there are different variations. One standard approach, reflected in the text of articles 8-11 of the ECHR, is to address the permissibility of restrictions through the three tests of (a) being prescribed by the law, i.e. having a proper legal basis, (b) serving a legitimate aim, and (c) being necessary in a democratic society. Much of the jurisprudence by the European Court of Human Rights (ECtHR) has been written so as to conform to this framework.[10] In practice, it is the third test of being necessary in a democratic society that has proven to be the most demanding one. It includes elements such as the choice of least intrusive measures, the requirement of proportionality and the criterion of staying within a margin of appreciation left for national authorities when addressed in European comparative perspective and subject to evolving understandings of a common European minimum standard. That said, there are also instances when the ECtHR has applied what can be seen as a fourth test, namely the special status of the 'essence' of a human right, a notion that has no counterpart in the text of individual provisions of the ECHR but that can very well be derived from the object and purpose of the ECHR as a whole.

Importantly, the idea of an inviolable essential core has been explicitly incorporated in the general clause on permissible limitations in the EUCFR, where article 52 (1) reads 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."

As can be seen, "provided by law" and "objectives of general interest" (legitimate aim) appear also here as separate tests for the permissibility of limitations. As a variation of the ECHR approach, necessity and proportionality are at least seemingly separate tests. The real addition to the ECHR text is in making the "essence" test explicit.

---

[10] See *e.g.* ECtHR, *Z. v. Finland*, app. n°22009/93, judgement of 25 February 1997, para 95.; *L.L. v. France*, app. n°7508/02, judgement of 10 October 2006, para 43 et seq. *Weber and Saravia* v. *Germany*, app. n°54934/00, admissibility decision of 29 June 2006; *S and Marper v UK* (2009) 48 EHRR 50; See also Céline Cocq and Francesca Galli, "Comparative law paper on data retention regulation in a sample of EU Member States" Deliverable 4.3 SURVEILLE project, 30 April 2013; Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Springer, Heidelberg, 2012.

In SURVEILLE we primarily base our legal assessment on the combined effect of the EUCFR and the ECHR but also look at universal human rights standards such as the International Covenant on Civil and Political Rights (ICCPR). In our earlier work in the FP7 project DETECTER and when entrusted with the mandate of UN Special Rapporteur on human rights and counter-terrorism the approach to permissible limitations on privacy (and other) rights was largely inspired by General Comment No. 27 on freedom of movement, adopted by the Human Rights Committee acting as the independent expert body under the ICCPR. Both in academic work in DETECTER and in a 2009 Special Rapporteur's report on the right to privacy as affected by the fight against terrorism, the following seven-part test for permissible limitations was presented:

(a) Any restrictions must be provided by the law;
(b) The essence of a human right is not subject to restrictions;
(c) Restrictions must be necessary in a democratic society;
(d) Any discretion exercised when implementing the restrictions must not be unfettered;
(e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim;
(f) Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected;
(g) Any restrictions must be consistent with the other rights guaranteed in the ICCPR.[11]

The main methodological challenges facing the fundamental rights intrusion analysis in SURVEILLE have been related on the one hand to a quest for applying a more rigorous permissible limitations test than the standard ECHR three-part test, including the issue how to incorporate the idea of an inviolable essential core in the assessments, and on the other hand to a need for a general European approach, not hampered by the fact that issues of national and public security and hence surveillance measures are largely in the competence of individual Member States. As the scenario-based assessments of specific surveillance technologies in SURVEILLE were conducted without a reference to a specific jurisdiction and national legal order,[12] it was unavoidably difficult or impossible fully to include the 'prescribed by law' test in the analysis. The latter challenge was by and large resolved by including in the intrusion analysis a presumption that a proper legal basis existed for each surveillance measure, this resulting in a caveat in the outcomes that where surveillance would appear permissible, its legal basis would still need to be verified. In addressing the first-mentioned

[11] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (Martin Scheinin), UN document A/HRC/13/37 paragraph 17; Scheinin and Vermeulen (footnote 8) p. 69.
[12] Céline Cocq and Francesca Galli, "The use of surveillance technologies for the prevention and investigation of serious crimes" Deliverable 4.1, SURVEILLE project, 31 October 2012; see also Philippe De Koster, "Analytic Report" *in Terrorism: special investigation techniques,* Council of Europe Publishing, 2007, p. 20.

challenge, we turned to Robert Alexy's theory of fundamental rights for inspiration.

1.1.4 Robert Alexy's Weight Formula

The fundamental rights intrusion analysis in SURVEILLE has been inspired by Robert Alexy but also by his critics.[13] At the outset, the legal research in SURVEILLE accepts that treating fundamental rights *primarily* as principles that are subject to a proportionality assessment and, hence, to a specific, analytically rigorous form of 'balancing', *can be* rational. This cautious approach is very different from political or legal approaches that would accept an *in abstracto* 'balancing' act between, say, privacy and public security under the assumption that a 'tradeoff' between the two is necessary, i.e. better security can only be achieved through giving away some of our privacy. Critiques against 'balancing' for its indeterminacy or irrationality may very well be justified in respect of such abstract and crude approaches to balancing but not necessarily in relation to Alexy's model.

Alexy has formulated the 'law of balancing' as follows: "The greater the degree of non-satisfaction of, or detriment to, one principle, the greater must be the importance of satisfying the other."[14] The link with SURVEILLE research is that under our approach the higher is the *fundamental rights intrusion score*[15] (to the detriment of the right in question), the greater must be the *usability score* (representing an actual, effective and efficient security benefit obtained through the use of a specific surveillance technology in a specific situation). Alexy then moves to semi-quantification of both the fundamental rights interference and the reasons justifying the interference, by using a triadic scale (light, moderate, serious) for both parameters.[16] The outcome is the Weight Formula, which can be presented in simple or complicated forms, for instance as follows:

$$W_{i,j} = \frac{I_i \bullet W_i \bullet R_i}{I_j \bullet W_j \bullet R_j}$$

In Alexy's explanation the Weight Formula, W_i and W_j stand for the abstract weights of the two competing principles P_i and P_j, (which as such are not used in this version of the formula but are represented by their abstract weights) and R_i and R_j "for the reliability of the empirical assumptions concerning what the

[13] For a critical discussion on Alexy's model, primarily in defence of the need to include all-or-nothing *rules* in human rights law, see, Martin Scheinin, 'Terrorism and the Pull of 'Balancing' in the Name of Security' EUI Law Working Paper 11/2009 pp. 55-63.
[14] Robert Alexy, A Theory of Constitutional Rights p. 102 (English translation from the 1985 German original Theorie der Grundrechte, Oxford University Press 2002, including an important postscript); Robert Alexy, 'Constitutional Rights and Legal Systems, in Joakim Nergelius (ed.), Constitutionalism - New Challenges: European Law from a Nordic Perspective, Martinus Nijhoff 2008 pp. 3-15; and Robert Alexy, 'The Construction of Constitutional Rights' Law & Ethics of Human Rights, vol. 4 (2010) pp. 19-32 at p. 28.
[15] SURVEILLE project, "Matrix of Surveillance Technologies" Deliverable 2.6, Tom Sorell (leader), 31 July 2013, p. 9.
[16] Alexy 2010 pp. 28-29.

measure in question means in the concrete case for the non-realization of the one principle and the realization of the other principle". Further, "I_i stands for the intensity of interference with the principle P_i …. I_j stands for the importance of satisfying the competing principle P_j". "Finally the outcome, $W_{i,j}$ stands for the concrete weight of the principle whose violation is being examined—in our case, that of P_i. The Weight Formula gives expression to the point that the concrete weight of a principle is a relative weight. It does this, in the simplest form, by defining the concrete weight as the quotient of the intensity of interference with this principle (P_i) and the concrete importance of the competing principle (P_j)."[17]

In SURVEILLE, Alexy's work has inspired the fundamental rights intrusion assessment where the abstract weight of a fundamental right[18] and the intensity of an intrusion into it through surveillance[19] are both assessed under a triadic scale (low/moderate/serious) and attributed the numerical values 1, 2 or 4.[20] The values are accorded through a careful reading of existing case-law by the ECtHR and the Court of Justice of the European Union (CJEU)[21] in comparable cases and the language used by the two courts to qualify the situation at hand. As the judicial findings are nevertheless extrapolated to new or hypothetical situations of the use of surveillance technologies, Alexy's reliability variable R is in SURVEILLE modified to represent the reliability of existing case law for the purpose of assessing the surveillance technology usage under assessment.[22]

Hence, the fundamental rights intrusion scores determined by the legal expert team in SURVEILLE closely resemble the numerator in Alexy's Weight Formula. But departing from Alexy, the denominator is not determined by the legal scholars but is replaced by a usability score determined by the technology assessment team in SURVEILLE. Instead of assessing the relative weights of two competing principles, SURVEILLE seeks to compare the fundamental rights intrusion against the security benefit (usability) obtained through the use of a particular surveillance technology.

Alexy's answer to the question concerning the absolute protection of the 'essential core' of a fundamental right, applicable as a rule and excluding the possibility of any 'balancing', would be in the fine-tuning of the scale. By defining

[17] Alexy 2010 p. 30.
[18] Variable W in Alexy's Weight Formula.
[19] Variable I in Alexy's Weight Formula.
[20] Alexy 2010 p. 31 where his proposal to use the values 1, 2, 4 is explained in a footnote: "The greatest advantage of the geometric sequence consists in its providing for the best representation of the overproportional increase of the power of rights as correlated with an increasing intensity of interference, a fact that serves as the basis for the refutation of the objection concerning the dissolution of the power of constitutional rights."
[21] See, in particular, Court of Justice of the European Union, Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*; and a case note written by Tuomas Ojanen in the SURVEILLE project, Annex E.
[22] In SURVEILLE, R is given the value 1 (clear and applicable case-law exists), ¾ (in the absence of clearly applicable case-law, the assessment is made through consensus by the legal expert team in SURVEILLE), or ½ (a layperson's opinion).

the weight of the right not to be tortured as serious-serious, one can make sure that it will never be outweighed by a competing principle as its weight will always be lower than serious-serious.[23] In SURVEILLE, we have followed this suggestion by defining the scale of the fundamental rights intrusion score as 0-16, while the highest usability score is 10. While 16 is the outcome of maximal abstract weight (4) multiplied by maximum-intensity intrusion (4), we have also left open the possibility of 'jumping' straight to the final score of 16 when a matter is identified as pertaining to the essential core of a fundamental right.

1.1.5 *Necessity, Proportionality and Justification (Legitimate Aim)*

In Robert Alexy's original Weight Formula, a proportionality assessment between the fundamental right in focus and the competing legitimate aim (e.g., another fundamental right or a collective good such as national security) is built into the equation between the numerator and the denominator. In the SURVEILLE method of intrusion assessment, only the numerator is included in the outcome of the legal assessment, the *fundamental rights intrusion score*. This score is based on the abstract weight of a fundamental right in a given situation and the depth of the intrusion into that right as it results from surveillance, and the initial score is subjected to certain corrective factors.

The separate *usability score*, resulting from the technology assessment, seeks to measure the contribution of a particular surveillance method towards the aim of surveillance, for instance the prevention or investigation of crime, or the protection of public order. Without such a legitimate aim being actually served, there cannot be justification for any surveillance that causes even a slight degree of fundamental rights intrusion. When a legitimate aim has been identified, the usability score seeks to assess the actual benefit generated by the surveillance method in question towards that legitimate aim. Hence, the usability score is itself an expression of the proven necessity of a given method of surveillance towards a legitimate aim that in principle makes its use justified. Hence, the usability assessment incorporates issues of justification (legitimate aim) and necessity. An intrusion into privacy or another fundamental right through the use of a surveillance technique can only be justified, even *prima facie*, if the surveillance is intended to serve an aim that is legitimate (e.g. the prevention or investigation of crime) and actually contributes towards that aim so that it can be deemed necessary in a democratic society. Both factors are inherent in the usability score (does the surveillance method actually work towards its intended goal), while the fundamental rights intrusion score measures the resulting negative impact on rights.

In the SURVEILLE method,[24] the *proportionality* between the actual benefit towards a legitimate aim delivered by surveillance and the resulting

[23] See, Alexy 2008.

[24] For a wider discussion on the methodologies for assessing the impact of technologies upon fundamental rights, developed in SURVEILLE, see: Maria Grazia Porcedda, A Methodology to Explore the Impact of Technologies on Rights; Annex F; Maria Grazia Porcedda, "Paper establishing classification of technologies on the basis of their intrusiveness into fundamental rights" Deliverable 2.4, SURVEILLE project, 30 April

fundamental rights intrusion is assessed by comparing the usability score and the fundamental rights intrusion score, also in light of the outcome of the ethics assessment. In some cases, the usability score will be so low (say, 3 out of 10, or lower) that the necessity of using that particular form of surveillance has not been demonstrated. In some other cases, the fundamental rights intrusion score will be so high (say, the maximum score of 16) that no benefit towards the, as such legitimate, aim of the surveillance can make it justified, as the negative fundamental rights impact would *always* be disproportionate when compared against the actual security benefit. In a third, presumably large, category of situations the usability score is high enough to demonstrate real benefits of the surveillance and hence its prima facie necessity, while the fundamental rights intrusion score at the same time is not manifestly so high as to signal an unavoidable human rights violation. In these situations a comparison between the usability score and the fundamental rights intrusion score will form the starting point for assessing the proportionality of a surveillance measure.

A clearly higher usability score, as compared against the fundamental rights intrusion score, will suggest that the surveillance is proportionate, whereas a clearly higher fundamental rights intrusion score will suggest that the measure is disproportionate. The comparison must, however, also be informed by the ethical risks identified in the ethics assessment, and include consideration of adjustments that might reduce the fundamental rights intrusion or improve the usability score. In particular, in the SURVEILLE methodology, the inclusion of Privacy by Design features has the capacity to both increase the usability score and reduce the fundamental rights intrusion, hence affecting the outcome of the proportionality assessment between the two. Further discussion is presented below in Section 3 and the accompanying Decision Support System illustration where the "holistic overall assessment" phase is the home for the proportionality assessment.

The SURVEILLE assessment methodology, including the place reserved in it for a proportionality assessment, can be applied in a wide range of situations, including when drafting *legislation* on surveillance, when deciding about the *development or deployment* of new surveillance technologies, when deciding about the *authorization* of using a particular surveillance technology, and also in a practical situation of *actual usage* of a technology.

1.2. Results of SURVEILLE Research

SURVEILLE seeks to assess the ethics, law and efficiency of surveillance, particularly in combating terrorism and other crime. To bring together the different disciplines and experiences in the project, we developed three scenarios that emulate real-life situations where surveillance is used. Three separate expert teams were to assess the use of a defined set of surveillance technologies or techniques as applied in each of the three scenarios, as to their

---

2013; SURVEILLE project, "Matrix of Surveillance Technologies" Deliverable 2.6, Tom Sorell (leader), 31 July 2013

moral risks (ethics), fundamental rights intrusion (law) and efficiency (technology assessment). The teams applied their own scoring methodology to assess each individual usage situation. The results were reported in SURVEILLE deliverables D2.6, D2.8 and D2.9.

The methodologies applied within SURVEILLE underwent some developments in the progression from the first to the third scenario. Nevertheless, as the main contours remained stable and as the common elements in the methodologies applied under the three assessments were predominant, it is possible to engage in a common discussion of the findings.

At a joint event convened at the end of October 2014 by the three FP7 projects SURVEILLE, RESPECT[25] and IRISS,[26] a joint policy paper emanating from the work done in the three parallel projects was presented to the European Commission and other policy-makers. In that context, the outcomes of SURVEILLE were reported through the following eight items which here have been revised in light of subsequent work on the third scenario.

1. Surveillance technologies and surveillance methods that target directly prohibited or otherwise dangerous *objects or substances* are to be recommended, including for technology development and deployment. They tend to create less ethical risks or fundamental rights intrusion than surveillance targeting people on account of their real or suspected involvement in prohibited or dangerous activity.

2. The assessments conducted in SURVEILLE demonstrate that *electronic mass surveillance*, including in the forms documented through the Edward Snowden revelations, fails, and fails drastically. It produces at best medium-level usability scores which are overshadowed by a very high degree of ethical risk, combined with levels of fundamental rights intrusion that on their own would make the surveillance legally impermissible under the EU Charter of Fundamental Rights and human rights treaties. In contrast, traditional (non-technological) surveillance measures produce clearly higher usability scores and a much better 'balance' when compared with the resulting fundamental rights intrusion.

3. Although surveillance may affect the enjoyment of a whole range of fundamental rights, including freedom of expression, freedom of association, freedom of assembly, freedom of movement, freedom of religion and the right of non-discrimination, SURVEILLE analysis indicates that *the right to privacy* and its 'sibling right', *the right to the protection of personal data*, usually are the immediately and directly affected fundamental rights. Assessing intrusion into these two rights is usually capable of including also any 'chilling effect' or other impact in relation to other fundamental rights, provided that third-party intrusion is included in the assessment. Hence, a proper assessment of impact upon privacy and data protection rights is capable of incorporating the negative

[25] Rules, Expectations & Security through Privacy-Enhanced Convenient Technologies (RESPECT)
[26] Increasing Resilience in Surveillance Societies (IRISS)

effects of surveillance upon other fundamental rights as well. That said, in particular where surveillance leads to law enforcement measures, such as the arrest and detention of individuals, it will be important to maintain a possibility to assess also direct impact upon other fundamental rights.

4. A range of *ethical risks* can be identified in the use of surveillance technologies, including moral risk of error, moral risk of intrusion, moral risk of discrimination, moral risk of damage to trust and of resulting chilling effect, and ethical proportionality. SURVEILLE research demonstrates that different surveillance technologies perform very differently in relation to these ethical risks. While some forms of surveillance pose no ethical risk, others can cause very high degrees of moral risk, which irrespective of any legal analysis should on its own be a source of caution as to their use.

5. One category of surveillance that is particularly suspect both in moral and legal terms and therefore impermissible, is surveillance based on algorithms or on other methods to *'profile'* individuals for targeted surveillance or other fundamental rights intrusions on account of their membership in a racial, ethnic, cultural, religious, political or other group. If selective targeting occurs, it should be based on individual conduct, not inborn characteristics or membership in a group.

6. A distinction between *'content'* (the confidential message passed by the sender to the recipient) and *'metadata'* (information about the parties and about a message being sent and delivered between them) is no longer a determining factor for the assessment of the level of ethical risks or fundamental rights intrusions resulting from surveillance. A combination of various forms of metadata can reveal more confidential and sensitive personal information than the actual content of the message. Justifications of surveillance based on the idea that it relates 'only' to metadata, should be rejected and attention should be given to assess the details, i.e. what types of metadata are at issue and what is their combined effect upon fundamental rights.

7. SURVEILLE assessment of surveillance technologies includes the consideration of *privacy by design* features in the technology. Adequate measures to reduce privacy intrusion and to protect personal data both increase the usability score of a technology and reduce the fundamental rights intrusion score, hence helping to reach an appropriate 'balance'. Parallel to the notion of privacy by design (PbD) SURVEILLE also discusses notions such as minimum harm by design (MHbD), transparency by design (TbD) and accountability by design (AbD).

8. Independently of any 'weighing' or proportionality, or any reference to democratic legitimacy as the source of authority in allowing surveillance, the requirement of a *proper legal basis* for surveillance that affects the enjoyment of fundamental rights by individuals is a separate necessary condition for any surveillance being permissible. Non-existent, vague or secret law, or law not subject to proper oversight, cannot be the basis for lawful surveillance. After the data retention ruling of 8 April 2014 by the EU Court of Justice, there is a need

for meticulous review of EU law and the laws of Member States in order to verify that a proper legal basis exists for every form of surveillance currently in place or under consideration for deployment.

Under the three scenarios examined by SURVEILLE, altogether 35 usage situations of various surveillance technologies or techniques were assessed separately for their ethical risks, fundamental rights intrusion and technological usability (effectiveness and efficiency). The number of technologies was smaller, as in several cases the same technology was used in different contexts. Combining the three parallel assessments and the outcomes presented in deliverables D2.6, D2.8 and D2.9 it can be summarised that in 16 out of 35 situations the surveillance appeared as *justified* in respect of a combination of the three different assessments. In these cases, surveillance was given a high usability score, combined with no major fundamental rights intrusion or major ethical risks. Three situations were categorised as *suspect* when a high usability score was coupled with significant fundamental rights intrusion but no significant ethical risk. Another seven situations were described as *highly suspect*, because of a high degree of fundamental rights intrusion coupled with significant ethical risk. Finally, nine of the 35 usage situations of surveillance technologies were assessed as legally *impermissible*, typically because the fundamental rights intrusion score was clearly higher than the usability score, including cases where the fundamental rights intrusion score was higher than the highest possible usability score.

General observations when comparing the three scenarios are that (1) in the organised crime scenario there was a wide range of outcomes as to the justified, suspect or impermissible nature of the surveillance technologies applied, while (2) in the terrorism prevention scenario the selected surveillance methods – in many cases indiscriminate methods of electronic mass surveillance – tended to render the outcome of assessment as impermissible, whereas traditional (non-technological) methods of surveillance were assessed as justified. In the urban security scenario, in turn (3) most methods of surveillance were assessed as justified in the given context.

1.3 Potential Applications of the SURVEILLE Scoring Methodology

Several applications for the SURVEILLE scoring methodology can be identified. Here, three proposals concerning such applications are made.

(1) *Decision Support System.* The SURVEILLE methodology of three parallel assessment procedures, a preceding phase of producing a technology description, and a subsequent phase of trying to reconcile the three parallel assessments (marked as “Revise and reassess” in Table 1), including through a feedback loop to the preliminary phase, can be developed into a Decision Support System. An illustration is provided on the next page. The three parallel pillars and the boxes above and below the pillars will each include a set of pertinent questions and the qualitative (yes/no) or quantitative (numerical scores) triggers they produce.

(2) *Usage Situations for the Decision Support System or its Outcomes*. Once finalised, the Decision Support System (DSS) can be utilised in a whole a range of situations or products, such as:

a) The scores of most commonly used surveillance technologies in their typical usage situations, and be presented in the form of a single-page scorecard to be carried in the pocket of a policeman or other operator of surveillance, for encountering repetitive situations. Such a scorecard will assist the operator to identify possible ethical risks and fundamental rights intrusions and to determine whether the expected security benefit will be sufficient to demonstrate the necessity and proportionality of the measure.

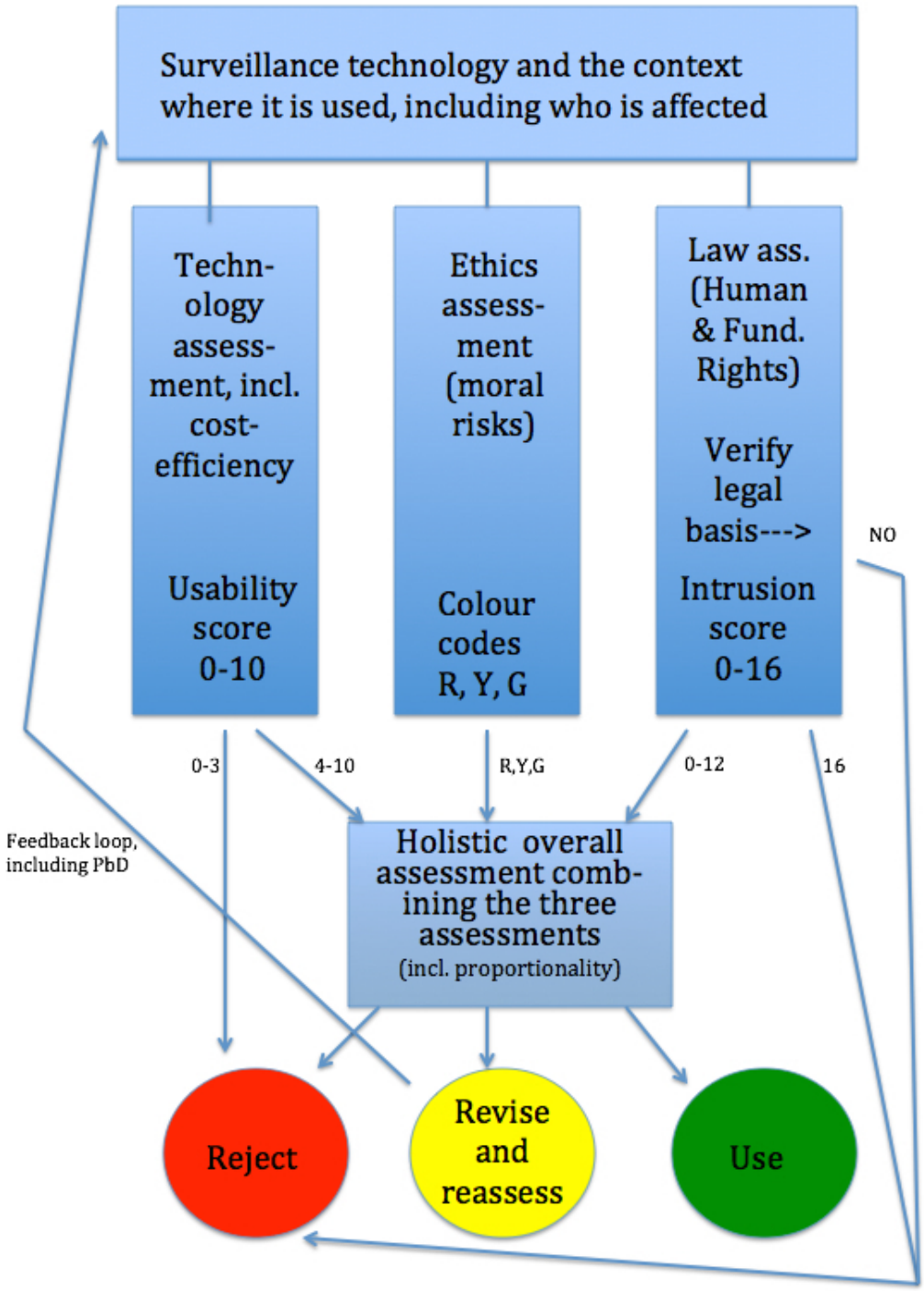
b) The DSS can be used to design an online or app-based tool for facing also new situations and for use in educational contexts, by including it the line of pertinent questions in each of the three pillars and the triggering values used for rejecting (in a given context) a particular surveillance technology or for engaging in a new round of adjustment and redesign in order to find a usage situation where the surveillance will be assessed as justified under a holistic assessment.

c) The DSS can be used as a framework for consensus meetings by three parallel expert groups and a joint reconciliation conference for novel issues, for instance when new surveillance technology is subject to approval for production, deployment or export beyond EU borders.

(3) The SURVEILLE scoring methodology and in particular the reconciliation phase following the three separate assessments, combined with the double role of Privacy by Design (PbD) in the methodology has potential to contribute towards informing the Privacy by Design discourse and concept.[27] In the SURVEILLE assessments, the inclusion of PbD features in a surveillance technology will result in a higher usability score when other things are equal; and they also have the capacity to mitigate the fundamental rights intrusion scores, for instance by eliminating or reducing third-party collateral intrusion in the privacy rights of other persons than the actual target of surveillance.

[27] The notion of Privacy by Design (PbD) has much intuitive appeal and is supported by many policy-makers. The notion is primarily associated with Dr Ann Cavoukian, the former Ontario Privacy Commissioner in Canada. See, e.g., Ann Cavoukian, 'Privacy by Design. The 7 Foundational Principles', August 2009, http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf/. Scholarly commentary of PbD has nevertheless remained reserved, partly due to the breadth and width of Cavoukian's concept. For a discussion paper produced within SURVEILLE, see Elisa Orrù et al., Report on methodology and criteria for incorporating perception issues in the design phase of new surveillance systems, SURVEILLE Deliverable D3.6, available at http://www.surveille.eu/index.php/research/publications/.

Table 1: Decision Support System based on SURVEILLE Research



2. Ethics of Surveillance: An Overview

2.1 The difficulty of justifying surveillance by democratic states

Surveillance is targeted or systematic monitoring of persons, places, items, means of transport or flows of information, in order to detect specific, usually criminal, forms of conduct, or other hazards, and enable, typically, a preventive, protective or reactive response, or the collection of data for preparing such a response in the future. In the SURVEILLE project, we have concentrated on surveillance by governments and their law enforcement personnel. The governments need not be national: local authorities are increasingly involved in surveillance, and their relatively small scale and proximity to electorates may appear to give them more legitimacy than bigger jurisdictions. It is not clear, however, that even surveillance with very local application and big local support is morally legitimate: it depends on the interests in play and the costs to those who are the targets of the surveillance.

In general, in SURVEILLE, we have argued that it is hard to justify sweeping surveillance operations either legally or ethically. In this part of D4.10 the main ethical considerations are reviewed. Some of these are related to the value of private life; others are connected to the typical evidence base for claims that surveillance will prevent harm; others again are connected to the norms of democracy as a morally motivated system of government. Democracy is the political system in which the will of a territorially located people is supposed to be done, usually by governments who have offered a certain party political position for endorsement, and who are elected by a majority in an election. Surveillance and strict policing can inhibit the expression of the will of the people, and it can inhibit the exercise of other personal freedoms associated with liberal democracy, including the freedom to oppose a government and defeat it at elections.

Throughout SURVEILLE we have considered cases in which a government or law-enforcement agency targets for surveillance citizens it is supposed to represent or protect. In this sort of case there are stringent moral limits on the permissibility of surveillance. Where one *individual* watches another e.g. to protect himself from the hostile future actions of the other, self-defence in some broad sense might justify the surveillance. But *governments* do not have a right to maintain themselves in the face of the non-violent hostility of citizens, or to take steps to pre-empt the effects of non-violent, lawful hostility. Still less do liberal democratic governments have prerogatives to watch people who are peacefully minding their own business, which is probably most of a citizenry, most of the time. Governments do not have these prerogatives even if it would make government more efficient, or even if it would help governments to win re-election. The reason is that it is in the interests of citizens not to be observed by the state when pursuing lawful personal projects. It is in the interests of citizens to have portions of life and of civil society that operate independently of the state, and, in particular, independently of opportunities for the state to exert control. The interests governments are supposed to protect are not their own, but those of citizens they represent, where citizens are taken to be the best judges of their own interests.

So if the surveillance of citizens is to be prima facie permissible by the norms of democracy, the surveillance must be carried out by governments either with the direct informed consent of citizens, or with citizens' consent to the use by governments of lawful means of preventing the encroachments on the interests of citizens. Surveillance programmes are not often made subject to direct democratic votes, though citizens in European jurisdictions are regularly polled about open camera surveillance.[28] Even if direct votes were held, however, it is not clear that support for these would always be informed. The costs and benefits are hard to demonstrate uncontroversially, and therefore hard for electorates to take into account in their deliberations. Moral theory allows the question of the justifiability of surveillance to be detached from informed consent. We can ask if what motivates a specific policy and practice of surveillance is the protection of widely acknowledged and genuine vital interests of citizens, and if surveillance is effective in protecting those vital interests.

2.2 Exceptionally, surveillance can assist the protection of vital interests:

All citizens, indeed all human beings, have a vital interest, other things being equal, in survival and in being free from significant pain, illness and hunger: if, in certain unusual situations, these vital interests could only be served by measures that were morally distasteful, governments would have reasons, though perhaps not decisive reasons, for implementing these measures. In a war, for example, a government might commandeer valuable real estate and transport for military purposes, and if these assets were necessary for defending a citizenry from attack, commandeering them might be justified, notwithstanding the interference with the property rights of those whose assets are seized. Might this also be true of surveillance, understood as a counter-terrorism measure, or as a tactic in the fight against organized crime?

Counter-terrorism and the fight against serious and organized crime have very strong prima facie claims to be areas of government activity where there are vital interests of citizens to protect. It is true that both liberal democratic and autocratic governments have been known to define "terrorism" opportunistically and tendentiously, so that in those cases it can be doubted whether counter-terrorism *does* protect vital interests of citizens, as opposed to the interests of the powerful in retaining power. But that does not mean that there is not an acceptable definition of terrorism under which counter-terrorism efforts *do* protect vital interests. For our purposes, "terrorism" is acceptably defined as "violent action on the part of armed groups and individuals aimed at civilians for the purpose of compelling a change in government policy irrespective of a democratic mandate".[29] Under this definition,[30] terrorism threatens an interest

[28] See for example EC FP7 Projects RESPECT http://respectproject.eu/ and SURPRISE http://surprise-project.eu/.

[29] On the definition of terrorism see Schmid, 2004, 'Terrorism: the Definitional Problem'. For philosophical discussions see Primoratz, 2004, *Terrorism: The Philosophical Issues, and* Goodin, 2006, *What's Wrong with Terrorism?*

[30] This definition differs only slightly from legal ones e.g., that proposed by Martin Scheinin: "Deadly or otherwise serious physical violence against 'civilians' (= human

in individual bodily security and survival, not to mention an interest in non-violent collective self-determination. These are genuine vital interests, and in principle governments are justified in taking a wide range of measures against individuals and groups who genuinely threaten those interests.

The fight against serious and organized crime can similarly be related to the protection of genuine vital interests. Much of this sort of crime is violent, and victimizes people, sometimes by, in effect, enslaving them (trafficking), or contributing to a debilitating addiction, or by taking or threatening to take lives. Here there are clear vital interests at stake, corresponding to not being enslaved, addicted or having one's life put at risk. Then there is the way that organized crime infiltrates and corrupts institutions, including law-enforcement and the judiciary. This can give organized crime impunity in more than one jurisdiction, and can create undemocratic centres of power capable of intimidating small populations of people, and even forcing them into crime, with its attendant accretions of coercion and violence.[31] Once again, certain vital interests of citizens –in liberty and in bodily security—are engaged.

If counter-terrorism and the fight against organized crime can genuinely be justified by reference to the vital interests that they protect, and if surveillance is an effective and sometimes necessary measure in counter-terrorism and the fight against serious and organized crime, is surveillance also morally justified? This question does not admit of a general answer, because so many different law-enforcement operations, involving different forms of surveillance, with different degrees of intrusion, could be described as contributing to counter-terrorism or to the fight against serious and organized crime. In order to be morally justified, various criteria need to be met by these operations, which I proceed to list in the next section. Even where these criteria are met, and surveillance is justified all things considered, it can be morally costly, because violations of privacy are prima facie wrong, and because surveillance often violates privacy[32] and the general norms of democracy.

2.3 Considerations relevant to the justifiability of surveillance: prevention vs prosecution

An important preliminary consideration is whether the operation is preventive or whether it is part of the prosecution of a crime that has already been committed.[33] Preventive operations are more problematic than prosecutorial interventions, because often no crime has been committed and because suspects can include citizens with no criminal record. Table 2 represents the reasoning

---

beings who are 'bystanders',) for the purpose of either instilling fear amongst the population or compelling the government into doing something."

[31] See Ashworth, 2010, *Sentencing and Criminal Justice* ch 6.4

[32] For the background theory of privacy motivating the claims put forward here, see John Guelke and Tom Sorell 'Technology and the unified theory of privacy' (work in progress), Annex L.

[33] See Lommell, 2012, 'Punishing the Uncommitted Crime', Ashworth, Zedner and Tomlin, 2013, *Prevention and the Limits of the Criminal Law* and Ashworth and Zedner, 2014, *Preventive Justice*.

that would be needed to reach the conclusion that a preventive policing operation using surveillance would be prima facie justified.

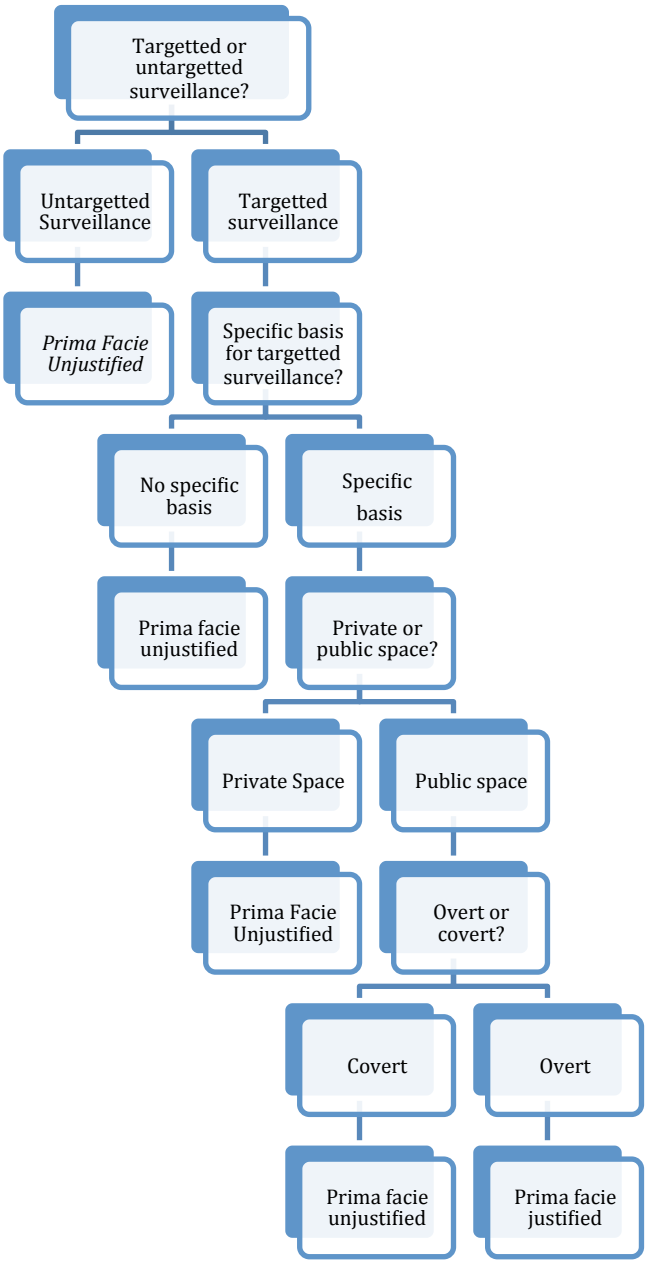


Table 2: Surveillance in Preventive Policing Operations

According to Table 2, to be prima facie justified in a preventive operation, surveillance would have to be targeted on the basis of specific evidence or intelligence, and be conducted overtly in public space. That is, it would have to be directed against a specific person or persons against whom there was some evidence or intelligence of wrongdoing or criminal activity, as opposed to being directed at anyone and everyone. Short of being based on evidence against

someone specifically, surveillance could reasonably be directed at people meeting an evidence-based profile.[34]

Further, for reasons connected to the way democracy requires the actions of government to be open to inspection by citizens, surveillance is better conducted in a public place than in a private one. A public place is one that is usually large enough for many people to gather and in which they observe and are aware that they may be observed by others. People do not need permission to enter many public spaces, although some of them might be reserved for ceremonial locations and otherwise have restricted access. A park or a city street would be examples of public places in the relevant sense. Here surveillance is less problematic, because observation is both permitted and expected, and surveillance is a species of observation. Extra reasoning would be needed to justify *covert* surveillance in public space and surveillance in private space, such as a home or private vehicle or a conventionally designated private place within a public space, like a restaurant table or a hotel room.

A preventive operation that is morally justifiable on balance, and that involves justified surveillance, is not necessarily justified at every stage. Surveillance operations are often protracted, and operational decisions have to be made on the basis of often incomplete and not necessarily accurate information. The scenario in D 2.6, for example, describes an operation lasting years directed against drugs importation and related firearms importation. At some stages in the scenario, surveillance takes place in public spaces (though covertly), and at other stages it penetrates private space and needs to reach a higher threshold of permissibility. The justification that in the scenario makes it possible to reach this threshold is (1) the justification, whatever it is, for preventing not only the importation of drugs but the importation of a firearm, with its life-threatening possibilities; and (2) the difficulty in the circumstances of preventing those offences or threats, or at least collecting evidence for a prosecution of people planning those things, without covert surveillance in private places. All things considered, the fact that the police go through the appropriate legal procedures, and get permission to conduct more intrusive surveillance, does not necessarily mean that the surveillance is legally justified. It may be justified—when the law adhered to is itself justifiable--, but the justification has to draw upon a basis that is not itself determined by the jurisdiction –that of international human rights or European fundamental rights—which rises above the particular jurisdiction and is able to call even judicial decisions made within it into question.

Moral philosophy gives an even more general perspective, since it offers frameworks in which even the implications of human rights law can be questioned. For example, moral philosophy is able to define the right in terms of effects that maximize human welfare in the circumstances of action. This can

[34] In the SURVEILLE project profiling has been defined as: 'a diverse range of activities directed towards developing and utilizing models that delineate different traits and characteristics of persons'. SURVEILLE Deliverable 4.2 'Paper on legal issues related to the use of surveillance data for profiling, pages' 2-5. Available at http://www.surveille.eu/index.php/research/publications/. On targeted surveillance and profiling see: K. Hadjimatheou 'The relative moral risks of targeted and untargeted surveillance' in Ethical Theory and Moral Practice, 2014 (17). Annex H.

make the numbers of lives affected have weight that they would not necessarily have in a human rights framework or in other kinds of deontology. In general, in SURVEILLE, ethical and legal approaches have tended to agree, but since philosophy tests its verdicts against conceivable possibilities as well as actual practice, agreement is not guaranteed. For example, "ticking bomb" cases are sometimes used to justify torture in exceptional cases for the purpose of saving life: these are widely and seriously discussed in philosophy, even though they are very rare in real life, and even though, as a matter of fact, torture does not seem to yield true information but information that those under interrogation think interrogators want to be given. In human rights law, on the other hand, ticking bomb cases are dismissed in absolute terms. Where ethics drawn from moral philosophy tends to agree with law, however, is in implying that laws and jurisdictions can be parochial and therefore can have less authority and objectivity than laws that reflect international standards. In philosophy arguments are sometimes drawn from various standards or principles for institutional design which can be independently justified.

Do law and moral philosophy agree that where crimes are particularly serious, preventing them, including by intrusive surveillance, where it is effective, is correspondingly urgent? Once again the scenario method employed in Work Package 2 reveals the difficulty of arriving at a completely general answer. To allude once more to D2.6, the systematic and large-scale importation of addictive drugs is recognized as a serious crime in most European jurisdictions and by Europol.[35] Does that mean that it should be prevented, if possible, including by intrusive surveillance, where that seems to be necessary? "Prevention" in D2.6 can mean more than one thing: disruption, with or without arrest, as when the police communicate to suspects they have been observing that their plans have been discovered. "Prevention" –with respect to the handling of drugs after importation--can also mean arresting those in possession of the imported drugs at the stage at which the drugs enter the jurisdiction, or more arrests at a later stage when importers and distributors both handle the drugs –but before they have been prepared for sale on the streets. The scenario allows for both of these forms of prevention to be considered.

Prevention with less serious effects for the perpetrators might be regarded as morally permissible even in the presence of intrusion, since the extra resources that intrusion gives the state against individuals does not result in the deprivation of liberty.[36] Intrusive prevention leading to prosecution and arrest based on secretly obtained evidence needs to reach a higher threshold for permissibility. The scenario is complicated by the fact that drugs importation is tied up with firearms importation. This introduces a direct threat to life into the deliberations of the police, a threat of greater harm than the importation of and

[35] See, Celine Cocq and Francesca Galli, The evolving role of Europol in the fight against serious crime: current challenges and future prospects, in Saskia Hufnagel and Carole McCartney (eds.), A question of Trust: International Police and Justice Cooperation, Hart publishing (forthcoming 2015); Annex D.

[36] For a preventive, rather than a punitive, justification for forms of monitoring such as the maintenance of sex offender registers, see K. Hadjimatheou 'Do we have a right to know about the criminality of others? Privacy, stigmatization, and criminal labelling.' (work in progress), Annex J.

distribution of drugs by itself. Although drugs importation and distribution are conventionally regarded as serious crimes, the loss of welfare through loss of life is more significant than the loss of welfare through non-lethal addiction. So in the scenario, action against the threat from firearms importation seems to be more urgent, and to permit intrusion and other normally illicit measures more readily, if they are effective in reducing or preventing loss of life, than preventive measures against drugs importation and distribution.

Imagine a different scenario. This time there is no firearms importation and no threat to life, but the policing operation is on a very large scale, because there is a prospect of dismantling a whole drugs importation and distribution network in a particular jurisdiction. The moral philosophy framework that connects the rightness of actions to the welfare-creating effects of those actions implies that in this case, too, more intrusive prevention might be justified, because of the benefits of greatly reduced, as opposed to slightly reduced, drug importation and distribution. Although within the moral philosophy framework intrusion is undesirable, other things being equal, because privacy has many welfare benefits, intrusion may still be judged to be a proportionate measure, because the disutility of intrusion is, let us stipulate, counter-balanced by the utility of a reduction in debilitating addiction, violence, and fear that results from the disappearance of the drug network. This gain in welfare can, in theory, justify intrusion just as much as the threat to life from firearms importation.

Moral philosophy can indeed go further, for it can use the same framework to discuss the criminalization of drug importation, distribution and possession, and can ask whether sentencing policy in different jurisdictions is too severe or adequate for all kinds of drugs.[37] As is well known, some classes of drugs are legal for adult citizens to use in certain approved locations in the Netherlands. Similarly, in certain states of the United States, marijuana can now legally be sold for medical purposes. These developments are sometimes justified on the ground that possession and use of soft drugs is, where illegal, a victimless crime, and that criminalization of soft drugs is therefore no more justified than the criminalization of alcohol and tobacco would be, even if there were positive health effects. Hard drugs are a different matter: here the health effects are severe, and the financial gains from importation and exportation are very great, and easily translated into disproportionate influence on law-enforcement, not to mention the development of autonomous but unaccountable power-structures violently defended by criminal gangs. Then, independent of gangs, there is the crime engaged in by lone addicts in order to finance their habit. So within this framework the importation and distribution of hard drugs appears as a serious crime against which intrusive measures could in principle be used.

2.4 The normative requirements of democracy and limits on surveillance

Additional justification for covert police action or for police action in a private place is required not just because of the welfare-benefits of non-intrusion for individuals, but also because of the way publicity is a requirement of the control

[37] See Husak, 2009, *Overcriminalisation* and Husak and Marneffe, 1992, *Drugs and Rights*.

of governments by citizens in a democracy. The exposure of the actions of the government or its agents to the scrutiny of those who are ruled—is a condition of the justified exercise of democratic power, and because ordinary citizens are supposed to be allowed – by both other individuals and government—unobserved space in which to conduct close relationships. Let us take the public exercise of power, and the private pursuit of an individual life in turn.

In democracies, citizenries confer power in three ways: by delegating the power to make law and interpret law authoritatively, by complying with laws made by those authorized to legislate, and by not impeding people authorized to adjudicate or enforce the law, or authorized to inflict lawful punishments. Covert action by institutions encourages citizens to doubt a central promise of democracy – that the will of the people will be carried out by the people's institutions - because covert action makes it hard for the people or their representatives to *see* whether their will is being done or not. But in exceptional cases covert action can sometimes be justified – if what is in the balance is great and imminent harm to citizens, and it is reasonable to believe that there is no public alternative available to the relevant agents in the period in which they have to act. Even in these cases the authorities do not necessarily act entirely covertly, since in developed liberal democracies they have to inform and get permission from bodies under democratic control before they engage in a covert operation.

Coming now to the presumption in favour of an undisturbed private life for ordinary individuals unless there is sufficient evidence or intelligence against them, this is connected with the liberal element in liberal democracy, the normative requirement of liberty, paradigmatically negative liberty or freedom from interference, and the assumption that individuals are the best judges of their own interests. Individuals in a liberal democracy are left to pursue their own lives as they see fit, within limits set by law, and with criminalization of acts being tied to harming others as opposed to self-harm.[38] Having a living space of one's own is normally regarded in liberal democracies as a precondition of an autonomous, independent adult life, or at least as facilitating an autonomous, independent life. This home space is the paradigm of the private space, the space over which the individual has the authority to permit or prohibit entry by others, even the state and its personnel, in all but a limited range of exceptional cases. There is a strong presumption in liberal democracy against forced entry or unconsented to entry to this private space, and the normal prohibition on the external observation of that space is connected to prohibition on entry. Observation through cameras or listening devices makes available to the observer the experiences of someone who is inside the private space. If there is a presumption against any incursions in this space, there is an even stronger presumption against secret incursions, as this takes away the prerogative of concealment that is open to everyone in a space they know is observed. The presumptions against intrusion and secret intrusion are reflected in the increasingly exacting justification required for these to be legally authorized in many mature democratic jurisdictions.

[38] Mill, 1859, *On Liberty*.

2.5 Surveillance in one-off preventive policing vs mass surveillance by governments

In the case of the anti-drugs investigation discussed in D2.6 the justification for surveillance is connected to the prevention of harm: harm to the target of the imported firearm, and harm to those affected by the importation and distribution of drugs. In the case of D2.8 the same sort of general justification seems to fit: in the relevant scenario a wide range of surveillance technology is used in a large-scale preventive counter-terrorism programme. The main lines of the scenario follow those of the American government's NSA programme of bulk monitoring of metadata drawn from citizens' e-mail communications. Where D2.8 departs from the NSA case is in having a number of jurisdictions involved. The few individual targets of surveillance in the scenario are selected on vague grounds.

The problem with justifying the D2.8 surveillance programme is that it appears to involve *highly* intrusive technology, applied specifically to persons against whom there is less than compelling evidence, *as well as* to many more people against whom there is no evidence of wrongdoing or illegality at all. So although the potential harm is very high on the scale of harms that can justifiably be prevented, the *probability* of the harm is not established to be high, nor is a very likely source for it established. This means that the effectiveness of using surveillance is in doubt, while the probability of intruding deeply and unjustifiably into the lives of people who are not involved in the least in terrorism is arguably very high. Taken together, these considerations add up to a strong case against the use of most of the surveillance techniques and equipment envisaged in scenario D2.8.

The D2.8 scenario raises more sharply than others considered in Work Package 2 the tensions between mass surveillance and the norms of democracy. In the case of the NSA and the security service of a Member State, that can be considered the real-life inspiration for D2.8, vast quantities of private communication between US citizens and foreigners were fully available for possible inspection with the not-hard-to- get permission of a special, semi-secret court (the FISA court). Metadata for communications between US citizens were also (but controversially) open to inspection under domestic law. The metadata of particular interest to the US government were those that would connect telephone numbers associated with alleged terrorists and telephone numbers that had previously not been of interest to the authorities. The US authorities wanted also to track indirect communications between forensically aware terrorists. So they tried to reconstruct chains between telephone numbers that had communicated with telephone numbers directly chained to terrorists. In this kind of chain, the telephone number of someone who had not communicated with a suspect, but who might have communicated with one of the suspect's callers, might be construed as interesting. Further jumps (allowing for chaining numbers of callers of callers of callers of suspects) were also taken into account. This produced a larger and larger network of possible callers of interest to the authority. The greater the number of jumps, the less discriminating the search for suspect numbers, and the weaker the evidence that numbers at this remove from genuine suspects were genuinely suspicious in turn. The fact that in the NSA scheme a very large number of communications were sifted through for no

specific reason, and, in addition, sifted through secretly, is clearly morally problematic for more than one reason.

Many critics have focused on the metadata collection as a privacy violation,[39] but the argument to be developed here is that the anti-democratic character of the metadata collection is more important. The American people were not told by their government that their communications were being collected in some form or sifted through on a huge scale: that fact was only publicized by a security breach on the part of Edward Snowden. Nor were the representatives of US citizens in Congress properly informed, not even security cleared members of relevant committees of the US Senate asking direct questions to the head of the NSA.[40] This means that some elements of the American government ceased to be subject to appropriate oversight while undertaking a massive programme of surveillance for which there was no mandate, and which would have been opposed vigorously by both the left and the libertarian right in the US. (Edward Snowden appears to have had right-leaning but libertarian party political sympathies).

The *privacy* violations in the NSA case are harder to judge. First of all, the collection of metadata was primarily connected with telephone–chaining, and while telephone-chaining is less plausible as a guide to suspects the more indirect it is (the more "jumps" it allows), this is a problem for due process rather than a problem of intrusion. On the other hand, privacy violations *were* potentially very serious in the case of telephone and email communication between US citizens and foreigners. But even here intrusion was mitigated by the use of "selectors". Only certain topics of conversation, certain mentions of certain names and terms, would trigger further investigation. It is not as if conversations were being listened to and analysed minutely. The effect of using selectors was to narrow down enormously the content extracted. And there has been no suggestion that US citizens in droves or many foreign citizens have been detained or arrested on the basis of the information collected. This probably shows that even when selectors have identified certain communications, as worth investigating further, the full content has not warranted arrests.

The D2.8 scenario is not like the NSA reality in every respect. First, it considers an EU jurisdiction, not the US. The EU jurisdiction is legally required to treat privacy as a fundamental right. Second, D2.8 is not only to do with the bulk collection of data from massive databases. Particular people are also targeted. In D2.8 there is weak circumstantial evidence that a particular EU national is in touch with someone of legitimate interest to the authority, and weak evidence again that an EU national has been in email communication with someone of interest to the security services in relation to the possible construction and importation of an explosive device.

There is also weak evidence in the scenario that "Omar Gunes" might be connected with an attack on transport infrastructure in the capital city of an EU jurisdiction. The very intrusive Finnspy software is brought into play in relation to this target and the belief in an imminent attack, rather than as a sort of

[39] See Joh, 2014, 'Policing by Numbers'.

[40] See for example http://www.newyorker.com/magazine/2013/12/16/state-of-deception

vacuum cleaner for everyone's personal data. But even when allowed to operate only on computers used in a small number of Internet cafes by someone who communicates occasionally with people who are of interest to the security service, the Finnspy software may still be more of a vacuum cleaner than the evidence of a security threat justifies. In a different way "optical splitting" may be too much of a vacuum cleaner, allowing perfectly innocent Internet activity that is no-one's business to be searched for patterns supposedly characteristic of organized criminals employing the internet. Even if certain personal patterns of activity lead to people being detained and then released without charge, it is not as if detention is costless or as if not being charged is the same as never having been a suspect at all. The use of surveillance software can exact costs from those who have done nothing wrong and who do not meet the threshold for being punished, but who in effect are punished in the sense of suffering institutional harm from the use made of the Finnspy and optical splitting.[41]

The discussion of ethics in D2.8 did not claim that the main costs were invasions of privacy. The main costs were associated with loss of liberty (even if short-lived) for detained subjects and being suspected of committing a criminal offence for no reason. Chilling effects –self-censorship, loss of spontaneity in Internet explorations—these were also important, though distinct from intrusion. Similarly for stigmatisation arising from the possible bad publicity visited on these people as a result of the suspicion. These effects once again seem distinct from loss of privacy or damage to privacy.

2.6 Urban security and urban surveillance

Urban jurisdictions are increasingly involved in surveillance or surveillance-related activities through the convergence of otherwise distinct political agendas. One is the "smart city" agenda. This is the aspiration to make the management of cities more efficient as measured by energy use, and the deployment of resources for transport, policing and emergency response.[42] Urban lighting which comes on only when there is real darkness, the ability to reset traffic light patterns according to traffic density; the ability to regulate flows of public transport; all of these are examples. Another agenda is a "localism" agenda. In certain countries, powers formerly exercised centrally are being devolved to regions or sub-regionally. A further agenda is that of connecting urban democracy and security to digital innovation, including digital social networks, location-tracking [43] and the possibilities of apps and "smartphones" as sources of real-time data about densities of people in particular places, plans of mass gatherings. Combining the localism and "digital"

---

[41] For arguments against the claim that giving publicity to criminal labels, for example by distributing information about individuals subject to preventive measures such as ASBOs or criminal prevention orders as a form of punishment, see K. Hadjimatheou 'Criminal labelling, publicity, and punishment' (work in progress' Annex I.

[42] For an example of typical projects one may see the New York based 'Centre for Urban Science and Progress' http://cusp.nyu.edu/.

[43] See, Jonathan Andrew, Developments in behavioural biometrics: Newfound utility in location data; Annex A; Jonathan Andrew, The 'Internet of Things', and safeguarding Personal location data; Annex B.

agendas produces, in some cities, a direct involvement in the policing of neighbourhoods that can border on vigilante-ism, but that often simply consists of co-operating in keeping an eye out for burglary, or that might offer a source of solidarity against e.g. the dominance of a neighbourhood by a criminal gang.

The scenario in D2.9 shows how the deployment of surveillance technology might reflect one of these agendas, or a combination. The main moral risks picked up in the Deliverable were not very different from those picked up in the other deliverables. Invasion of privacy, the risk of loss of liberty, the operation of discrimination through the use of questionable profiles in algorithms; these are indeed moral problems and risks, but they have an apparently different character when the underlying agent is not the Big Brother of a central or state government, but a smaller, less threatening and apparently more responsive jurisdiction like a city. It is as if the localism of the security policy takes away some of its threat. The fact that the policy might have been endorsed by those directly affected by it in an election in which it might have been a prominent issue; this seems to make it much more benign than e.g. the NSA policy, which was secret even from senior legislators and which was certainly never submitted to an electorate.

Is localism purifying in that way? Not necessarily. First, some local jurisdictions are hard to distinguish from the state. There are successful city-states like Singapore and very small city-based states, such as those in the Gulf. Then there is Mexico City, a megalopolis of a federal district, which is also a big living laboratory for a large array of smart security technology designed for it by Thales, the large European technology developer. Mexico City is too big and too involved with the government of Mexico to be a convincing example of a city whose smart technology is owed to localism or made user-friendly because of localism. On the other hand, its technologies or related technologies might be adopted by the politicians of other smaller cities to implement a security policy that is genuinely driven by local concerns.

For example, the imaginary city X of the D2.9 scenario does not seem to be remotely on the scale of Mexico City, and yet in the scenario it employs the Cybels technology that was developed by Thales for Mexico City. Cybels is supposed to be a tool for getting early warning of otherwise hard-to-police mass gatherings, including riots. There is evidence, for example, that the London riots had focal points created by social networking activity and chat on the part of members of local criminal gangs.[44] Although some of the chat was coded or expressed in a hard to understand slang, it was penetrable and could have made the targetting of police personnel and the prevention of looting more effective. Social networks and social media were a big source in London of video evidence of offences and of images of offenders. In combination with a highly effective mass campaign encouraging Londoners to put names to those images, this evidence turned into a basis for the very efficient prosecution of looting offences. Given the relatively high usability score of Cybels, and its probable marketability

[44] See for example http://www.theguardian.com/media/2011/aug/08/london-riots-facebook-twitter-blackberry and http://www.theguardian.com/media/2012/mar/28/uk-riots-twitter-facebook.

to cities like X in addition to London and Mexico City, how, morally speaking, should its introduction be regarded? [45]

With skepticism, Cybels may be in its element in a city with chronically high rates of serious crime and criminals who use social networks exhibitionistically, or it may come into its own exceptionally, when social network chat has to be monitored at high speed to prevent looting or rioting. That said, its everyday use in relatively peaceful cities with social networks dominated by the law-abiding and discussing nothing criminal is clearly unjustified. Social networks generate links between like-minded people who might not otherwise meet: they are channels for gaining more specialized knowledge, expressing opinion, and organizing political action. People use social networks not expecting to receive official attention, and Cybels does not seem to alert those whose open access information is being collected that their information is of interest to the authorities. This gives an unacknowledged dual use to open access that is welfare reducing for those who value unobserved networking and knowledge building and who want to organize politically within the law. The costs to these people remain even if there is a big electoral following for Cybels, built on the false impression that there are high rates of crime in a city. As a morally preferable alternative to using Cybels, the police could present themselves openly on social media and appeal for information; they could mount campaigns showing the harm done by particular offences, or produce programmes about serious, unsolved crimes to be broadcast to those in the population who might be witnesses.

There are moral objections to two further technologies mentioned in the scenario in D 2.9: hard to observe but not covertly deployed drones carrying cameras, and location-tracking through smartphones. Drones are widely available and cheap, and their operation easily evades official oversight. Camera technology on which drones serve as platforms are less likely to have the privacy-by-design software of conventionally mounted, openly displayed CCTV cameras in a public space. But these platforms are not exactly hidden, and they do not operate in private space. So they seem to belong on the morally less problematic end of the surveillance spectrum while being nearly as inconspicuous as concealed equipment. In fact, they soften the distinction between covert and overt surveillance, and this is undesirable for all of the reasons connected to the benefits of private life to individuals and publicity of institutional action to democracies.

The second, morally problematic technology is smart phones—adapted to the purposes of official data gathering. Smart phones leave records of their use by owners and often the continuous real-time location of a given person, and so carry great risks of exposing information about people's movements, activities and contacts that they often would not want to disclose to friends, still less the police, the state or a tabloid newspaper. Yet through downloadable apps and

[45] For arguments in favour of the claim that using evidence gathered via surveillance and detection technologies to identify suspects and build criminal cases could have a positive effect in protecting the innocent from wrongful conviction see K. Hadjimatheou 'The presumption of innocence and the use of surveillance and detection technologies by police' (work in progress, Annex K)

other software, smart phones are a potentially valuable interface between a public in need of services, and states that supply them and are authorized to supply them. Many smartphones in combination can give accurate pictures in real times of crowd densities in an emergency prevention or response situation, and particular smart phones could be wired up to communicate directly with emergency services if monitored data of selected vital signs conformed to some pattern for an imminent health risk. The welfare increasing possibilities of the smart phone need therefore to be combined with technological and other safeguards on the malicious or opportunistic use of data or images that their owners have legitimate reasons for not wanting to make public, e.g., the reason that it enables them to have intimate relations with some people.

Although there is a well-established recognition of the threat of Big Brother at the level of states, and relatively recent experience of intense surveillance of great numbers by the Stasi in the former East Germany, these risks may not be associated with the otherwise more benign face of urban governments, especially against the background of a localist ideology: i.e., the ideology that democracy is better when it involves fewer people and less geography and fewer levels of authority—i.e. where rulers and ruled are much closer in size to one another and share the same accessible space. The scenario in D2.9 suggests that potentially highly intrusive technology may give local government opportunities for intrusion and control that disrupt this ideal of unthreatening government. Furthermore, national governments may, by promoting a localist agenda and autonomy for citizens in regard to local matters, make it easier for local authorities to introduce surveillance regimes that national governments leave alone, despite their contravening treaties entered into at national level. If cities in the future gain in autonomy, this problem may grow.