FP7-285556 SafeCity Project

Draft Deliverable D7.2

Title: SafeCity Policy Making

Deliverable Type:	**CO**
Nature of the Deliverable:	**O**
Date:	**21/03/2013**
Distribution:	**WP7**
Editors:	**ARATOS**
Contributors:	**HI-IBERIA, MCC, KEMEA, EVERIS**

***Deliverable Type:** *PU= Public, RE= Restricted to a group specified by the Consortium, PP= Restricted to other program participants (including the Commission services), CO= Confidential, only for members of the Consortium (including the Commission services)*

**** Nature of the Deliverable:** *P= Prototype, R= Report, S= Specification, T= Tool, O= Other*

Abstract: This document overviews the defined resolution activities and accordingly supported legal documentation required to comply the SafeCity project against social, ethical and legal implications.

DISCLAIMER

The work associated with this report has been carried out in accordance with the highest technical standards and SafeCity partners have endeavored to achieve the degree of accuracy and reliability appropriate to the work in question. However since the partners have no control over the use to which the information contained within the report is to be put by any other party, any other such party shall be deemed to have satisfied itself as to the suitability and reliability of the information in relation to any particular use, purpose or application.

Under no circumstances will any of the partners, their servants, employees or agents accept any liability whatsoever arising out of any error or inaccuracy contained in this report (or any further consolidation, summary, publication or dissemination of the information contained within this report) and/or the connected work and disclaim all liability for any loss, damage, expenses, claims or infringement of third party rights.

List of Authors

Partner	Authors
ARA	Nikos Bogonikolos , Giorgos Kostopoulos, Stratoula Kalafateli
EVR	Mario Carabano
HIB	Roberto Giménez, Raul Santos, Diego Fuentes
MCC	Fernando Garcia
KEM	George Leventakis, Georgios Eftychidis, Lilian Mitrou

Document History

Date	Version	Editor	Change	Status
20120321	0.1	[ARA] Nikos Bogonikolos, Giorgos Kostopoulos, Stratoula Kalafateli	Constructing the skeleton of the report	Draft
20120430	0.2	[ARA] Nikos Bogonikolos, Giorgos Kostopoulos, Stratoula Kalafateli	Updated structure, sent for initial partners' contribution	Draft
20120914	0.3	[ARA] Nikos Bogonikolos, Giorgos Kostopoulos, Stratoula Kalafateli	First draft of the deliverable, sent for partners' contribution	Draft
20130315	0.4	[EVR] Mario Carabano, [KEM] George Leventakis, Georgios Eftychidis, Lilian Mitrou, [MCC] Fernando Garcia, [HIB] Roberto Giménez, Raul Santos, Diego Fuentes	Partners Contributions	Draft
20130320	0.5	[ARA] Nikos Bogonikolos, Giorgos Kostopoulos	Pre-Final, ready for review version	Pre-final
20130328	0.6	[ARA] Nikos Bogonikolos, Giorgos Kostopoulos	Final Version	Final

Table of Contents

List of Figures

List of Tables

Glossary

Acronym	Meaning
ICT	Information and Communication Technology
EU	European Union
FP7	Framework Programme 7
EC	European Commission
PS	Public Safety
UC	Use Case
PoC	Proof of Concept

References

Number	Reference
[1]	Safecity Deliverable D7.1, Social, Ethical and Legal Implications
[2]	ICT Research -The policy perspective: Freedom in europe, Securing our Technological Future, European Commision Information Society and Media
[3]	Institutions and member states of the European Union, "Charter of Fundamental Rights of the European Union", 7 December 2000. Available online at http://en.wikisource.org/wiki/Charter_of_Fundamental_Rights_of_the_European_Union
[4]	EU Member States, "The Treaty on the Functioning of the European Union", 13 December 2007, Lisbon Portugal. Available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:en:PDF
[5]	Digital Agenda: http://ec.europa.eu/digital-agenda/

1. Introduction

1.1 Scope and purpose of this document

This document aims to define policy making activities in the SafeCity project according to Public Safety UCs. The deliverable is going to be the result of a continuous research and consists of basic guidelines and restrictions to be adopted after the project end, upon dissemination and exploitation activities of the SafeCity project.

The SafeCity project makes use of advanced networking and situational awareness technologies, studied at the level of functionalities (SafeCity WP2), an analysis of technical requirements (SafeCity WP3) and an actual experimentation plan (SafeCity WP4). During the project's lifetime the legal framework concerning individual rights that is in force both in EU and the respective milestone has been analyzed, the social implications related to problems raised within the society from the application of new policy, methodology and technology and the ethical implications focusing on the individuals have been investigated and gathered to Deliverable D7.1 [1].

The current document is developed in parallel with SafeCity deliverable D7.1 [1] which explores the legal, social and ethical implications arising during the implementation of the SafeCity project.

1.2 SafeCity policy making activities

The current document presents an overview of the strategy actions to be applied for the implications defined in D7.1.

Section 2 presents the importance of ethics in ICT Research and in Monitoring & Surveillance Research and makes a reference to the ethical implications that have been identified and analyzed at the SafeCity Deliverable 7.1 [1] and provides some general guidance upon resolving those.

Sections 3 presents an overview of the social implications as have been recognized during the implementation of the SafeCity project [1] and underlines the importance of social impacts.

Section 4 underlines the importance of legal aspects in Public Safety and Security, presents the legal framework concerning individual rights that is in force both in EU and the respective milestone and provides some general legal considerations about the current EU legal framework.

Section 5 presents an in-depth analysis of the implications concerned with each task in the SafeCity project and how this is being accordingly treated.

2. The Importance of Ethics in Research

2.1 Ethics in ICT Research

In recent years there has been an increase in the importance of ethical issues related to ICT research and technological developments. The ICT research and technological developments should follow principles regarding dignity, freedom, equality, solidarity, citizens' rights and justice. Researchers should comply with national legislation, European Union legislation, respect international conventions and declarations and take into account the Opinions and Recommendation of Ethics Councils, Commissions etc. with focus on the Opinions issued by European Group on Ethics. However, consideration of ethical issues goes beyond simple compliance with current regulations and laws.

The right to privacy and the right data protection are fundamental rights and as they are strictly related with the dignity and the personality of an individual they are of crucial importance for ICT research. The majority of European citizens view personal privacy as an important issue. For that reason researchers have to ensure that the methodology and the means of research do not contravene the right to privacy and data protection.

The emergence of increasingly unpredictable, uncertain and unquantifiable benefits and risks associated with ICT research indicates the need to establish a procedure that will critically reflect on the ethical, social and sometimes environmental implications of both the development and usage of ICT. A procedure that will embed ethical considerations in ICT by discussing the needs and goals of the society and then serving as a framework to guide research towards these goals. That procedure is called **ethics reviews**.

Ethics review is an integral part of research ethics that promotes the adherence to ethical norms in research so as to maintain the aims of research, such as knowledge, truth, avoidance of error and harm. Ethics reviews are processes set up to find out if ethical norms are respected during research. This process understands the ethical norms involved in the research, discovers both actual and potential ethical problems associated with the research and makes certain these norms are adhered to and the problems get effective solutions. Owing to the dynamic nature of ethical problems, ethics reviews are based on a process that operates both before, during and after the research. This helps in developing a guideline that makes research effective.

This Deliverable aims to deliver the basic guidelines and restrictions after the project end, upon dissemination and exploitation activities of the SafeCity project. Ethics reviews developed at D7.1 [1] took an important role to identify the guidelines and restrictions presented in Section 5.

2.2 Ethics in Monitoring & Surveillance Research

A lot of studies and work have been made regarding the ethics in surveillance research. The D7.1 [1] has tried to summarize the basic ethical implications arisen from the usage of surveillance technologies. Ethics in Monitoring & Surveillance Research are crucial as the surveillance itself is imminent to human rights' laws. Possible subjects for discussion arise concerning the usage of surveillance technologies such as:

- What are justifiable reasons for surveillance?

- Are there categories of people who should be immune from surveillance?
- Is intention relevant to surveillance?
- Is there a default right not to be surveilled?
- How should the question of legitimate authority be addressed in surveillance?
- Is there such a thing as harmless surveillance?
- When does surveillance become necessary?
- Are all the legal limitations kept when establishing a surveillance system?
- Incorporating ethics in surveillance research is vital for protecting fundamental values for both the individual and the society, ensuring that values such as dignity, equality and respect for privacy, are not infringed or jeopardized in a disproportional way and extent. Privacy meant as dignity and protection of personal autonomy is strictly interrelated with surveillance and is essential for the surveillance researcher to ensure that all legal conditions and requirements have been taken into consideration and that the surveyed persons, in our case the citizens, are aware of the fact of monitoring and their rights.

2.3 Ethical considerations

At Deliverable 7.1 [1] the ethical considerations are identified, summarized here in Table 1. As described above it is very essential to take the ethical part under consideration while establishing a surveillance system based on modern technology, ICT and automation.

The ethical considerations raised concern the infringement of fundamental rights and liberties and the lack of respect to the citizen's privacy and anonymity. The competent authorities and the responsible personnel must take care of the personal data of the citizens ensuring that the citizens are aware of being monitored, their personal data are not going to be transmitted or in any way disclosed to third parties or used in an unlawful way and that their fundamental rights and freedoms are protected by the EU Legal Framework and the national laws of the European countries each citizen belongs to.

Table 1: Ethical Considerations and suggested resolution activities

Reference Name	Full Name/ Type	Level (EU, local)	Suggested Resolution Activities
EC.1	Fairly and lawfully processed personal data	EU, local	1. The citizen has to be aware of his rights 2. The citizen has to be aware that he is being monitored 3. The data processor has to be controlled on a continuous basis 4. Data access should be restricted to authorized personnel, via the

			introduction of authentication processes and dynamic password level accesses
EC.2	Processed for limited purposes personal data	EU, local	1. The data processor/controller has the duty to define precisely the purposes of his processing and to make them explicit 2. The data gathering should be checked by third independent parties, in order to ensure that the data are not used for illegal purposes or for purposes different than they were collected for
EC.3	Adequate, relevant and not excessive personal data	EU, local	1. The collected data should be checked by third independent parties to ensure that only the necessary data have been gathered 2. In case of gathering "useless" personal data they should be immediately deleted 3. Legal control of the data gathering and processing procedures 4. Masking capabilities to the sensors (cameras) to avoid any incidental data collection
EC.4	Accurate personal data	EU, local	1. Legal control of the data gathering procedure 2. Supervision of the data collectors and the decision making personnel 3. Data Subject access to personal data processed
EC.5	Data should not be kept longer than necessary	local	1. Define a period of time for storing the data 2. Data need to be stored in a secure located, interconnected only with local private network of high security 3. Automatic destruction of the data after the allowed timeframe already defined
EC.6	They have to be processed in accordance with data subjects rights	local	1. Legal control of the gathering and processing procedure 2. Informed consent should be acquired from the respective authorities of the area where the framework is expected to be applied

			3. Subjects rights respect
EC.7	They must be securely exchanged via encryption mechanisms	local	1. High security measures should be taken in all communication channels 2. Data access should be given only in authorized personnel 3. The data exchange should be validated and checked frequently 4. High security techniques to ensure safety of the data from malicious attacks
EC.8	They must not be transferred to countries without adequate data protection	EU, local	1.Special policies have to be designed for handling data amongst different countries 2. All parties involved should record the measures taken in order to ensure that transferred data flow is compliant with the requirements of the law 3. All parties involved in data exchange and transfer should report the data movement's, the reasons to be transferred at any time following the EU Legal framework and the national laws
EC.9	They must securely be destroyed after their usage with absolutely no chance of retrieval	EU, local	1. A timeframe should exist on how long the data will be available for access 2. Erase mechanisms should be developed in order to ensure that there is no chance to be retrieved by anyone 3. The erase processes must be checked frequently
EC.10	Citizens must be aware of being under surveillance and others have access to their personal data	local	1. The authorities must inform the citizens of: - their rights -the areas under surveillance -the reasons to be surveilled -what kind of data are to be acquired 2. The involved parties must give access to the citizens to their personal data
EC.11	Define the criteria under which a citizen is marked	EU, local	1. The authorities must define policies regarding the objects/citizens who might be

	as suspicious		characterized as suspicious 2. The citizens should be aware of these policies
EC.12	Secure storage and management of the personal data	EU, local	1. Data need to be stored in a secure location, interconnected only with local private network of high security 2. The data access in the database should be restricted to authorized personnel only 3. The data storage and the personnel who have access to them must be frequently checked 4. Develop security mechanisms to all communication channels
EC.13	Objective interpretation of data content	EU, local	1. The decision making process must be developed by a team of experts 2 The decision making process should not only be based on the results of the automatic system but on the evaluation of the expert's team
EC.14	Respect the citizen's privacy and individuality – try to keep the anonymity	EU, local	1. Nobody should have access to the stored data with the exception of the specifically authorized authority and personnel. 2. The personal info of the citizens must be revealed to authorities only in case of prosecution of crime
C.15	The cameras should be located in such way so as to not record through a resident's window	local	The sensors / cameras must have special filter capabilities and must be correctly programmed to avoid the recording of data through a resident's window
EC.16	The citizens must be aware of the fact that they are monitored, of their legal rights and of the impact on their lives	EU, local	As EC.10
EC.17	Information input into the databases is prone to human and device error	EU, local	This policy must be taken into account during the decision making process
EC.18	Respect to the citizen's	EU, local	1. Citizens must be aware of being monitored

	autonomy and trust		2. Citizens must have access to their personal data 3. Citizens must be aware of their rights
EC.19	Use of personal data according to human rights and democratic practice	EU, local	As EC.18
EC.20	Ensure the end-users that their personal data will not be used against them (Confidentiality)	EU, local	1. The authorities must inform the citizens about the installation of the surveillance system and take their consent in case they participate in specific actions (e.g research) 2. The authorities must convince the citizens that the surveillance measures are taken to decrease the criminality ratio in their city by increasing the level of trust of the citizens to the authorities. 3. The authorities must inform the citizens of their rights in order to gain their confidence and their trust.
EC.21	Consider the ethical cost of the applied technologies, the advantages and disadvantages (cost-benefit ratio)	EU, local	1. Before the installation of a surveillance system to an area of interest all parameters should be taken into account concerning the ethical costs, potential harms and the advantages of the installed system 2. If the citizens are strongly negative on the installation of a system in their neighborhood then this must be taken strictly under consideration
EC.22	Ensure that dignity is not violated or jeopardized at any case	EU, local	1. The involved parties must ensure the security of the personal data 2. The citizens must be aware of the data gathering and processing procedures and their rights
EC.23	People must feel free. Danger of people feeling less free because of legal public behavior like attending a political rally, entering a doctor's office, or even joking	EU, local	As EC.22

	with a friend at the park will leave a permanent record, retrievable by authorities at any time.		

3. The importance of Social Impacts

3.1. The Social aspect of Public Safety and Security

SafeCity tries to ensure citizens feel safe within their surroundings. Social implications are neither imposed by some legal party nor are they referenced in relevant legislations. They are driven by the social acceptance of the wider public and represent the social opinion and impacts, focusing attention not on the individual, as this is more apparent in ethical considerations, but rather on the society.

Public Safety is very important for the citizens as it ensures a better quality of life. An area under surveillance is less susceptible in criminal attacks and threats making citizens feel safe within their surroundings.

Live examples of usage of surveillance technologies have pointed out that the criminality ratio is significantly decreased while the majority of citizens want the installation of the systems especially in areas where the criminal attacks are often.

But there are negative social considerations that have to be taken into account regarding Public Safety and Security technologies. Some of them have arisen from the "invisible" nature of the Surveillance Systems. This has impact on democracy and raises concerns with regard to the right to privacy. A lot of surveys have indicated that the citizens do not feel free but limited and discomfort when they are under surveillance.

As it comes from the above mentioned aspects of Public Safety and Security all concerns have to be taken into account when installing a surveillance system and estimate the benefit – cost ratio in order to find out the social and ethical cost and the benefits received by the system's installation.

3.2. Social Implications turning to threats

Globalization and digital convergence in the emerging knowledge society has raised complex ethical, legal and societal issues. We are faced with complex and difficult questions regarding the freedom of expression, access to information, the right to privacy, intellectual property rights, and cultural diversity.

Two main social problems have been recognized as an incoming threat due to the increasing digitization of the information and the monitoring of a city by integrating different sensors allowing information acquisition on multiple levels and in many areas where the citizen may appear. These are:

- ✓ The phenomenon of **Digital Divide**, where the categories of people who can't access or use this kind of technology are automatically excluded (e.g. low income families, elderly people etc)
- ✓ The phenomenon of **Social Sorting,** where some target groups which want to live a simple and traditional life are excluded or forced to follow the technological privileges proposed by their society.

Social discrimination can turn as boomerang into a set of riots and crime scenes. All people regardless their age, color, wealth, political or religious beliefs etc must feel that their human rights are respected and the society has to take measures to ensure and protect it.

3.3. Social Implications

The table below summarizes all social implications that have been identified during the SafeCity project's lifetime. We have followed a dynamic approach and determined the different criteria and how they are enforced as a consequence of the technological innovations being studied.

The social implications concern the relationship between the citizens and the society and how this is affected. In the table below you can find some resolution activities suggested by us trying to protect the humans' rights and freedoms and in parallel introduce a humanistic surveillance system.

We strongly believe that the use of technology can help people feel secure in their surroundings and reduce the ratio of criminality assuring a better quality of life. If the approach is human oriented then the "citizen – society" relationship remains in balance.

Table 2: Social Implications and suggested resolution activities

Reference Name	Full Name/ Type	Level (EU, local)	Suggested Resolution Activities
SI.1	The human need for privacy and its implication and impact on democracy	EU, local	1. Inform the citizens of their rights 2. Delete the data after a preset (short) time unless they are needed for a specific purpose of law enforcement and prosecution of crime 3. Take strict security measures to ensure that the personal data are not going to be used by persons and/or third parties which are not authorized
SI.2	The privacy policy	EU, local	As SI.1
SI.3	The invisibility of the surveillance systems as the observer has to be invisible in order to not influence the subjects	EU, local	Inform the citizens of the existence of the surveillance systems, mainly by specific signs
SI.4	The processing of body and face video undermines an individual' self determination	EU, local	1. Citizens must be aware of the processing techniques and the technical possibilities/potential used 2. Processing of collected /stored data only in case of a criminal incident 3. Masking techniques in cameras to avoid any incidental data

			collection
SI.5	The citizens do not feel secure but limited	EU, local	Inform citizens of the advantages of the system and the decrease in criminality ratio wherever it has been installed
SI.6	Human rights (lack of freedom, respect to the other's privacy, freedom of the speech)	EU, local	As SI.1, EC.1
SI.7	Questions evoke about the necessity of these implications	Local	As EC.21 – take into account the cost-benefit ratio before installing the system
SI.8	Questions evoke about the impact of this kind of technologies (They can't prevent the crime from occurring nor do they examine the underlying social interactions which have led to the occurrence of the crime)	EU	The involved parties have to understand that the surveillance systems identify suspicious actions and that they give evidence if a crime takes place. They do not substitute the role of Justice
SI.9	Creating a society that's devoid of trust with respect to its citizens	Local	1. Citizens must be aware of being monitored 2. Citizens must have access to their personal data 3. Citizens must be aware of their rights
SI.10	People feeling discomfort when they know that they are monitored	Local	As EC.21
SI.11	Citizens are losing their trust towards the authorities because of the feeling that authorities are not sufficiently able to protect them or because authorities can misuse the private data	Local	1. The appropriate level of security is enforced across all communication channels, upon the according protocols, data monitoring and auditable data exchange 2. The system must be validated and checked frequently by authorized controllers 3. The system validation needs to be reported and monitored
SI.12	Concerns of the quality of	EU	Ensure citizens that the surveillance system will improve

	life		their quality of life as it will reduce the ratio of criminality in their neighborhood
SI.13	Digital exclusion of citizens not enable to have access in a smart phone	Local	1. Care from the authorities to give smart phones to any citizen that can't afford it 2. Find new solution to give access to the citizens to the proposed system (e.g. install public areas in the city where the citizens can have access to services offered by a smart phone)
SI.14	Exclusion of some target groups which want to live a simple and traditional life. It can even lead to compulsion to follow the technological privileges (Social Sorting)	Local	The proposed system will be established in areas of the city with high criminality ratio and not to the whole city
SI.15	Concerns about the minimal human intervention. A machine takes important decisions of e.g. a criminal behavior- Is the machine error free? – Accountability in case of error	EU	1. The decision making procedure must be based on the results of the surveillance system but not relied on them. 2. The final decision must be taken by a team of experts (increase the human intervention)
SI.16	Increase of stress on the surveillance professionals	EU, Local	Professional trainings must be organized to all operators in order to understand the system' equipment
SI.17	Decrease of vigilance of the human operators due to the presence of this technological eye	Local	1. Frequent check upon the human operators vigilance 2. Professional trainings upon the system's procedures and the necessity of the human intervention in the final stage of decision making
SI.18	The citizen as object of study and analysis	EU	1. The personal data must be used only for the specific purposes they were collected for 2. The personal data must be destroyed after a predefined countrywide timeframe. Further retention has to be specifically

			justified. 3. Data erase processes must be effective to ensure that no data retrieval will be possible for anyone 4. The citizens must be aware of the monitoring system 5. High security measures in all procedures and data access restricted to authorized personnel only 6. Only in specific areas
SI.19	Not democratic as individuals are restricted to being bodies without subjectivity	EU	The citizens must be aware of the monitoring system and specifically for: - their rights - the areas under surveillance - the purposes for being surveilled (advantages and disadvantages) - what kind of data need to be acquired
SI.20	Cost-benefit ratio	Local	As EC.21
SI.21	Creation of a "Big Brother" Society	EU	As SI.18
SI.22	Insecure data protection	EU	1. Ensure that the appropriate level of security is enforced across all communication channels, upon the according protocols, data monitoring and auditable data exchange 2. The parties accountable for the data management across all stages liable to report the data's movements at any time 3. Data access restricted to authorized personnel only via the introduction of authentication processes and dynamic password level accesses 4. The data need to be stored in secure databases interconnected only with private local network of high security 5. Data erase processes must be effective and ensure that the data are permanently destroyed and

			nobody can retrieve them 6. All stages must be frequently checked
SI.23	Data Subject rights	EU	1. The citizens need to know that: - Everyone has the right of access to data which has been collected concerning him/her - Everyone has the right to have his/her personal data rectified - Everyone has the right of blocking his/her data if their accuracy is contested by the data subject or the controller no longer needs them, or the processing is unlawful. - Everyone has the right of erasing his/her data if their processing is unlawful. - Everyone has the right to object to the processing of his/her personal data.

4. Legal Implications

4.1 Legal Considerations

The public expects, and on occasions demands, the state to provide for their protection. Their cultural norms are such that, notwithstanding the rarity of the occasion, becoming a victim of crime is an event likely to undermine their trust and confidence in the institutions of government responsible for their safety and security. Also, the public culture demands stability and normality.

Moreover, the culture of companies involved in the development of advanced technologies is one of exploration of the near possible. They seek to explore the realms of science and sometimes expect to develop new technologies that may, at that time, have little, or even sometimes no, practical security application. Their culture can be one that places the technological journey of exploration at the centre of their endeavor and as such may be one that is undertaken at the expense of wider considerations.

Finally, the culture of those agencies responsible for the security of citizens may sometimes be one within which the primacy of the protection of the majority could be at the expense of a minority.

Taken together therefore the cultural demands of the public – for safety, of the technologists – for advancement and security agencies – to safeguard others will mean that legal, ethical and social considerations can become a virtual battleground within which everyone loses. For example, the public can demand the state guarantees their safety but are intolerant of any loss of their freedoms and liberties. The technologists can develop solutions to problems that may not yet exist or inadvertently create new insecurities, e.g. internet pedophilia and the security apparatus of the state and private capital can be attracted to compromise, such that the rights of others are restricted.

So, the Legal aspect for Public Safety and Security is important to ensure both the security of citizens through the practical application of new technologies which are interfaced with law enforcement and the respect of all citizen rights.

4.2 Current EU Legal Framework

The EU has established a Legal Framework to protect fundamental rights and freedoms. We have gathered all EU Framework for the protection of human rights and for the protection of personal data in the following table.

Table 3: Legal Framework adopted by EU for the protection of the rights of EU citizens

	Legal Framework	**Relevant legal consideration**
	Human Rights Perspective	
LC.1	**European Convention on Human Rights (ECHR)**	Respect for private and family life, home and correspondence
LC.2	**Charter of Fundamental Rights of the**	Human dignity is inviolable

LC.3	**EU (CFREU)**	Everyone has the right to the protection of personal data concerning him or her
LC.4		Persons with disabilities have the right to benefit from measures designed to ensure their independence
	EU Legal Framework for the Right of Data Protection	
LC.5	**Directive 95/46/EC**	Principles for personal data processing
LC.6		Data subject consent for the processing of personal data
LC.7		Data quality requirements
LC.8		Security of personal data processing
LC.9	**Regulation (EC) No45/2001**	Principles for personal data processing
LC.10		Data subjects rights
LC.11		Exemptions and restrictions
LC.12	**Council Framework Decision 2008/977/JHA**	Protection of fundamental rights when processing personal data in the framework of police and judicial cooperation in criminal matters
LC. 13	**Proposal for a Directive of the European Parliament and of the Council**	Limitations to rights of the data subjects with the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.
LC. 14		Security and confidentiality measures to be adopted by the controller and processor
LC. 15	**Proposal for regulation of the European Parliament and of the council**	Principles for processing of personal data
LC. 16		Data subject right to be forgotten
LC. 17		Data protection by design and default
LC. 18	**Directive 2002/58/EC**	Security of communications
LC. 19		Confidentiality of communications
LC. 20		Data retention data must be erased or made anonymous when they are no longer required,

		except if the subscriber has given their consent
LC. 21		Penalties for data breach
LC. 22	**Directive 2006/24/EC**	Data retention security and responsible management
LC. 23		Authorized persons accessibility
LC. 24		Data destruction at the end of the retention period
LC. 25	**Directive 2009/136/EC**	Privacy and confidentiality of the processing personal data

4.3 Legal considerations

Based on the considerations regarding personal privacy and value of private data, a set of implications were considered in Deliverable D7.1 [1]. As a reminder, these implications are summarized below:

- **Collection of data/sensitive data:** SafeCity makes use of data including sensitive personal data to identify and/or exclude an individual; the collection and use of data and especially the sensitive ones have to be done in compliance with the relevant regulation in force and taking into account the basic principles of privacy and data protection such as the necessity of collection and the proportionality between the purpose to be achieved, the means used and the harm /infringement caused to citizens and their rights

- **Data storage, access and distribution, management and control:** SafeCity examines the temporary storage of sensitive data in order to allow their processing to take place. However, the data being collected and stored in the context of SafeCity, as well as future developments expected to take place upon Public Safety, need to be protected by specific and clear policies regarding the bodies being responsible for their storage and use. Sensitive data need to be stored in secure places, specially selected to serve their purpose, posing effective access control and back-up policies.

- **Data retention and secure expel:** SafeCity stores personal data during a limited and defined period of time, this issue usually differs countrywide; however, the data acquired need to be completely erased from the system according to the underlying regulations.

- **Citizen's awareness:** SafeCity proposes a complete framework for Public Safety and policy and regulatory action should be carried out with the aim of respecting the citizen's rights lawfully being informed of when, where, upon what and from whom the citizen is being monitored.

Notwithstanding the current EU legal framework, these implications are going to require additional policy and regulatory actions, that is, legal actions, in the domain addressed by the SafeCity project.

The most important legal action to be envisaged is to set up a unique European policy framework which guarantees a high level of protection for the privacy of individuals at the same time the free movement

of personal data within the European Union (EU) is regulated. This initiative should be regulated from European Commission by means and European Directive.

Obviously, the central actor responsible is the EC. The EU recognizes its role and responsibilities in the development of both policies and practices that reduce crime and risks, e.g. those posed by terrorism, etc. Furthermore, the European Countries have had to accept this Directive by means of the national acts according to Article 32 from this Directive.

Also, the Organisation for Economic Co-operation and Development (OECD) could elaborate the identified issues and prepare actions since its mission is to promote policies that will improve the economic and social well-being of people around the world. Also, European DPAs (Data Protection Authorities) could contribute to the elaboration of the identified issues and the preparation of actions since the Art. 28 of the EU Data Protection Directive promote it in this way.

Currently, the Digital Agenda for Europe is the more relevant policy initiative. The overall aim of the Digital Agenda (as part of Horizon 2020 strategy) is to "deliver sustainable and social benefits from a digital single market based on fast and ultra-fast internet and interoperable applications". The Digital Agenda recognizes seven major challenges: Fragmented digital markets; Lack of interoperability; Rising cybercrime and low trust; Lack of investment in networks; Insufficient R&D; Lack of skills; Fragmented answers to societal questions.

Several of these policy and regulatory challenges are very relevant to the implications identified in SafeCity which require such legal innovations in order to bring success. Overall, the acquisition of sensitive data and data storage, access and distribution, management and control are highly related to the Digital Agenda for Europe, through the Action 12 - Review the EU data protection rules belongs to Pillar I - Digital Single Market. In short, this action intends to review the EU data protection regulatory framework to strengthen individual rights and tackle emerging challenges from globalization and new technologies since data protection rules vary quickly and are difficult to understand.

5. Applying Social and Ethical frameworks in Public Safety Use Cases

5.1 Defining implications

Despite the importance of the Legal Framework in European and National level is very important to apply Social and Ethical frameworks in Public Safety Use Cases. In this chapter we are trying to define policies as they have been identified during the implementation of the SafeCity's Use Cases.

These policies have taken under consideration:

- ✓ The EU Legal Framework
- ✓ The national regulations in the countries where the Use Cases has taken place (Sweden, Spain)
- ✓ The social considerations identified during the implementation activities
- ✓ The ethical implications
- ✓ The Human rights
- ✓ The responsibilities of the stakeholders

The important issue is to try to find the golden ratio between the public rights and the benefits gained from using modern surveillance technologies. We have to define the lines of overlapping:

- When does technology stop being beneficial (causes more harm than good)?
- When do public rights are being taken advantage of and create lacks for citizen security?

Without a doubt the proposed technologies have made a **societal revolution** with a great reach for a better and more secure life. Technology helps enhance society's knowledge; it also gives hope to the citizens regarding their personal safety, the safety of their families and property and improves the relationship between the citizen and the authorities as people feel that they are important and protected members of the society.

The definitions of harm and good are often vague. What can seem to be beneficial at one point in time can often appear harmful in the long term, and vice versa. It is hard to predict the long term effects of any phenomenon, and modern technology is so pervasive that it is difficult to accurately understand the effect it is having now.

It goes without saying it all depends on who's behind the keyboard, which has the authority to have access in personal data. It's the same principle with the gun. It's not the gun itself, but the person behind the gun and how that person uses it.

Ethicists, philosophers, computer scientists and economists, social commentators and politicians, even teachers, have weighed in on the potential dangers of ICT, automation and surveillance technologies.

The right of handling valuable personal data by a third person, the authority to have access in all citizens' data, the monitoring and tracking of a person can give power to people which they shouldn't

have it. It can also make citizens feel insecure, less free and confident. This could cause a gap between the authorities and the citizens. For these reasons the citizens must be aware of their rights, the EU Legal Framework and the national laws be adopted to protect them. Moreover ethical and social frameworks must be applied to ensure that the personal data are not going to be used by third persons or other Member States without the permission of the persons and that the stakeholders act with respect to the citizens.

But there is another aspect that has to be taken into account. There are a lot of cases where people use their public rights in order to avoid being judged or punished for a crime they have indeed committed.

For this reason the legal, ethical and social framework has to consider how to establish its rules in order to avoid bad use of them.

5.2 Making ICT technology more legally and socially respectful

The developers and providers have to comply with legal, social and ethical considerations in order ICT technology is being applied in a beneficial way.

According to the "ICT Research: The Policy Perspective" [2], information and communication technology is vital for our security. It can protect us from threats, deliver fair and consistent justice and underpins our free and progressing society.

This Research underlines that "*it took generations to build our democratic values. Europe must now foster them and carry them into the digital age."* Indeed the citizens have to understand that ICT promises us a safer environment to live but it has to be done in compliance with democracy and human rights.

Our freedom and security – and a fair judiciary system – is enshrined in Europe at the very highest level within the **Charter of Fundamental Rights** [3] and subsequently becoming binding through the **Treaty of Lisbon** [4]. These key documents affirm the rights of every European citizen in the areas of human dignity, freedom, equality, solidarity, citizenship and justice.

As the ICT Research correctly declares: "Europe works hard to guard the 'four freedoms' – the free movement of people, goods, services and money… The efforts to improve our security, uphold democracy and freedom and deliver fair justice take place at all levels of the EU and in all spheres of its government and administration – from open collaboration, EU legislation and regulation, awareness-raising activities and numerous cooperative actions including R&D". [2]

Although the legislations and laws that Europe has established for its citizens to feel safe online, people still feel insecure and less confident with the ICT Technology. A better coordinated European response to personal data protection is part of the solution. Moreover there is the need to driving forward research into cutting-edge hardware and software security technologies for networks and services. It is also developing technologies that give users more control of their precious personal data.

According to Deliverable 7.1 [1] there are many key points that need to be taken into account. There is the need to develop services which will ensure that the personal data should not be stored, transferred, edited etc if the European laws are not obeyed. Citizens must be aware that they are monitored and they should know their rights.

The EU Directive on the identification and designation of European Critical Infrastructures specifically mentions the ICT sector as one of Europe's critical infrastructures. It is crucial that we can trust hardware and software to be robust, resilient and reliable. **ICT must be trustworthy.**

One of the major objectives of the SafeCity Project is to establish an intelligent Public Safety system in respect with the human rights, European Legislations in personal data protection and national laws. The Public Safety policies which are mentioned in the following sections aim to ensure that the proposed technologies will be legally and socially respectful.

5.3 Overlaying Management Protocols

The system proposed in the SafeCity project and established during the PoC has taken into consideration all legal, ethical and social implications. As we have already mentioned developers have to take into account the legal, social and ethical framework and research has to be accomplished regarding the security aspects and the protection of data.

We should also consider that the handling and control of data cannot be a priori controlled by developers and are therefore left to the hands of PS organizations' internal procedures to be maintained.

As mentioned in the Deliverable 7.1 [1] the **data controller** must be identified taking into account all types of delegations of service provision that may happen. So, in the public safety scenario for example, the data controller may be the Command and Control center operator, the provider of technical services, or third parties having been made responsible for the data processing, or all of these actors simultaneously. Due account must be taken of the fact that the scenario involves a network of actors, and of applications, and therefore complexities regarding the ascription of responsibilities among actors. It is the duty of the data controller to assess the quality of the data processor and his ability to provide adequate security measures. Furthermore the data controller has to define precisely, in a written contract, the missions of the data processor, and to check if the data processor does respect entirely the limits of his contractual duties.

Management Protocols outline security protocols for all faculty and staff participating in public safety activities. There should be a constant control that the security systems work properly, that the data processor respects the privacy of the data he handles and all legal aspects are obeyed.

5.4 Public Safety Policies

Policies as have identified during the implementation of PS Use Cases and the implementation of the SafeCity Project.

Unique Reference Name	Reference Name	Level (EU, local)	Objective	Guidelines and restrictions
P.1	Kind of data to be acquired (type of sensors)	EU	Adequate, relevant and not excessive personal data	Images, video (CCTV Cameras), voice, environmental measures etc only from the surveilled area and not from inside a

				resident's window for the purposes referred to the P.2
P.2	Justified reasons of the specific types of data to be acquired	EU	Fairly and lawfully processed of personal data	Data are gathered in order to : - Monitor the area of suspicious objects/people in terms of left objects that may contain bombs or identified criminals (decrease the criminality ratio) - Monitor the entry in secure areas - Detect orphan objects - Detect suspicious behavior (in terms of suspicious movement patterns, such as loitering) - Monitor the area for environmental factors and indicators - Monitor the road conditions (weather, traffic flows and fluency)
P.3	Selection of places from where such data are to be acquired	EU, local	Adequate, relevant and not excessive personal data Respect to citizen privacy	- City's areas of high criminality - Roads of high ratio of accidents - Roads of high traffic - Secure areas There must be signs in the surveilled areas informing for the monitoring system The monitoring inside a residence is forbidden The authorities should obtain a detailed plan of the installed system and the exact positions of the sensors
P.4	Validation of the acquired data	local	Fairly and lawfully processed of personal data	- Masking capabilities to the cameras in order not to collect sensitive data - Correct programming of the sensors to obtain only the

				desired information - The data acquired from the sensors must be checked once a month by a team of experts (plus the functionality of the sensors) - The team of experts must fill a consent report - The report must be validated by the superior of the PS department - The surveyed areas must be checked once a week to notice any changes in the system - A report must be filled in and validated by the superior of the PS department
P.5	Testing of the sensors before the installation	Local	Personal data processing compliance Adequate, relevant and not excessive personal data	- The sensors/cameras must be tested before installation to ensure that they obtain only the desired information - An official permission must be given in order for the sensors to start functioning and retrieve data
P.6	Testing and validation of the sensors/cameras after the installation at a 1 month basis	Local	Adequate, relevant and not excessive personal data Legitimacy of personal data processing by reasons of national security	-The sensors/cameras must be tested after installation to ensure that they obtain only the desired information - Once a year a report on the effectiveness of the system must be accomplished (e.g. statistics on the decrease of crimes, traffic flow graphs etc)
P.7	Testing and validation of the communication channels between the sensors and the gateway (ad-hoc networks)	Local	Security in the processing of personal data Confidentiality of the personal data	- Testing of the security techniques used upon the integrity of the system's components, information exchange and data loss - on a 7 days basis - Reports on potential threats detected - Continuous update of the security protocols

				- Checks accomplished by authorized controllers
P.8	Data storage time for the sensors network	EU, Local	Personal data collection for specific, explicit and legitimate purposes. Security in the processing of personal data	Data stored in the sensors network for a very short time obeying the latency requirements of the C2 Center Usage of encryption techniques
P.9	Data Storage time for the processing network	EU	Personal data collection for specific, explicit and legitimate purposes. Security in the processing of personal data No personal data storage longer than needed	- 7 days interval - The database is accessible only by a local network - Password protected; passwords change frequently and automatically - Access to the database has only authorized personnel of the C2 Center with limited permissions (not editing/deleting rights) - Data are stored in an encrypted format
P.10	Data Management Personnel responsible in the sensors network area	Local	Security in the processing of personal data Confidentiality in the processing of personal data	- Authorized data controllers checking the functionality of the sensors and the gateway - Authorized personnel checking the security of the communication channels - No access to the personal data - Fill in reports and send them for validation to the superior of the relevant department of the city's authorities
P.11	Data Management Personnel responsible for the processing network area	Local	Security in the processing of personal data Confidentiality in the processing of personal data	- Authorized operators of the C2 Center - Being supervised - Reports in case of an incident - Access to the database only in case of an incident detected (alert) and after the permission of the supervisors - Objective selection of the

				personnel
P.12	Reports generation upon the data's movements at any time	Local	Data subject rights	The authorized personnel is responsible to generate reports at any time regarding the movement of each citizen personal data after a citizen's request The reports must be checked by external supervisors before being submitted to the citizen (if they are corresponding to the true situation)
P.13	Data Security from the Gateway to the C2 Center	Local	Security in the processing of personal data Confidentiality in the processing of personal data No personal data storage longer than needed	- Testing of the security techniques used upon the integrity of the system's components, information exchange and data loss - on a 7 days basis - Reports on potential threats detected - Continuous update of the security protocols - Checks accomplished by authorized controllers - Usage of encryption techniques
P.14	Data access	Local	Data subject rights Security in the storage of personal data	- Data access must be permitted to the citizens under request, except if there are other citizens that are compromised - Data access must be allowed only in the authorized personnel and only if it is necessary - The accessibility must be controlled by the following ways: 1. Log files of who has entered the database and the actions he has made (automatically generated by the system) 2. Passwords must change frequently by the supervisors 3. The operator who wants to

				access the database must request special permission explaining the reasons he wants to act so
P.17	Checking the personal stored data integrity procedures	Local		Data checking upon: - if they are still in use - if they have been erased properly
P.18	Destruction of personal data	Local, EU	No personal data storage longer that needed Security of personal data	- Automatically - Manual destruction only under request and only by authorized personnel - In a 7 days basis
P.19	Data erase processes	Local, EU	Security of personal data No personal data storage longer that needed	- Effective - Keep up with new technologies and threats - Everyday check upon the effectiveness, data loss, level of security
P.20	Citizens awareness of the installed system	EU, Local	Respect to citizen privacy Data subject rights	- By using the traditional methods of mass approach and dissemination - Citizens awareness of any changes to the system (e.g. regarding the installation of a new sensor) - Information given to the citizens should include brief remarks of the accountable authority, the means (e.g. CCTV cameras, microphones, kinds of sensors etc) being deployed, the types of data and their rights
P.21	Legal authorization for each of the sensor sites	Local	Prior legal authorization required	The installation of any kind of surveillance system is forbidden if it is not legally authorized
P.22	System's validation and check	Local	Security of the processing of personal data	- Frequently - By authorized controller -Reports generation - Monitoring of the reports by external supervisors
P.23	Versioning of the system's	Local	Security of the processing of	- Each application's, protocol's etc versioning

	respective protocols, applications etc		personal data	must be clearly marked and reported - Any changes in the versioning must be reported
P.24	Reports upon potential threats and attacks	EU, Local	Security in the processing of personal data Confidentiality in the processing of personal data	In case of a malicious attack a report must be generated and submitted to the accountable authorities National wide knowledge transfer
P.25	Social feedback upon the citizens' acceptance	Local	Respect to citizen privacy	Frequent polls to find out the citizens' acceptance Offer the means to the citizens to make their complaints/suggestions etc The system is not going to be installed if the citizens do not accept it
P.26	Dissemination of the system's outputs	EU, Local	Respect to citizen privacy	Publishing of alerts generated from the system (e.g. publish to television/radio, road-signs, alerts to citizens' smart phones in case of an incident near to their location)
P.27	Definition of criminal activity	EU, local	Objective criteria under an individual is marked as suspicious/criminal	- The database of criminals is unreachable by anyone without permission as provided by law. - Suspicious/Criminal activity is determined regardless the nationality, skin color, religion of the object - Both system's results and human intervention are required for decision making
P.29	Handling data amongst different organizations, countries etc	EU, local	Legal transfer of personal data	- Data transfer between different organizations of the country is allowed after authorized permission (in national level) - Data transfer between different member states of the European Union is allowed after authorized permission (in European

				level) - Data transfer between a member state and a non-member state is allowed after authorized permission (in European and national level) - The subject must be aware of the data transfer and the way they are transferred (paper, digital format etc.) - Data transfer by using encryption techniques
P.30	Establishment of a Local Surveillance Commission	Local	Data subject rights Personal data legislation compliance	- Handling matters regarding the surveillance system - Consisting of legal entities, experts on surveillance systems, members of the city's authorities and other high qualified members - Supervised by National Government and EU authorities
P.31	Command and Control Center Personnel	Local	Security of personal data processing Confidentiality of personal data processing	- Operated by policemen expertise in decision making - Permission to view on-line images in the consoles - Different access levels between the personnel

6. Conclusions

This deliverable presented the policies that have been created towards the Safecity Project execution. Major Input has been collected towards the project execution, but also during the execution of the two PoCs (In Stockholm and Madrid). Taking account of all the ethical, social and legal implications in European and national level we presented the overall policy making framework for Safecity.