RESPECT

Rules, Expectations & Security through
Privacy-EnhancedConvenient Technologies

Project Publishable Summary

1. Publishable summary

Summary description of project context and objectives

Convenience and cost-effectiveness are the two key considerations for both citizens and law enforcement and intelligence agencies when deciding which technologies to embrace or avoid in the Information Society. State actors and private corporations adopt information communication technologies (ICTs) because they are cost-effective. The motivation for adoption may be different in the private and public sectors but once adopted these ICTs are then capable of being bridged in multiple ways permitting police/intelligence agencies to go beyond the data they gather directly but also increasingly tap into data gathered and stored by private corporations. These ICTs, which have to date gone through a period of largely organic growth, will be deemed to be “in balance” if they are implemented in a way which respects individual privacy while still maximising convenience, profitability, public safety and security.

RESPECT investigates if the current and foreseeable implementation of ICTs in surveillance is indeed “in balance” and, where a lack of balance may exist or is perceived by citizens not to exist, the project explores options for redressing the balance through a combination of Privacy-Enhancing Technologies and operational approaches. Investigating at least five key sectors not yet tackled by other recent projects researching surveillance (CCTV, database mining and interconnection, on-line social network analysis, RFID & geo-location/sensor devices, financial tracking), RESPECT also carries out quantitative and qualitative research on citizens' awareness and attitudes to surveillance.

RESPECT produces tools that will enable policy makers to understand the socio-cultural as well as the operational and economic impact of surveillance systems. The project has three sets of outcomes:

a. a draft model law on surveillance safeguards – this is model law lays down safeguards to protect the fundamental rights and freedoms of individuals when surveillance systems are deployed and used, as well as when non-surveillance data are used for the purpose of surveillance.
b. a decision-support tool aimed at assisting decision makers entrusted with the acquisition of new surveillance technologies – this decision support tool includes basic indicators for assessing the legal basis; assessing the impact on citizens' privacy; promoting privacy by design and by default; economic cost and social costs of the proposed system.
c. a set of policy recommendations that follow from the findings of research carried out within this project.

The project's main objectives are to:
1. Review the actual effectiveness of surveillance systems and procedures used in Europe in preventing/reducing crime; and in tracking evidence for improved prosecutions of crimes and acts of terrorism.

2. Identify and examine the social and economic costs involved in the adoption and implementation of identified surveillance systems and procedures.

3. Determine the legal basis adopted for these systems and procedures, identifying best practices that have evolved from the legal basis and lacunae that may exist.

4. Explore European citizens' awareness/acceptance of surveillance systems and procedures based on attitudes to efficiency, economic and social costs.

5. Identify the possible effect of cultural influences on citizens' acceptance of surveillance systems and procedures.

6. Compare and/or further develop findings on these systems, procedures and attitudes with findings found in the FP7 CONSENT and SMART projects.

7. Establish best-practice criteria developed on the basis of operational, economic, social and legal efficiency and citizen perceptions

8. Develop a tool-kit capable of pan-European application composed of three main items: a) a matrix-style checklist incorporating operational, technical, economic, social, and legal factors which can be used as a decision-support tool for policy-makers assessing systems specifically designed for surveillance; b) system design guidelines; and c) Model force-level regulations which can be adopted by a police force for when deploying surveillance systems including large-scale integrated systems.

Based on the findings of the research project, this eighth objective has been revised to develop: a. a model law laying down safeguards to protect the fundamental rights and freedoms of individuals when surveillance systems are deployed and used, as well as when non-surveillance data are used for the purpose of surveillance; b. a decision-support tool for policy-makers assessing systems specifically designed for surveillance; c. list of policy recommendations that reflect full awareness of the economic and social costs, (lacking) legal frameworks and citizens' attitudes towards surveillance.

Description of work performed and main results

The project aims to produce a balanced and well-rounded approach to identifying the opportunities and risks inherent to the use of surveillance in a society where privacy and data protection are fundamental rights. This will in turn produce tools that will enable policy makers to understand the socio-cultural as well as the operational and economic impact of surveillance systems. Additionally the project will develop a. a decision-support tool for policy-makers assessing systems specifically designed for surveillance taking into account legal, privacy economic and societal implications in account; b. a draft model law on surveillance and safeguards for persons subject of surveillance; c. list of policy recommendations that reflect full awareness of the economic and social costs, (lacking) legal frameworks and citizens' attitudes towards surveillance.

First 18 months (1 February 2012 till 31 July 2013)

In the first 18 months of the project (1 February 2012 till 31 July 2013) the project prepared a classification of surveillance methods (WP2). This classification was used as a basis on which a status quo analysis of five key sectors - CCTV (WP4), database mining and interconnection(WP5), on-line social network analysis(WP6), RFID & geo-location/sensor devices(WP7) and financial tracking (WP8) – was carried out. For each of these key sectors, RESPECT partners examined the surveillance practices in each sector, an analysis of the costs of these practices and the impact on privacy of these sectors.

The status quo analysis did not deal solely with applications of surveillance on a sector-by-sector basis (WPs4-8). It also mapped out characteristics of laws governing surveillance and identified lacunae/new safeguards as well as best practices (WP9). By thus combining an analysis of how, why and when surveillance may be used in multiple application sectors, and a complementary structured understanding of the legal framework to follow under the impact stream, the status quo analysis provides the prerequisite knowledge to enable the RESPECT team to move on to examine citizen attitudes before venturing to come up with the final design solutions and new operational safeguards. In parallel to the status quo analysis, three sets of theoretical frameworks were developed: an impact assessment framework (WP3); a framework to measure the economic costs of surveillance (WP10) and a draft road map to map the social costs of surveillance (WP 13).

There are a number of findings that are common to all the different key sectors under review, namely that gradually more of the technologies used in surveillance are 'smart', that is some degree of automation in the surveillance is present. This development necessitates even more that economic, social and privacy costs are included in impact assessments of surveillance systems at the start and duration of the use of the system. These impact assessments have by and large been missing so far, mostly because there are few methods so far to measure the economic, social and legal costs of systems, as was found out in the research carried out in WP9, 10 and 13.

The results of the research carried out in the first 18 months of the project have been presented during the first RESPECT Policy Workshop – "OPENSUR-2013: Privacy Enabled Surveillance?" held in Ljubljana, Slovenia on 2-3 July 2013. The aim of the workshop was to present the findings of the research carried out and to discuss with stakeholders the implications of these findings. 60 participants attended among which invited speakers from the Slovenian Data Protection Commission, Yorkshire & Humber Police, United Kingdom, Dutch National Police, Big Brother Watch, United Kingdom, researchers from the IRISS and SURVEILLE projects.

Second 18 months (1 August 2013 – 31 January 2015)
Based on the work in the first 18 months, the second 18 month period (1 August 2013 – 31 January 2015) focused on the quantitative (WP11) and qualitative (WP12) measurement of citizens' attitudes towards surveillance systems and procedures.

In the quantitative measurement of citizens' attitudes, a total of 5,361 individuals from 28 countries completed a specifically prepared questionnaire. The questionnaire was available online in all languages of the European Union between November 2013 and March 2014. Additionally, the questionnaire was administered in a number of face-to-face interviews in order to also reach those citizens who do not use the internet. From the responses, it can be assumed that the majority of respondents to this survey are frequently exposed to a variety of surveillance measures that are intended to fight crime. For thirteen European countries (Austria, Bulgaria, Czech Republic, Germany, Italy, Malta, Netherlands, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom) the number of respondents met the required target quota (sample of 3,115 respondents) to be representative, on age and gender, of that country's population aged 18 years and above. While a full report of the key findings with potential policy implications can be found in Deliverable 11.3, we report here some key findings. These include that:

1. Citizens show two distinct, and very different, reactions to surveillance. Some people feel secure in the presence of surveillance, whilst in others surveillance produces feelings of

insecurity. But, overall, more citizens feel insecure in the presence of surveillance than secure in the presence of surveillance.

2. Citizens who consider themselves to live in an area with increased security risks also show this same pattern of results.

3. Only a minority of citizens feel that they are well informed about laws and regulations regarding the protection of personal data gathered via surveillance, and only a small minority feel that these laws and regulations are effective.

4. Although overall the majority of citizens feel insecure rather than secure in the presence of surveillance, amongst those citizens who perceive laws and regulations regarding the protection of personal data gathered via surveillance as effective, the majority feel secure in the presence of surveillance. Increasing the perceived effectiveness of data protection laws related to surveillance may increase citizens' feelings of security in the presence of surveillance.

7. The link between perceived effectiveness of laws and regulations and citizens' feeling of security/insecurity in the presence of surveillance is stronger than the link between perceived effectiveness of surveillance measures themselves and feelings of security/insecurity

8. A majority of citizens feel that they have no or little control over the processing of personal information gathered via surveillance measures, and they have no or little trust that government agencies or private companies protect this personal information. This perceived lack of trust is particularly strong in relation to the data handling of private companies. There is a generally strong perception of the risk of data misuse and misinterpretation.

8. A majority of citizens feel that most types of surveillance have a negative impact on their privacy (except CCTV), and they generally perceive a great risk of privacy violation.

10. Financial compensation against greater privacy invasion through surveillance is not acceptable to a majority of citizens.

In the qualitative measurement of citizens' attitudes, focus groups were carried out in 14 countries, namely Austria, Bulgaria, Czech Republic, Germany, Italy, Malta, the Netherlands, Norway, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom. The focus group discussions were carried out amongst three age groups.

Several key findings and common themes have emerged from the analysis and comparison of all the 14 country focus group discussions. The findings are explained in detail in deliverable 12.3. These include, among others, that,

1. There was a recurring idea across many groups that instead of increased surveillance, more policemen or security guards should be preventing crime, especially on the street. The predominant perception was that if people see policemen then they would know that they can receive help in case of any need. Technical surveillance systems would not necessarily give people such feelings of security.

2. Beside CCTV, financial tracking was seen as one of the most convenient methods for purposes such as the prevention of money laundering and verifying of financial transactions.

3. Another surveillance technology perceived by many participants as rather convenient was GPS technology that helps to locate people in an emergency. On the other hand, they saw GPS tracking as the most privacy invasive technology, because, unlike CCTV cameras, they felt that it cannot be ensured that locations are observed only in certain circumstances. Besides, it was seen to be more 'personal', detailed and practically unavoidable.

4. Participants had difficulties in discussing cost efficiency, as no costs associated with the surveillance measures were defined and no such information is normally publicly available. In some groups, participants perceived the use of the newly introduced surveillance measures in the scenario as an additional threat to their privacy. They did not feel that the

safety level would rise as a result of these measures. On the contrary, they argued that people could feel criminalized and their rights could be limited.

5. Some participants felt there should be more of a focus on measures that would eliminate the causes for the change of the security climate or increased lawlessness, rather than on introducing additional surveillance measures.

6. Nearly all participants trusted the state more than private companies to manage their personal data collected via surveillance services. The main reasons were that private companies were perceived as complying with fewer legal requirements and that they are commercially driven rather than serving public interests. Despite trusting government agencies more than private companies, the participants perceived government agencies to be less effective in some countries (such as Slovenia) and consequently, less able to efficiently process (but also potentially misuse) personal information.

7. A number of participants believed that laws relating to data protection sometimes contradict each other and can be broadly interpreted. For many participants, therefore, they do not represent comprehensive safeguards because they depend additionally on the interpretation of judges or lawyers. This is where, some participants felt, the EU needs to do more. Having said that, they felt there would be limited benefits to improving privacy laws, if those individuals who are handling personal data are not independently scrutinised and managed themselves. Any databases containing personal data should, thus, be properly protected and a strict authorisation procedure for their users should be implemented.

8. Many participants held a view that people are not given the option of opting out of surveillance technology and services, because they have become a social and technological standard. There was also perceived to be a massive change in the way people communicate – everything is done digitally, but not everyone is aware that surveillance may be being carried out.

Two more WPs were active during the second 18 month period of the RESPECT project: WP14 and WP15. The aim of WP14 was to review the work of other security related research and to analyse their implications for the RESPECT project and to indicate some policy conclusions based of the relations between the findings in RESPECT and in other projects. During this second period, WP14 reviewed the research of the following projects: CONSENT, SMART, IRISS; SURVEILLE; DETECTER; SAPIENT; PRESCIENT; PRISMS; SurPRISE and PATS. Detailed policy implications of these projects is found in deliverable 14.3.

Following the results of the research carried out in WP2-WP14, it became increasingly evident that the objectives originally planned for WP15 had to be modified. Primarily the objectives of drafting model force-level regulations and system design guidelines could not be achieved at this stage of development of the current legislative framework at a European level and at a national level (as should be evident from the research carried out of the review of laws and other regulations governing surveillance (WP9).

Amongst the overall findings of WP9 (and other work packages, e.g. WP4 – CCTV) is that the use of surveillance technologies is often only regulated partially, if regulated at all. Furthermore only particular categories of surveillance technologies are regulated or only particular sectors are regulated. This creates a situation of inconsistencies and lacunae. It was therefore considered to be premature to draft model force-level regulations or system design guidelines while a consensus about the regulation of such matters at a European or national level is lacking.

Moreover, from the research carried out in WP4-8, 9, 11, 12 and 14, and from developments that happened during the course of the project, it was increasingly noted that one of the major issues with the use of surveillance technologies is that the rights of individuals subject of surveillance are rarely provided for at law. In essence, individuals who are the subject of surveillance have few legislative safeguards and remedies if their rights are breached. Furthermore from the research of the SMART project[1] and the discussions held within that project with stakeholders on the model law on smart surveillance technologies, it was seen that a need for a regulatory framework laying down safeguards to protect the fundamental rights and freedoms of individuals was necessary not only when smart surveillance systems were being used but whenever surveillance systems were being used. A broad, across surveillance systems, regulatory framework was missing and necessary.

All these considerations led the Consortium to revise the objective of WP15 to focus on the creation of proper foundations for European consensus on a legislative approach to surveillance. This now takes the form of a model law laying down safeguards to protect the fundamental rights and freedoms of individuals when surveillance systems are deployed and used, as well as when non-surveillance data are used for the purpose of surveillance. Hence the project embarked on an equally ambitious task of preparing a draft model law on surveillance safeguards, while also building on the results of other European collaborative research projects in the SEC area.

A second policy workshop on citizen attitudes and criteria for fairness was held on 17-18 September 2014 in Barcelona. The workshop – "Technology and Crime: Law, Privacy and Policy in the Era of Big Data"[2] - was well attended (more than double the participation originally planned) with participants from Europe and beyond presenting related work and contributing constructively to the project. Invited guests included the Chief Executive of the Association of Chief Police Officers, UK; a member of the prosecutor's office in Norway, senior police officers from Spain, representatives of the cities of Barcelona and Vilvoorde (Belgium) and stakeholders from the private sector from the Netherlands and Spain. The relative proceedings have been submitted to the EC (D.17.3). In this workshop the preliminary results from the quantitative and qualitative measure of citizens' attitudes to surveillance systems and procedures were reported on and discussed with the participants.

A Joint Final Event – between the RESPECT, SURVEILLE, IRISS projects - was held on 29-30 October 2014 in Brussels. The event – called "DEMOSEC: Democracy and Security"[3] - brought together the research and results of the three projects – RESPECT, SURVEILLE, IRISS. It was very well attended by a large variety of stakeholders including European policy makers, national policy makers, private sector representatives, law enforcement and intelligence services representatives. In preparation for the Joint Final Event, the RESPECT consortium worked on preparing policy conclusions from the RESPECT project. These policy conclusions/implications were then added to the policy conclusions and implications of the SURVEILLE and the IRISS projects in a joint policy brief which was publicly discussed in the final session of the Joint Final Event.

Last 4 months (1 February 2015 – 31 May 2015)

The last 4 months of the project focused primarily on the finalisation of the reporting on the quantitative and qualitative measurement of citizens' attitudes towards surveillance systems and procedures (WP11 & WP12).

Various informal meetings with stakeholders were organised to discuss the various drafts of the model law on surveillance safeguards prepared as part of WP15.

The results of all the project were presented during a three-day final conference – "Security, Convenience and Privacy: Trade-offs in the information society?"[4] held on 20-22 April 2015 in Brussels. It was very well attended by a large variety of stakeholders including European policy makers, national policy makers, private sector representatives, law enforcement and intelligence services representatives. One day of the conference was entirely dedicated to discussing the draft model law prepared by WP15 with the various stakeholders. The open and frank discussion that took place was very useful for the preparation of the next version of the draft law (submitted as deliverable 15.2).

Expected final results and potential impacts

RESPECT has been designed to contribute to several impacts/goals listed in the relevant call and the Security Work Programme 2011. The specific call that RESPECTS fell under (SEC-2011.6.1-5) explicitly stated that "The outcome of the work should provide decision- makers with a better understanding of the impacts of different surveillance systems, and also help manufacturers and end-user better adapt the systems and their deployment." Furthermore, it is specifically seeks to ensure, also in line with the Work Programme, that the impact of the proposed technologies on the society, the organisational processes and the respect of legal requirements, such as respect for fundamental rights are embedded in the deliverables ensuing from this project.

The project findings from RESPECT will deliver to policy makers a toolkit which will provide:

a. a draft model law on surveillance safeguards – this is model law lays down safeguards to protect the fundamental rights and freedoms of individuals when surveillance systems are deployed and used, as well as when non-surveillance data are used for the purpose of surveillance.

b. a decision-support tool aimed at assisting decision makers entrusted with the acquisition of new surveillance technologies – this decision support tool includes basic indicators for assessing the legal basis; assessing the impact on citizens' privacy; promoting privacy by design and by default; economic cost and social costs of the proposed system.

c. a set of policy recommendations that follow from the findings of research carried out within this project.

Through the three key Toolkit deliverables outlined above, the RESPECT project would achieve an overall impact whereby many forms of surveillance may be usefully deployed to enhance security yet in full compliance with the legal principles entrenched in Article 8 of the European Convention on Human Rights, and especially with the articles 7 and 8 of the EU Charter of Fundamental Rights.

It is expected that the Toolkit produced by RESPECT will also achieve further impact through:-
- Development of industry standards: as part of the recommendations in the policy brief;

- Educational measures: Educational measures may be directed at both providers and users of many forms of surveillance.

With its extensive European coverage and its interdisciplinary focus on a the resolution of a problem that may both affect citizens' individual rights and security the RESPECT project is a prime example for research undertaken to provide guidance to policy makers in the area of security and privacy.

The RESPECT project in this reporting period has sought and found extensive and intensive engagement with its stakeholders among which Law Enforcement Agencies (e.g. via various INTERPOL regional meetings), Policy makers, Civil Society other relevant FP7 projects and during the Final Conference in April 2015.

[1] Scalable measures for automated recognition technologies Grant Agreement 261727.
[2] http://respectbarcelona.eu/
[3] http://www.jointfinalevent2014.eu/
[4] http://conference.respectproject.eu/