Final Report Summary - SURVEILLE (Surveillance: Ethical Issues, Legal Limitations, and Efficiency)

Executive Summary:
SURVEILLE (Surveillance: Ethical Issues, Legal Limitations, and Efficiency) was a 41-month collaborative project under the Security Call of FP7, responding to topic FP7-SEC-2011.6.1-5 ‘Surveillance and the challenges for the security of the citizen’. It was a highly interdisciplinary programme of research that will help decision-makers to make better choices concerning the development, deployment and use of surveillance technologies. The Consortium brought together cutting edge expertise in, inter alia, technology assessment, ethics, and law.

SURVEILLE conducted a comprehensive survey of surveillance systems and technologies that are currently used in Europe or that are likely to be deployed in the near future. It addressed the legal limits on surveillance and the ethical issues it raises. It also assessed the effectiveness and efficiency of surveillance technologies in improving security. It developed a multidisciplinary methodology for the comprehensive assessment of the usability (i.e. effectiveness and efficiency), moral hazards and fundamental rights intrusion of any particular surveillance technology in a given context. Relying on a scenario-based approach, three parallel expert teams assessed the same surveillance technology in the same situation, aiming at semi-quantitative or qualitative scoring of each technology for its usability, moral hazards and fundamental rights intrusion. The three assessments were reconciled through a phase of holistic overall assessment, with a view towards determining whether the surveillance technology in question could be recommended in the situation in question, was subject to hesitations or qualifications, or should be rejected as impermissible in the specific context. In this multidisciplinary methodology, Privacy by Design has a special place, as its introduction will improve the usability score, lower the fundamental rights intrusion and constitute a tool in redesigning a technology or its usage so that an otherwise problematic form of surveillance can be improved so that it passes all tests.

SURVEILLE also surveyed and examined existing empirical research on perceptions of surveillance and surveillance technologies amongst the general public and specific target groups, and sought to inform decision-makers and other relevant stakeholders about the public acceptability of these technologies. Interactions between SURVEILLE and technology developers and end-users, including through an Advisory Service for developers and two end-user expert panels (one with local authorities, one with police authorities) contributed towards helping decision-makers and manufacturers to adapt their systems to legal and ethical limitations and public concerns, as well as end-users to deploy systems more effectively while at the same time in compliance with legal and ethical limitations and taking into account public perceptions.

SURVEILLE produced a wide range of research reports submitted to the Commission as project deliverables and in most cases also published on the website of the project. The research has already resulted in several academic publications in peer-reviewed journals or as book chapters. Work will continue for academic and other publications, including an open access Working Paper series. SURVEILLE developed new and innovative methodologies for the multidisciplinary assessment of surveillance technologies in a wide range of usage situations. Its work contributes towards a structured and rational discussion and decision-making process that can take into account as diverse factors as the improvement of security, the financial cost,
moral hazards, and the intrusion into privacy and other fundamental rights (both of the actual target and of bystanders). It can also be utilised in discussions on Privacy by Design, including towards the adoption of a Standard.

Project Context and Objectives:
The SURVEILLE proposal was drafted and submitted in 2010. Already at that stage it was able to affirm a trend over the preceding ten years, when EU member states have found uses for an increasing variety of surveillance technologies. These technologies include traditional video surveillance, such as CCTV, audio surveillance tools, location tracking devices such as GPS, and computer and telecommunications monitoring equipment. The proposal further stated that the increased use and development of these technologies has partly been a conscious response to specific security risks, such as terrorism, the continued rise of organised crime, and concerns over border security. Public policy has been characterized by the adoption of a ‘proactive attitude’, that is, a shift in emphasis from reactive to ‘preventive’ measures. Whereas reactive measures try to address crimes already committed or to ward off immediate danger, ‘preventive measures’ are concerned with potential and future dangers. As also stated in the SURVEILLE proposal in 2010, the use of surveillance technologies has been subject to wide criticism by social scientists, lawyers, ethicists and the media. Although some efforts have been made to protect individual privacy in the design of security technologies, many civil society actors, politicians and journalists increasingly invoke the so-called ‘surveillance state’, including with references to George Orwell’s dystopia ‘1984’. European citizens expect and deserve a better informed and more transparent public discussion on surveillance, including its benefits, technological solutions, and adverse effects.

SURVEILLE was proposed as a project that would systematically review the impacts of different surveillance systems, and also help manufacturers and end-users better to develop and deploy these systems. It was crafted as a highly multidisciplinary project combining law, ethics, sociology and technology analysis in a small number of highly collaborative, cross-cutting work packages. SURVEILLE would assess surveillance technology for its actual effectiveness in fighting crime and terrorism, for its social and economic costs, and would survey perceptions of surveillance, mainly through reviewing earlier and parallel studies. The investigation of societal and ethical aspects would focus on undesired side effects of surveillance systems. SURVEILLE would address legal limitations on the use of surveillance technologies as well as ethical constraints. SURVEILLE was to include analysis of the potential of Privacy by Design and privacy-enhancing technologies in the context of surveillance systems. It would interact with technology developers and manufacturers through a systematically delivered Advisory Service. It would interact with end-users of surveillance and aim at wide dissemination, including amongst European and national decision-makers.

The trends outlined in the SURVEILLE proposal have very much continued throughout the life of the project (2012-2015). More than perhaps ever before, surveillance has continuously figured high on the agenda of national and European decision-makers as well as media outlets and new social media, and academic discourse. The risks calling for increased surveillance have not faded away. On the contrary, Europe has continued to be faced with the risk of terrorism and also as an actual target of terrorist acts. Also organised crime, including money laundering, drug trafficking and trafficking in persons have proven persistent. Technology development has been rapid, so that new methods of surveillance have been developed, discussed and deployed during the implementation of the project. Three events or developments that have particularly shaped the context where SURVEILLE was conducting its research deserve to be mentioned separately: (1) the June 2013 revelations by former CIA and NSA contractor Edward Snowden concerning electronic mass surveillance by the United States and its European collaborators, (2) the April 2014 ruling by the Court of Justice of the European Union in the Digital Rights Ireland case, annulling the EU Data Retention Directive and in multiple ways shaking the societal and legal discourse on surveillance, including in the issues of ‘balancing’ and the distinction between ‘content’ and ‘metadata’, and finally (3), the terrorist attack against Charlie Hebdo in Paris in January 2015. The first one of these three developments, the Snowden revelations, shaped the research process by directing the work on the terrorism prevention scenario (D2.8) on new forms of electronic mass surveillance. The second one, the CJEU ruling, affected the fundamental rights assessments conducted in the project, reinforcing the evolving methodology and affecting the reliability scores in the actual assessment. As the third major event, the Charlie Hebdo attack, occurred when the actual research was almost complete, it had more an effect on the dissemination activities of the project (including the Final Conference) than the deliverables.
The main objectives of SURVEILLE were:

1. To provide a comprehensive survey of the types of surveillance technology deployed in Europe.
2. To assess the benefits and costs of surveillance technology. (By ‘benefits’ we mean the delivery of improved security; by ‘costs’ economic costs, negative public perceptions, negative effects on behaviour, and infringement of fundamental rights.)
3. To identify, elaborate and assess the whole range of legal and ethical issues raised by the use of surveillance technology in the prevention, investigation and prosecution of terrorism and other crime - including those related to fundamental rights.
4. To communicate continuously the results of the research to a representative sample of stakeholders: European decision-makers, law enforcement professionals, local authorities, and technology developers, and to receive feedback to inform continuing research.

These four objectives were successfully pursued throughout the project. Each Work Package served to meet, or to contribute towards, one or more of these objectives. Towards that end each Work Package was operationalised through sets of sub-objectives and tasks.

Project Results:
Three of the main results of SURVEILLE have been reported as exploitable foregrounds. They are described first here below, followed by another subsection on other main results, through six selected examples.

(1) The SURVEILLE project serves the general advancement of knowledge with its innovative and exploitable methodology of assessing surveillance technologies for their usability, ethics and fundamental rights intrusion through three parallel semi-quantitative expert assessments and a subsequent holistic reconciliation of the outcomes from these three ‘pillars’.

SURVEILLE conducted a series of multidisciplinary assessments of a wide range of surveillance technologies. This was done by looking into surveillance as used in three scenarios: detection and investigation of trans-border organised crime, terrorism prevention, and urban security for the preservation of public order. In each scenario, three parallel expert teams assessed the same technologies for their technological usability (effectiveness and efficiency), moral hazards and fundamental rights intrusions. The resulting three scores were combined and subjected to a holistic process of reconciliation where Privacy by Design has a special role, as it is capable of simultaneously improving the usability score and reducing moral hazards and fundamental rights intrusion. The work on the three scenarios was reported in deliverables D2.6 D2.8 and D2.9. The methodology is further explained in D3.9 and D4.10 and popularised in the SURVEILLE Briefing Note.

(2) SURVEILLE results can be exploited in the elaboration of European standards, in particular in the implementation of standardisation request M/530 by the European Commission for European standard(s) addressing privacy management in the design and development and in the production and service provision processes of security technologies. The SURVEILLE methodology for the scoring of surveillance technologies, including the role of Privacy by Design in it, should be incorporated into the work towards the standard(s) in question. Besides affecting both the usability score and the fundamental rights intrusion score at the first phase of parallel expert assessments, Privacy by Design figures also in the feedback loop after the second phase, a first round of holistic reconciliation of the outcomes of the three parallel expert assessments. It will then guide a third phase of efforts to redesign a technology that was not approved for use in the first round.

As reported in SURVEILLE deliverable D4.10 and popularised in the SURVEILLE Briefing Note, the multidisciplinary and semi-quantitative methodology of scoring surveillance technologies can serve as the basis for a Decision Support System that will assist policymakers, technology developers, end-users and those supervising the use of surveillance, including courts, in making a proper assessments of each surveillance technology in a given usage context, through a structured and rational process that combines as diverse factors as the improvement of security, the financial cost, moral hazards, and the intrusion into privacy and other fundamental rights, both of the actual target and of bystanders. This line of SURVEILLE work can be utilised in the implementation of Standardisation Request M/530 by the European Commission (Standardisation request...
addressed to the European standardisation organisations in support of the implementation of privacy and personal data protection management in the design and development and in the production and service provision processes of security technologies, 20 January 2015).

(3) The third type of exploitable foreground produced by SURVEILLE pertains to the field of policies, and in particular professional training. As part of its Work Package 5 (Stakeholder interaction), SURVEILLE included two end-user panels coordinated, respectively, by its two end-user partners, Merseyside Police (MERPOL) and the European Federation for Urban Security (EFUS). The former engaged with European police authorities and the latter with European cities, municipalities and regions. In addition, WP5 included a series of interactions with law enforcement officials in an actual training context, namely trainings organised by SURVEILLE partner Raoul Wallenberg Institute of Human Rights and Humanitarian Law (RWI). Building upon these lines of work, RWI then led the process towards the elaboration of a SURVEILLE proposal for a training course for police, prosecutors, judges and local authority end-users in the responsible use of surveillance technologies. The proposal is module-based, with differentiation between trainings for the police, for judges and prosecutors, and for local authorities. The proposal was reported in SURVEILLE deliverable D5.7 and positively evaluated by the SURVEILLE Advisory Board. EFUS and RWI have assumed responsibility for seeking opportunities for the exploitation of the product after the close of the SURVEILLE project. RWI seeks to do this both through its own training activities and in collaboration with CEPOL, while EFUS is relying on its own membership of more than 300 cities and municipalities.

Beyond the above-described three categories of exploitable foreground, SURVEILLE produced also several other innovative results of which a non-exhaustive selection is presented here below.

(4) In its Work Package 3 (Perceptions and Effectiveness of Surveillance) SURVEILLE developed a novel methodology for the technology assessment of surveillance technologies. This methodology was utilised for producing the usability score explained above under item (1). However, independently of its use within the overall multidisciplinary SURVEILLE methodology, the technology assessment methodology developed in WP3 represents on its own an important result from the research. As summarised in the final deliverable from WP3, deliverable D3.9 the usability score follows from ten separate factors which in most cases can be given 0, 0,5 or 1 points each. The elementary scores are added together, so the maximum overall score is 10.

One group of factors assesses the effectiveness of a surveillance technology, i.e. whether and to what extent it is capable of producing the intended outcome of, e.g. increased security. The three components within this category are named as delivery, context and sensitivity. Another group of three factors assesses the financial cost of the surveillance technology, by looking separately into initial cost, personnel requirements and additional running costs. Further, Privacy by Design was integrated into the technology assessment by again scoring it across three separate factors, namely data collection, data access and use, and data protection. Finally, a tenth point can be afforded for proven technological excellence. The outcome of the combination of the 10 factors is the usability score which can be seen to provide a rational and structured way of assessing whether surveillance serves a legitimate aim, and whether the degree to which it actually delivers towards that aim demonstrates that the particular form of surveillance being assessed is necessary in a democratic society.

(5) Similarly, the fundamental rights assessment methodology developed in Work Package 4 (Law and ethics of surveillance technologies) is on its own innovative and suitable for applications outside the overall SURVEILLE methodology of combining parallel expert assessments. In WP4, the lawyers in SURVEILLE developed a fundamental right intrusion analysis to asses the negative effect of surveillance upon privacy and other fundamental rights. Such an assessment is needed for a rational discussion on whether the benefits of a particular form of surveillance (usability, see previous item) is proportionate in respect of its unavoidable negative impact. This line of work was based on a systematic study of the case-law by the European Court of Human Rights and the Court of Justice of the European Union. Building upon that body of case law, a semi-quantitative methodology of a fundamental rights intrusion score was developed. It is based on three factors that are assessed separately: the importance (or weight) of a fundamental right in the given situation (max. 4), the depth of the intrusion into that right as
resulting from surveillance (max. 4), and the reliability of these assessments in the light of existing case-law (max 1). The three sub-scores are multiplied by each other and result in a fundamental rights intrusion score of maximum 16. In an innovative way the methodology secures the protection of the essential core of fundamental rights, as the score for measures that impede the core area of fundamental rights would typically be 16, i.e. higher than the highest possible usability score. The methodology is also capable of addressing the old debate of the distinction between ‘content’ and ‘metadata’ in communications surveillance by enabling a nuanced and controllable assessment methodology, instead of relying on a simplistic dichotomy. This kind of an approach is necessitated by the CJEU ruling in the Digital Rights Ireland case, rejecting the old simplistic approach.

(6) Furthermore, in the legal dimension of SURVEILLE, it is an independent and important finding that privacy and data protection, assessed separately from each other, generally provide a good proxy for assessing the overall fundamental rights impact of surveillance. The right to the protection of personal data needs to be treated as an independent fundamental right, as often the scores received gave it a significantly different intrusion level than for the more general right to privacy. Taken together, these two rights, however, appear to be capable of capturing the overall fundamental rights impact, as separate assessments for rights such as freedom of movement, freedom of expression, freedom of religion, freedom of association and assembly, and the right to equal treatment tended to obtain lower scores than privacy and/or data protection, and these other impacts could therefore be included in the assessment under privacy and data protection.

(7) Also in Work Package 4, important work was done to map and systematise the range of moral hazards related to surveillance. This line of work, conducted by the ethicists in SURVEILLE, was applied in the scenario-based assessment of a wide range of surveillance technologies to identify their distinctive ethical risks and to rate the severity of each identified moral risk using a three-stage system of colour codes. For instance in deliverable D2.9 this methodology was used to assess separately three types of ethical harm: moral risk of error leading to significant sanction, moral risk to trust and chilling effect, and moral risk of intrusion. This categorisation and semi-quantification through illustrative colour codes (green, yellow, red) represents a novel methodology to increase the granularity of information produced by ethical assessment of surveillance.

(8) As reflected above, SURVEILLE research incorporates the notion of Privacy by Design and shows a way forward as to its operationalisation into decision-making on the deployment and use of surveillance technologies. In addition, SURVEILLE conducted also conceptual work on the notion of Privacy by Design and its alternatives. Reference is made to deliverable D3.6 and the alternative notions of Minimum Harm by Design, Transparency by Design, and Accountability by Design discussed therein.

(9) SURVEILLE Work Package 5 included a highly innovative Advisory Service through which SURVEILLE expertise was made available to surveillance technology developers, projects presented under FP7 or Horizon 2020, and end-users who were all able to receive expert advice on ethical issues that might arise in the envisaged use of their existing or future technologies. During the life of SURVEILLE, 24 such interactions with a wide range of ‘clients’ took place. The Advisory Service was reported in deliverables D5.8 and D5.10 and evaluated in D5.9. The experience of SURVEILLE will be valuable in the future, and one option would be to make an independent ethics assessment of surveillance technology a mandatory phase in the preparation of proposals under Horizon 2020. The experience of the SURVEILLE Advisory Service demonstrates that the scope of such review is very different from traditional ethics review procedures that focus on the protection of personal data of humans involved in the research process and other issues of research ethics.

Potential Impact:
SURVEILLE was designed as a multidisciplinary high-impact project that combines academic excellence with intense developer and end-user engagement. Throughout its life span, and also after the end of its funding as an FP7 project, SURVEILLE has continuously been striving to give decision-makers a clear view of the state of the art on efficient, ethical and legal use of surveillance technologies and pave the way towards an improvement of current practices. It has developed and applied novel methods to the evaluation of the effectiveness of surveillance technology in delivering better security. Through its Advisory
Service it was continuously engaging with technology developers, and similarly through two expert panels with two important categories of end-users, namely police and local authorities. All three groups of actors will benefit from the effectiveness and efficiency assessment and the clear ethical and legal framework produced in SURVEILLE. Through innovative and original academic research in ethics and law SURVEILLE contributes to deepening the understanding of the legal notions of privacy and data protection, and of related ethical issues that are all often distorted in public discourse. SURVEILLE strives to produce a new understanding of the process and outcomes of introducing Privacy by Design features into technology. It is able to provide decision-makers with a better understanding of the impacts of different surveillance systems. It will help those manufacturing, commissioning, exporting, and using surveillance technologies better to adapt surveillance systems and their deployment to improve security, comply with ethical principles and legal limitations including those resulting from privacy and other fundamental rights, and to take into account the expectations and perceptions of the public.

The multidisciplinary methodology developed in SURVEILLE for assessing surveillance technologies and their use in varying situations, as presented in project deliverables, including D2.6 D2.8 D2.9 D3.9 and D4.10 and as popularised at the end of the project’s funding period in the SURVEILLE Briefing Note, provides for a structured and rational decision-making process over the use of surveillance, including the choice of the most appropriate methods of surveillance all-things-considered.

The results of SURVEILLE dismiss categorical views, such as that all surveillance is bad and will unavoidably result in the erosion of privacy and other fundamental rights and the creation of a surveillance state, as well as the opposite view that security, as an individual right or a collective interest, would always trump privacy and other fundamental rights. The outcomes of SURVEILLE demonstrate that in a structural and rational process of assessment and decision-making there is a proper place for ‘balancing’, i.e. a comparison between the proven security benefit and the adequately determined level of intrusion into privacy and other fundamental rights. In the SURVEILLE methodology, this ‘balancing’ must take place on the basis of the concrete facts concerning a usage situation, a specific technology, and the actual impacts of the use of that technology.

The ‘usability score’ as defined in the SURVEILLE methodology, is based on ten different factors that, inter alia, attest to the actual benefit towards better security delivered by the technology, its financial costs and its capability of incorporating Privacy by Design features. The higher the usability score is, the more likely it is that a specific form of surveillance in a specific situation will meet the legal requirements of serving a legitimate aim and being necessary in a democratic society. In a proportionality assessment, or a process of ‘balancing’, the usability score will nevertheless need to be compared against the ‘fundamental rights intrusion score’ resulting from three factors, namely an assessment of the weight of the particular dimension of privacy or other fundamental right affected by the surveillance measure in question, a similar assessment of the depth of intrusion into that right, as caused by surveillance, and a reliability factor based on the existence or non-existence of authoritative case law by the European Court of Human Rights or the Court of Justice of the European Union. The higher the fundamental rights intrusion score is, the more likely it will be that a particular form of surveillance will not pass the proportionality test, even if its usability score is also high. In the SURVEILLE methodology, the holistic process of reconciliation between the usability score and the fundamental rights intrusion score is informed by the separate ethics assessment, namely the mapping of possible moral hazards of the use of surveillance. Ethical risks were categorised as low, moderate or high, represented by different colour codes (respectively, green, yellow and red). Their inclusion in the overall reconciliation secures that the ultimate proportionality assessment will not be simply a matter of comparing the two numerical scores resulting from the two other assessments but that it will look into all aspects of the situation. In some cases, the overall assessment will result in approving the use of a particular surveillance technology in a given situation. In some other cases, it will result in the rejection of one technology, this outcome calling for the search of alternative methods of surveillance that would be less intrusive but would not compromise the security benefit delivered. Perhaps most important, however, is a third category where the holistic reconciliation between the three expert assessments will result in a need to redesign the technology or its specific use. Here, the notion of Privacy by Design becomes a central component of the SURVEILLE methodology. The inclusion of Privacy by Design features in a technology will increase its usability score, lower its fundamental rights intrusion score, and in many cases help to alleviate also the moral hazards identified. In short, the SURVEILLE methodology acknowledges the
potential of Privacy by Design features in creating a win-win situation. Through such improvements, a technology that was originally rejected, may become approved for use.

The outcomes of SURVEILLE are important for European surveillance technology design, manufacture, export, deployment and use. By subjecting the existing or future technologies to the assessment methodology developed in SURVEILLE, Europe can make sure that most effective and efficient methods of surveillance are chosen and that they are used in ways where the unavoidable intrusion into privacy and other fundamental rights in minimised and always kept proportionate to the security benefit obtained through surveillance. The methodology provides prospects for certification of technologies, including for export to non-EU countries and for Privacy by Design features. By following this path, European technology producers and exporters, as well as those deciding about the deployment and use of surveillance, can make sure that surveillance is conducted in forms that are capable of meeting the acceptance of the population.

For securing the lawfulness, ethical acceptability and actual acceptance by the population, surveillance needs to be subject to transparency and effective oversight. SURVEILLE provides the necessary tools for Europe choosing that path. Its multidisciplinary and multidimensional assessment methodology over concrete usage situations of surveillance technologies can also be applied by courts or other oversight bodies. Instead of applying an abstract approach of ‘balancing’ between important societal values such as security and privacy, they will be able to make informed, structured, and controllable decisions based on the actual effectiveness, efficiency, moral hazards and fundamental rights intrusion of any surveillance technology. Effective oversight, in turn, is crucial for obtaining acceptance among the population for chosen methods of surveillance.

The dissemination activities of SURVEILLE were reported in three dissemination reports that all are in the public domain, deliverables D6.3 D6.4 and D6.5. In addition, public deliverable D6.6 is a separate report on the most important dissemination event of the project, a Final Conference in May 2015. Through its inclusion in the broader State of the Union Conference convened by the EUI, the project managed to secure the attention of major European policy-makers and major media outlets. The list of dissemination activities submitted in this Final Report comprises 137 entries.

Through its three Annual Forums for Decision-Makers and its Internet portal, blog and Twitter feed, SURVEILLE has been continuously contributing to a better informed European, national and international discussion of efficiency, ethics and fundamental rights considerations in respect of the use and development of surveillance technologies. SURVEILLE sought direct engagement with European-level decision makers throughout its life and will continue to do so after the close of its funding period. The project has direct and continuous contact with the Council (the office of the EU Counter-Terrorism Coordinator), the Commission (DG Migration and Home Affairs) and the Parliament (the LIBE Committee and its Secretariat).

List of Websites:
SURVEILLE website: http://www.surveille.eu
Contact details for the consortium leader: Professor Martin Scheinin, European University Institute, Department of Law, Via Boccaccio 121, 50133 Florence, Italy. Phone +39 055 4685 589. E-mail martin.scheinin@eui.eu

Related information

<table>
<thead>
<tr>
<th>Result In Brief</th>
<th>Surveillance technology assessed for usability, cost, ethics and legality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documents and Publications</td>
<td>final1-surveille-briefing-note-and-dss.pdf</td>
</tr>
</tbody>
</table>

Reported by
EUROPEAN UNIVERSITY INSTITUTE